Information Fusion-based Cybersecurity Threat Detection for Intelligent Transportation System

Abdullahi Chowdhury
School of Computer Science
The University of Adelaide
Adelaide, Australia
abdul.chowdhury@adelaide.edu.au

Ranesh Naha
School of ICT
University of Tasmania
Hobart, Australia
raneshkumar.naha@utas.edu.au

Shahriar Kaisar
Dept. of IS and Business Analytics
RMIT University
Melbourne, Australia
shahriar.kaisar@rmit.edu.au

Mohammad Ali Khoshkholghi
Dept. of Computer Science
Middlesex University
London, UK
a.khoshkholghi@mdx.ac.uk

Kamran Ali
Dept. of Computer Science
Middlesex University
London, UK
k.ali@mdx.ac.uk

Antonino Galletta
Dept. of Computer Science
University of Messina
Messina, Italy
angalletta@unime.it

***Abstract*—Intelligent Transportation Systems (ITS) are sophisticated systems that leverage various technologies to increase the safety, efficiency, and sustainability of transportation. By relying on wireless communication and data collected from diverse sensors, ITS is vulnerable to cybersecurity threats. With the increasing number of attacks on ITS worldwide, detecting and addressing cybersecurity threats has become critically important. This need will only intensify with the impending arrival of autonomous vehicles. One of the primary challenges is identifying critical ITS assets that require protection and understanding the vulnerabilities that cyber attackers can exploit. Additionally, creating a standard profile for ITS is challenging due to the dynamic traffic pattern, which exhibits changes in the movement of vehicles over time. To address these challenges, this paper proposes an information fusion-based cybersecurity threat detection method. Specifically, we employ the Kalman filter for noise reduction, Dempster-Shafer decision theory and Shannon's entropy for assessing the probabilities of traffic conditions being normal, intruded, and uncertain. We utilised Simulation of Urban Mobility (SUMO) to simulate the Melbourne CBD map and historical traffic data from the Victorian transport authority. Our simulation results reveal that information fusion with three sensor data is more effective in detecting normal traffic conditions. On the other hand, for detecting anomalies, information fusion with two sensor data is more efficient.**

***Index Terms*—Information fusion, Cybersecurity, Intelligent Transport Systems, Threat Detection**

I. Introduction

The widescale adoption of Intelligent transportation systems (ITS) globally has resulted in enhanced traffic and safety conditions, reduced traffic congestion, and rapid dissemination of critical traffic updates. ITS uses a variety of technology, including sensors, communication systems, and data analytics tools, to monitor and optimise traffic flow, route planning, and other elements of transportation management in real-time. Anomalies in Intelligent Transportation Systems (ITS) refer to any behaviour or activity that deviates from normal or expected patterns of behaviour, which can indicate that the ITS system is under cyberattack. Anomalies can significantly impact the performance of ITS and may lead to service disruption, traffic congestion, financial loss, and loss of lives [1]. Perrine et al. [2] demonstrated that disabling as few as seven signals during peak time periods for a few hours using the maximum vehicle affected model can cost around US$0.93 million, and the maximum vehicle flow targeting method can cause damage of around US$0.98 million if 26 signals are impacted. Therefore, relevant research communities are actively working on anomaly detection techniques in ITS.

Detecting anomalies in Intelligent Transportation Systems (ITS) is crucial as they can significantly impact the identification of potential cyberattacks, prevent accidents and other incidents, and improve transportation efficiency and safety. Anomaly detection can be used in intelligent traffic management systems to monitor and respond to traffic incidents in real-time, improving traffic flow and reducing congestion. In [3], the authors utilised a dynamic traffic system model to illustrate the impact of traffic signal attacks. With computational efficiency, they were able to simulate the network-wide effects of intersection failures. They also performed green traffic signal phase time analysis, which provided insight into detecting intrusions. However, a theoretical model for intrusion detection and its evaluation and validation have not been specifically performed. A visual analytics technique was suggested by Turner et al. [3] to identify unusual signal patterns that could indicate intrusions into the system. The work focuses on data signal attacks, DoS and DDoS attacks, and light control attacks. The authors provide a detailed analysis of these attacks and describe their impact on ITS. In recent work, Xiang et al. [4] proposes a novel approach for predicting congestion attacks. The authors focus on variable spoofing frequency attacks, which is a type of GPS spoofing attack, and developed a machine learning-based approach for predicting these attacks in traffic signal systems. To advance the research in this area, [5] introduced an approach for identifying traffic signal intrusion. However, the main problems with these

approaches are that important traffic signal parameters, such as vehicle speed are not considered. Besides, while creating the baseline traffic scenarios, the noise of the traffic characteristic while collecting traffic data was not considered. By addressing these research issues we introduce an Information fusion-based anomaly detection system for ITS with the following important contributions:

- A theoretical model was developed to generate a baseline traffic flow model for ITS. This model utilises real-time and historical traffic data to detect anomalies using an information fusion technique. The proposed information fusion-based anomaly detection process involves data preprocessing (noise detection using Kalman filter), probability calculation, and decision-making to improve the accuracy of anomaly detection by combining data from multiple sensors and sources.
- For the first time in ITS anomaly detection, we addressed the issue of reducing noise in observed traffic conditions for different contexts (e.g., peak, off-peak, public holiday). To achieve this, we utilised the Kalman filter to develop a predictive traffic model as a baseline model. This approach significantly improves the accuracy and efficiency of our system.
- A dynamic statistical anomaly detection model was developed to represent the distribution of data at different intersections for different time windows. The proposed statistical model is used to identify data points that fall outside the expected range of values by setting a threshold based on the probability distribution and using information fusion.

II. Related Works

ITS face a multitude of attack vectors, such as cyberattacks targeting autonomous and cooperative automated vehicles, Distributed Denial of Service (DDoS) attacks, and assaults on traffic signals and routing systems. Petit and Shladover [6] investigated potential cyberattacks on autonomous and cooperative automated vehicles. The authors identify several types of attacks, including spoofing, jamming, malware injection, DoS, and fake message injection, that can be performed on different attack surfaces of autonomous and cooperative automated vehicles. In addition, the work highlights the vulnerabilities of communication devices such as navigators, sensors, cameras, and connections like GPS, USB, Bluetooth, Wi-Fi, and Zigbee in these systems. Sun et al. [7] reviewed the security and privacy issues in the Internet of Vehicles (IoV). The authors classify five broad types of attacks, including attacks on Authentication, availability, secrecy, routing, and data authenticity attacks., and explore the relevant solutions. Specific attacks mentioned in the paper include Sybil, GPS deception, masquerading, wormhole, eavesdropping, and Denial of Service (DoS) attacks, as well as route modification and replay attacks, among others. Using complex network theory, Han and Lin [8] analysed the features of public transportation systems by constructing a complex network of transportation systems. They investigated the robustness of these systems under fixed and random attacks and found better resilience under random attacks. A multivariate stream analysis approach proposed to identify and mitigate DDoS attacks in VANETs was proposed by Kolandaisamy et al. [9]. The authors emphasise the importance of Identifying and preventing DDoS attacks in VANETs to ensure the reliability and safety of vehicular networks.

Huq el al. [10] presented some real-world ITS attacks. Alnbulsi and Islam [11] investigate to protect against code injection attacks. In a code injection attack, the attacker injects malicious code into a vulnerable application in order to execute unauthorised commands. The attacker typically exploits a vulnerability in an application's code or input validation routines to inject and execute their code. The injected code can be used to modify or delete data, install malware, steal sensitive information, or carry out other malicious activities. Code injection attacks can manifest in various forms, including SQL injection, command injection, and buffer overflow attacks [12]. These attacks can be very damaging, leading to system crashes, data loss, or even full system compromise.

In [9], authors developed a sophisticated multivariate stream analysis approach for detecting and mitigating Distributed Denial of Service (DDoS) attacks in VANETs. Their method relied on vehicle-to-vehicle communication via Road Side Units (RSUs), and they evaluated its performance using an NS2 simulator. The findings of their study indicate that the approach is highly effective in identifying DDoS attacks and minimising their effects on VANET communication. Turner et al. [3] proposed a visual analytics framework for detecting potential attacks on traffic control systems. The authors preprocess the traffic light data to correct errors and detect missing entries. They then generate an overview of the data using calculations such as the decomposition of traffic light cycles and statistical computation. This overview helps in detecting abnormal patterns in traffic light data and can aid in detecting DoS attacks, data signal attacks, and light control attacks. Xiang et al. [4] proposed a machine learning approach to predict congestion attacks. To accomplish this, the authors created a spoofing attack scenario and collected traffic flow data with various spoofing frequencies. The authors identified the potential congestion attacks by extracting vital features from traffic flow data and utilising ensemble learning techniques to detect the correlation between these features and the occurrence of abnormal congestion and attacks. With the aid of supervised learning using past data, their system can analyse the current attack frequency and forecast potential congestion attacks.

Although the above approaches shed some light on anomaly detection in ITS, they did not take into account crucial traffic signal parameters, such as vehicle speed is not considered. In addition, they did not properly construct a mass value function for flow rate and speed. Furthermore, they did not properly address the noise characteristics of traffic patterns.

III. Proposed Anomaly Detection System

The proposed approach uses an information fusion technique to detect anomalies in ITS. The information fusion

(for multi-sensor data) technique combines information from multiple sensors to obtain a more accurate and complete representation of the monitored ITS. In the case of using evidence from three different types of sensors in ITS, the process involves combining data from all three sensors to obtain a more reliable and robust estimate of the measured quantity.

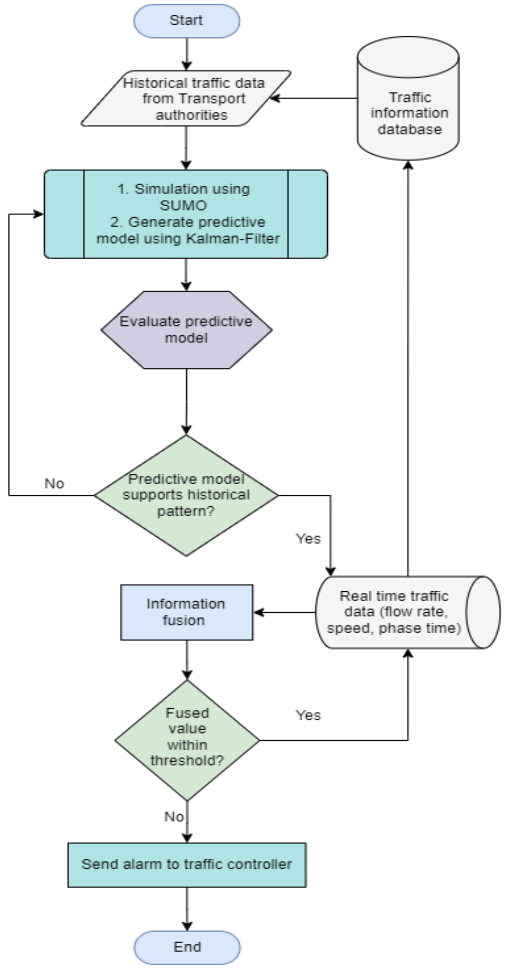


Fig. 1. The operational flow chart of the proposed anomaly detection system.

A. Overview of the Proposed Anomaly Detection System.

The flow chart of our proposed model is shown in Figure 1. The steps to perform information data fusion using evidence from three sensors are:

1) Collect data from three sensors: Collect data (flow rate, Average vehicle speed, and phase time) from three sensors that measure the same quantity or parameter. The data collection method is described in Section III-B
2) Pre-process the data: Pre-process the data from each sensor to remove any noise, outliers, or errors. This may involve filtering, smoothing, or interpolation. In this step, baseline traffic characteristics for the observed intersection are created (refer to Section III-D).
3) Combine the data: Combine the data from all three sensors using a fusion algorithm. Two fusion algorithms, including Kalman filtering and the Bayesian method (Dempster-Shafer decision theory), are used to calculate the probability of normal observations for individual and multiple sensors. The fusion algorithm should consider the sensors' characteristics, such as their accuracy, precision, reliability, and correlation between the measurements.
4) Evaluate the results: Evaluate the sensor data fusion results to determine the estimate's accuracy and reliability. This involves comparing the fused estimate with the measurements from each individual sensor or with a reference measurement obtained from another source to detect anomalies.
5) Refine the fusion algorithm: If the results of the sensor data fusion are not satisfactory, refine the fusion algorithm by adjusting the parameters or using a different fusion method. By using evidence from three sensors and performing sensor data fusion, obtaining a more accurate and reliable estimate (detecting anomaly) of the measured quantity is possible than from any individual sensor alone.

B. Traffic data monitoring

For the simulation setup, we used Simulation of Urban Mobility (SUMO) [13]. The historical hourly traffic data was collected from VicRoads [14]. Vicroads uses Sydney Coordinated Adaptive Traffic Systems and different in-road sensors to collect these data. The flow rate, average vehicle speed, and phase time for three intersections of Melbourne CBD were taken from Victoria's (Australia)Department of transport Open hub data [15].

Phase time refers to the duration of time that a specific signal phase is active. A signal phase is a specific combination of traffic movements that are allowed to proceed at a traffic signal, such as vehicles travelling through an intersection in a particular direction or pedestrians crossing the street. The duration of the phase time is typically set based on factors such as traffic volume, pedestrian demand, and the length of the crossing distance. In SCATS, phase time can be adjusted dynamically in response to real-time traffic conditions.

Cycle time, on the other hand, refers to the total time required for all signal phases to be completed and for the traffic signal to return to the first phase. It includes the time for each individual phase as well as any necessary delay between phases. Cycle time is typically determined based on factors such as the number of phases, the amount of time needed to clear traffic from each phase, and the amount of time required for pedestrian crossings. In SCATS, cycle time can also be adjusted dynamically to respond to changes in traffic demand. Average vehicle speed refers to the average speed of vehicles travelling through a given section of roadway over a specific period of time. It is typically measured using sensors placed along the roadway that detect the passage of individual vehicles and record their speed. Average vehicle speed is a

key indicator of traffic congestion, as slower speeds are often associated with higher levels of congestion.

Flow rate, on the other hand, refers to the number of vehicles passing through a given section of roadway per unit time. It is typically measured using sensors that detect the passage of individual vehicles and record the time at which each vehicle passes the sensor. Flow rate is a key indicator of traffic volume, as higher flow rates are typically associated with higher levels of traffic.

In ITS using SCATS, average vehicle speed and flow rate are used to optimise traffic signal timing by adjusting the duration of signal phases and cycle times in response to real-time traffic conditions. For example, if average vehicle speeds are lower than normal or flow rates are higher than normal, SCATS may adjust signal timing to give priority to the direction of traffic with the highest demand in order to reduce congestion and improve traffic flow.

C. Baseline model

Developing a traffic predictive model involves using historical traffic data and traffic volume estimates from the Kalman filter to forecast future traffic volumes.

D. Kalman filter for noise reduction

By using historical traffic data and the traffic volume estimates from the Kalman filter to develop a traffic predictive model, it is possible to obtain more accurate and reliable traffic flow data. This can be used to optimise traffic flow and manage congestion during peak periods, resulting in a more efficient and safe transportation system.

We consider the ITS as a stochastic system that is linear and varies discretely over time with k sensors as:

$$x(\Upsilon+1) = \alpha(\Upsilon)x(\Upsilon) + \beta(\Upsilon)i(\Upsilon) + \gamma(\Upsilon)\xi(\Upsilon), \quad (1)$$

$$y_i(\Upsilon) = G_i(\Upsilon)x(\Upsilon) + \psi_i(\Upsilon), \quad i = 1, 2, ..., k. \quad (2)$$

In the above equations, $x(\Upsilon) \in R^n$ represents different states while $y_i(\Upsilon) \in R^{m_i}$ shows the measurement of different sensors. Here, $i(\Upsilon) \in R^p$ represents a known control input, white noises are represented by $\xi(\Upsilon) \in R^r$ and $\psi(\Upsilon) \in R^{m_i}$, and $\alpha(\Upsilon)$, $\beta(\Upsilon)$, $\gamma(\Upsilon)$, and $G_i(\Upsilon)$ indicates matrices with time-varying properties and compatible dimensions. Considering the above representations, similar to the work proposed in [16], the following assumptions can be made:

A1. white noises $\xi(\Upsilon)$ and $\psi_i(\Upsilon)$ are correlated with zero mean and following properties:

$$\mathfrak{E}\left\{\begin{bmatrix}\xi(\Upsilon)\\ \psi(\Upsilon)\end{bmatrix}\begin{bmatrix}\xi^T(l) & \psi^T(l)\end{bmatrix}\right\} = \begin{bmatrix}Q(\Upsilon) & S_i(\Upsilon)\\ S_i^T(\Upsilon) & R_i(\Upsilon)\end{bmatrix}\delta_{\Upsilon l},$$

$$\mathfrak{E}\left[\psi_i(\Upsilon)\psi_j^T(l)\right] = S_{ij}(\Upsilon)\delta_{\Upsilon l}, \quad i \neq j. \quad (3)$$

Here, the mathematical expectation is represented with $\mathfrak{E}$ while the transpose matrix is represented with superscript T. The Kronecher delta function is denoted with $\delta_{\Upsilon l}$

A2. The initial state $x(0)$ does not depend on white noises $\xi(\Upsilon)$ and $\psi_i(\Upsilon)$, where $i = 1, 2, ..., k$, and the maintains the following:

$$\mathfrak{E}x(0) = \mu_0,$$

$$\mathfrak{E}\left[(x(0) - \mu_0)(x(0) - \mu_0)^T\right] = P_0 \quad (4)$$

Considering the measurements at state $x(\Upsilon)$ from different sensors, i.e., $y_i(1), y_i(2), ..., y_i(\Upsilon)$, the Kalman filter for the optimal information fusion $\hat{x_0}(\Upsilon|\Upsilon)$ that can meet the following requirements:

requirement 1 there are no biases, i.e., $E\hat{x_0}(\Upsilon|\Upsilon) = Ex(\Upsilon)$

requirement 2 identification of the optimal values for the matrix weights $\bar{A}_i(\Upsilon)$, where $i = 1, 2, .., k$ that can minimise error variance for filtering with $\tau\left[H_0(\Upsilon|\Upsilon)\right] = min\{\tau\left[H(\Upsilon|\Upsilon)\right]\}$. Here, $H(\Upsilon|\Upsilon)$ and $H_0(\Upsilon|\Upsilon)$ represent the variance of an arbitrary and optimal fusion filter, respectively, with the weights of matrix and τ shows the trace of a matrix. Sun and Deng [16] considered the linear minimum variance and established that the maximum likelihood fusion criteria can be met even without considering a standard normal distribution. Interested readers may refer to that study.

Under the assumptions specified in A1 and A2, the i-th local sensor subsystem of system (1) and (2) (which incorporates multiple sensors) can attain the most optimal Kalman filter and leading to the following equations.

$$\hat{x_i}(\Upsilon+1|\Upsilon+1) = \hat{x_i}(\Upsilon+1|\Upsilon) + D_i(\Upsilon+1)\chi_i(\Upsilon+1), \quad (5)$$

$$\hat{x_i}(\Upsilon+1|\Upsilon) = \bar{\alpha_i}(\Upsilon)\hat{x_i}(\Upsilon|\Upsilon) + \beta(\Upsilon)i(\Upsilon) + L_i(\Upsilon)y_i(\Upsilon) \quad (6)$$

$$\chi_i(\Upsilon+1) = y_i(\Upsilon+1) - G_i(\Upsilon+1)\hat{x_i}(\Upsilon+1|\Upsilon), \quad (7)$$

$$D_i(\Upsilon+1) = P_i(\Upsilon+1|\Upsilon)G_i^T(\Upsilon+1)[G_i(\Upsilon+1)P_i(\Upsilon+1|\Upsilon) G_i^T(\Upsilon+1) + R_i(\Upsilon+1)]^{-1}, \quad (8)$$

$$P_i(\Upsilon+1|\Upsilon) = \bar{\alpha_i}(\Upsilon)P_i(\Upsilon|\Upsilon)\bar{\alpha_i}^T(\Upsilon) + \gamma(\Upsilon)[Q(\Upsilon) - S_i(\Upsilon)R_i^{-1}(\Upsilon)S_i^T(\Upsilon)]\gamma^T(\Upsilon) \quad (9)$$

$$P_i(\Upsilon+1|\Upsilon+1) = [I_n - D_i(\Upsilon+1)G_i(\Upsilon+1)]p_i(\Upsilon+1|\Upsilon), \quad (10)$$

$$\hat{X}_i(0|0) = \mu_0 \quad P_i(0|0) = P_0. \quad (11)$$

$$\bar{\alpha_i}(\Upsilon) = \alpha_i(\Upsilon) - L_i(\Upsilon)G_i(\Upsilon) \quad (12)$$

$$L_i(\Upsilon) = \gamma(\Upsilon)S_i(\Upsilon)R_i^{-1}(\Upsilon) \quad (13)$$

The equations above feature $D_i(\Upsilon)$ and $\chi_i(\Upsilon)$, which correspond to the filtering gain matrix and innovation process (i^{th} sensor) subsystem. Additionally, the matrices $P_i(\Upsilon|\Upsilon)$ and $P_i(\Upsilon+1|\Upsilon)$ represent the filtering and prediction error variance for the first step, respectively.

The proposed model entails each sensor subsystem evaluating the states and conducting independent anomaly detection. If a subsystem detects an anomaly, it is isolated and reported. Otherwise, the estimations are transmitted to the initial fusion layer. In this layer, the estimation error of all the pairs of sensors is utilised to calculate the cross co-variance in each time step. The estimations along with the variances are also passed to the next fusion layer where these values from faultless subsystems are used to determine the optimum values for the weight matrix and attain the optimal fusion filter.

In our proposed scenario we can consider that it uses multiple sensors to measure different attributes, such as average vehicle speed, signal phase time, and flow rates. In this case, a system with three sensors can be denoted as:

$$x(t+1) = \begin{bmatrix} 1 & T & T^2/2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \xi(t), \quad (14)$$

$$y_i(t) = G_i x(t) + \psi_i(t), \quad (15)$$

where $\psi_i(t) = \lambda_i \xi(t) + \eta_i(t)$, $i = 1, 2, 3$ and the sampling period is presented with T. If ss(t), $sf(t)$, and $sp(t)$ represent the vehicle speed, flow rate, and phase time, at time t respectively, the state can be denoted as,$x(t) = \begin{bmatrix} sf(t) & ss(t) & sp(t). \end{bmatrix}$. The measurement signals and noises at time t are depicted with $y_i(t)$ and $\psi_t(t)$, respectively, for $i = 1, 2, 3$. $\xi(t)$ shows the Gaussian white noise that has a mean of zero and a variance of σ_ξ^2. Furthermore, λ_i shows a constant scalar while $\eta_i(t)$ shows a Gaussian white noise independent of $\xi(t)$ with zero mean and variance matrices $\sigma_{\eta_i}^2$. The objective here is to determine the optimal Kalman Filter ($\hat{x_0}(t|t)$) for information fusion.

Using the historical data from Vicroads, we simulated both normal and intrusion scenarios in traffic signal systems. To simulate normal traffic conditions, the flow rate, vehicle speed, and phase time of a specific intersection were obtained from our simulation model developed using SUMO, with traffic distributions initiated using normal historical traffic information obtained from the VicRoads online data [14]. To replicate real-world traffic conditions in our simulation, we selected the density, vehicle speed, and phase time of incoming and outgoing traffic for the intersection of interest from the range of historical data collected from 2016-2018 available on the VicRoads website.

For intrusion scenarios, the vehicle speed, flow rate, and/or average phase time for a specific scenario were changed to simulate an attack on the traffic signals. The intrusion was simulated by inducing changes in either the flow rate, vehicle speed, or phase time of the intersection. If the intrusion lasts for a very short time (less than one cycle time), the data for flow rate, vehicle speed, and phase time will remain within the range of 68% to 95% confidence intervals. However, if the intrusion lasts longer, the data will go outside the 95% confidence interval. In order to address both short and long-term intrusions, adjustments were made to the flow rate, vehicle speed, or phase time to ensure they fell within the 68% to 95% confidence intervals in some instances (Scenario 2, Scenario 4, and Scenario 6), while exceeding the 95% confidence intervals of the corresponding historical data in other instances. The induced average vehicle speed of an intersection was also inserted while the phase time and flow rate were kept normal.

E. Probability Mass Function

We utilise an inference method based on DS decision theory [17] to determine whether an ITS is functioning normally or abnormally. To define the frame of discernment, our system uses three propositions for an observation being: normal ($\mathfrak{N}$), intruded ($\mathfrak{I}$), and uncertain ($\mathfrak{N} \vee \mathfrak{I}$). We statistically measure the belief function for each sensor for flow rate, vehicle speed, and phase time. We utilise probability mass functions based on historical data from the corresponding time window of that day (15-minute intervals) to calculate the probability of any specific observation being normal.

The lower limit of the probabilistic value of the j^{th} intersection being normal for y events can be defined using the belief function of the DS theory [18]:

$$bel_j(\mathfrak{N}) = \frac{1}{1-k} \times \sum_{\cap E_w(t) = \mathfrak{N} \neq \emptyset} ; \prod_{1 \leq w \leq y} m_j(E_w(t)) \quad (16)$$

where k is defined as:

$$k = \sum_{\cap E_w(t) = \emptyset} ; \prod_{1 \leq w \leq y} m_j(E_w(t)) \quad (17)$$

As per Shannon information theory [19], the uncertainty is the highest when $m_j(E_w(t)) = m_{jw}(\mathfrak{N})$=0.5. Note, here, $m_{jw}(\mathfrak{N})$ denotes the probabilistic value of a mass function for w^{th} event ($E_w(t)$) having j^{th} intersection being normal. If the value of $m_{jw}(\mathfrak{N})$ moves in either direction from 0.5, the uncertainty decreases. The uncertainty associated with $m_{jw}(\mathfrak{N})$ i.e., the probability, m_{jw} $(\mathfrak{N} \vee \mathfrak{I})$ is defined as:

$$\begin{aligned} m_{jw}(\mathfrak{N} \vee \mathfrak{N}) = -m_{jw}(\mathfrak{N}) log_2 m_{jw}(\mathfrak{N}) - \\ (1 - m_{jw}(\mathfrak{N})) log_2 (1 - m_{jw}(\mathfrak{N})) \end{aligned} \quad (18)$$

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

$$m_{jw}(\neg \mathfrak{N}) = 1 - m_{jw}(\mathfrak{N}) - m_{jw}(\mathfrak{N} \vee \mathfrak{I}) \quad (19)$$

The upper limit (plausibility) of j^{th} intersection being normal is defined as:

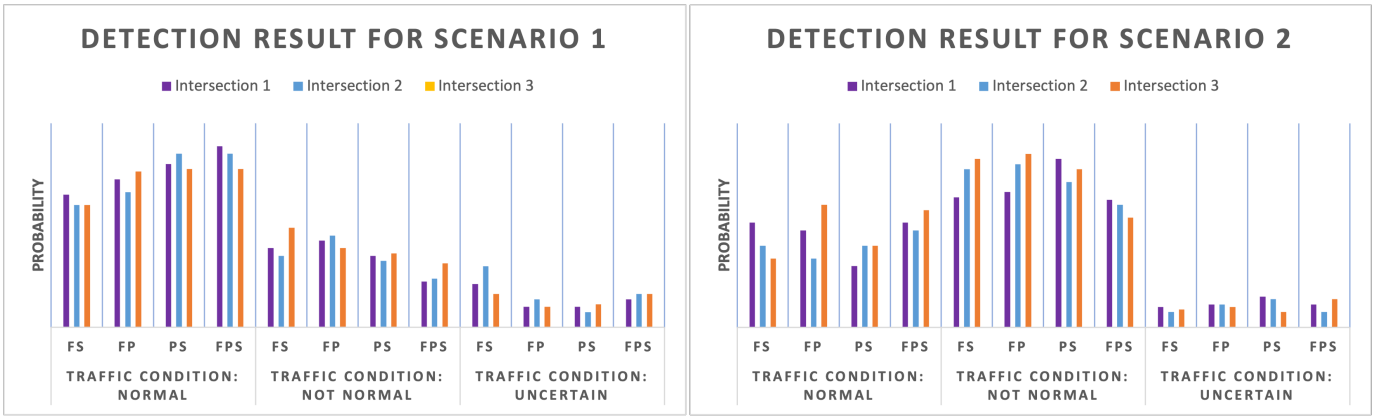
$$pl_j(\mathfrak{N}) = 1 - bel_j(\mathfrak{I}) \quad (20)$$

For obtaining the uncertainty value and then the belief value using (18) and (16), respectively, we need to calculate $m_j(E_w(t))$ for the flow rate, vehicle speed and phase time.

One or more of the sensors used to collect data for the TMS may be targeted by an attacker seeking to intrude. To detect any such intrusions, we can compare the observed values of a sensor with its corresponding original historical

TABLE I
THE OVERALL PROBABILITY FOR FLOW RATE, PHASE TIME, AND AVERAGE VEHICLE SPEED IN SIX DIFFERENT SCENARIOS (S1-S6)

	F			S			P		
	$P(\mathfrak{N})$	$P(\mathfrak{I})$	$P(\mathfrak{N} \vee \mathfrak{I})$	$P(\mathfrak{N})$	$P(\mathfrak{I})$	$P(\mathfrak{N} \vee \mathfrak{I})$	$P(\mathfrak{N})$	$P(\mathfrak{I})$	$P(\mathfrak{N} \vee \mathfrak{I})$
S1	0.56	0.32	0.12	0.61	0.28	0.11	0.68	0.2	0.12
S3	0.65	0.27	0.08	0.46	0.48	0.06	0.71	0.21	0.08
S5	0.49	0.34	0.17	0.43	0.45	0.12	0.57	0.3	0.13
S2	0.38	0.53	0.09	0.18	0.75	0.07	0.17	0.73	0.1
S4	0.22	0.72	0.06	0.41	0.47	0.12	0.25	0.67	0.08
S6	0.42	0.43	0.15	0.32	0.59	0.09	0.31	0.62	0.07



(a) Anomaly detection for normal traffic condition

(b) Anomaly detection for intruded traffic condition

Fig. 2. Probability for flow rate, average vehicle speed, and phase time for normal traffic condition and intruded traffic condition for Scenario 1 and 2.

values that have not been altered. To develop probability mass functions, denoted as $m_j()$, we employ a DS theory-based fusion approach defined in (16) and (20). By comparing the observed and historical values, our approach can identify any abnormal or anomalous sensor behaviour, which may indicate a security breach.

F. Results and Analysis

We used 1472 sample data points for the three intersections for each piece of evidence ($\mathfrak{F}$, $\mathfrak{P}$, $\mathfrak{S}$), the combination of two pieces of evidence ($\mathfrak{FP}$, $\mathfrak{PS}$, $\mathfrak{FS}$, $\mathfrak{FSP}$) and six different scenarios. Therefore, the total number of observations we used is $368 \times 3 \times 7 \times 6 = 185472$. These 1472 sample data points were distributed to 41, 39, and 42 observations (15-minute intervals) for Intersections 1, 2, and 3, respectively. Table I shows the probabilities of signals being normal ($\mathfrak{N}$), Intruded ($\mathfrak{I}$), and the uncertainty ($\mathfrak{N} \vee \mathfrak{I}$) for Scenarios 1-6 having various flow rates, average speeds, and phase times. Note, Scenarios 1, 3, and 5 were created using the original data collected from VicRoads to emulate normal traffic conditions without intrusion. Whereas, Scenarios 2, 4, and 6 were created to induce intrusions by using the same data but manipulating a combination of flow rate, phase time, and average vehicle speed.

Table I shows the probabilities of different traffic conditions for six different traffic scenarios, each characterised by three traffic variables: flow rate, vehicle speed, and phase time. The traffic conditions are classified into three categories: normal ($\mathfrak{N}$), not normal ($\mathfrak{I}$), and uncertain ($\mathfrak{N} \vee \mathfrak{I}$). The abbreviations used in the table are:

P($\mathfrak{N}$): Probability of normal traffic condition

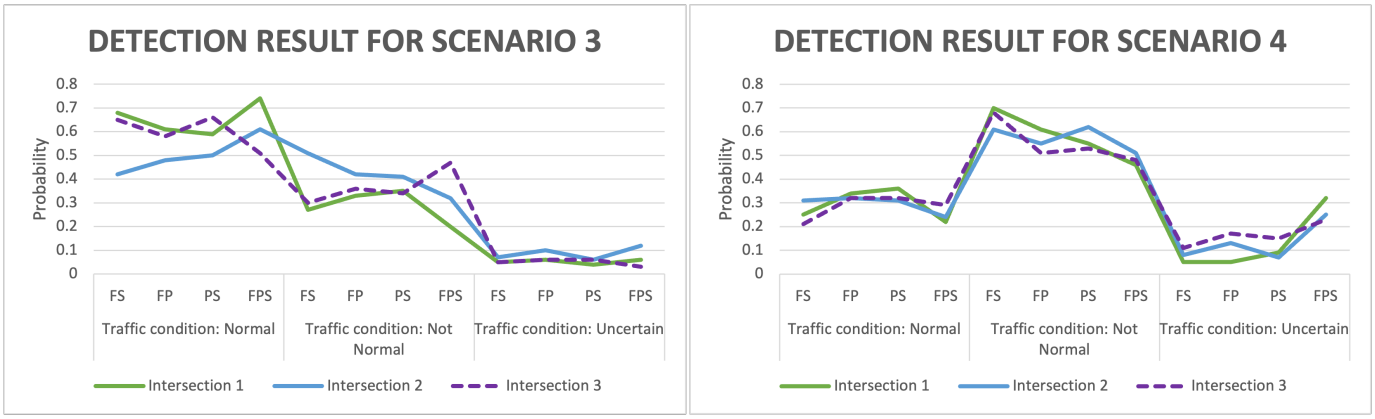
P($\mathfrak{I}$): Probability of not normal traffic condition

P($\mathfrak{N} \vee \mathfrak{I}$): Probability of uncertain traffic condition

For each traffic scenario (S1 to S6), Table I shows the probability values for each of the three traffic variables (flow rate, vehicle speed, and phase time) for each of the three traffic condition categories. For traffic scenario S1, the probability of having a normal traffic condition ($\mathfrak{N}$) is 0.56 for flow rate, 0.61 for vehicle speed, and 0.68 for phase time. The probability of having a not normal traffic condition ($\mathfrak{I}$) is 0.32 for flow rate, 0.28 for vehicle speed, and 0.2 for phase time. The probability of having an uncertain traffic condition ($\mathfrak{N} \vee \mathfrak{I}$) is 0.12 for flow rate, 0.11 for vehicle speed, and 0.12 for phase time. It is hard to determine whether the sensors were compromised by using data from a single sensor.

Figures 2a - 3b display the anomaly detection results and their uncertainty values produced by our system for Scenarios 1 to 4 for multiple sensors. We utilised four different combinations of two observations, including flow rate and phase time ($\mathfrak{FP}$), flow rate and vehicle speed ($\mathfrak{FS}$), phase time and vehicle speed ($\mathfrak{PS}$), and flow rate, phase time, and vehicle speed ($\mathfrak{FPS}$).

For intersection 1 in Figure 2a, the probability of having a normal traffic condition ($\mathfrak{N}$) is 0.52 for $\mathfrak{FS}$, 0.58 for $\mathfrak{FP}$, 0.64 for $\mathfrak{PS}$, and 0.71 for $\mathfrak{FPS}$. The probability of having a not normal traffic condition ($\mathfrak{I}$) is 0.31, 0.34, 0.28, and 0.18



(a) Anomaly detection for normal traffic condition

(b) Anomaly detection for intruded traffic condition

Fig. 3. Probability for flow rate, average vehicle speed, and phase time for normal traffic condition and intruded traffic condition for Scenario 3 and 4.

for $\mathfrak{FS}$, $\mathfrak{FP}$, $\mathfrak{PS}$, and $\mathfrak{FPS}$, respectively. The probability of having an uncertain traffic condition is 0.17, 0.08, 0.08, and 0.11 for the same traffic variables. The combination of flow rate, vehicle speed, and phase time in the FPS variable can provide a more nuanced understanding of traffic conditions than simply looking at the fused value of two sensors (e.g., $\mathfrak{FP}$, $\mathfrak{FS}$, $\mathfrak{PS}$). This is because $\mathfrak{FPS}$ captures the proportion of flow that is under the speed limit, which can be affected by both vehicle speed and phase time. Therefore, using combinations of three traffic conditions may indeed provide better results for analysing normal traffic conditions than using only two conditions. However, this would depend on the specific context (e.g., intruded traffic conditions) and it would require further analysis and validation.

The results of anomaly detection and their corresponding uncertainty values for Scenarios 1 to 4 across multiple sensors are presented in Figures 2a - 3b. Three distinct combinations of two observations were employed in the analysis, comprising of flow rate and phase time ($\mathfrak{FP}$), flow rate and vehicle speed ($\mathfrak{FS}$), phase time and vehicle speed ($\mathfrak{PS}$), and one combination of three observations, flow rate, phase time, and vehicle speed ($\mathfrak{FPS}$).

Figure 2a illustrates the outcomes of anomaly detection at Intersections 1, 2, and 3. The probability of normal traffic conditions ($\mathfrak{N}$) is 0.52 for flow rate and vehicle speed ($\mathfrak{FS}$), 0.58 for flow rate and phase time ($\mathfrak{FP}$), 0.64 for phase time and vehicle speed ($\mathfrak{PS}$), and 0.71 for flow rate, phase time, and vehicle speed ($\mathfrak{FPS}$) for Intersection 1. Conversely, the probability of not normal traffic conditions ($\mathfrak{I}$) is 0.31, 0.34, 0.28, and 0.18 for $\mathfrak{FS}$, $\mathfrak{FP}$, $\mathfrak{PS}$, and $\mathfrak{FPS}$, respectively. For uncertain traffic conditions, the respective probabilities are 0.17, 0.08, 0.08, and 0.11. The results indicate that the combination of three traffic conditions in $\mathfrak{FPS}$ can provide a more comprehensive analysis of traffic conditions compared to the fused value of two sensors, such as $\mathfrak{FP}$, $\mathfrak{FS}$, or $\mathfrak{PS}$. This is because $\mathfrak{FPS}$ captures the proportion of flow under the speed limit, which can be affected by both vehicle speed and phase time. However, this conclusion is dependent on contextual factors, such as intruded traffic conditions, and necessitates further investigation and verification.

Figure 2b presents the results of anomaly detection at Intersections 1, 2, and 3. For Intersection 1, the probability of normal traffic conditions ($\mathfrak{N}$) is 0.41, 0.38, 0.24, and 0.41 for flow rate and vehicle speed ($\mathfrak{FS}$), flow rate and phase time ($\mathfrak{FP}$), phase time and vehicle speed ($\mathfrak{PS}$), and flow rate, phase time, and vehicle speed ($\mathfrak{FPS}$), respectively. In contrast, the probability of not normal traffic conditions ($\mathfrak{I}$) is 0.51, 0.53, 0.64, and 0.5 for the same variables. Our analysis suggests that fusing all three sensors can result in better results if the traffic condition is normal (no sensors are intruded). However, if there is an intruded scenario, combining data from two sensors provides better results. Additional tests performed on normal and intruded traffic conditions are displayed in Figure 3a and Figure 3b, which support our findings.

Figure 3a presents the probabilities for normal traffic conditions at Intersection 1, where the values for flow rate and vehicle speed ($\mathfrak{FS}$), flow rate and phase time ($\mathfrak{FP}$), phase time and vehicle speed ($\mathfrak{PS}$), and flow rate, phase time, and vehicle speed ($\mathfrak{FPS}$) are 0.68, 0.61, 0.59, and 0.74, respectively. The probabilities for not normal traffic conditions for the same variables are 0.27, 0.33, 0.35, and 0.20, respectively. In Figure 3b, it is apparent that for all intersections, the probability of traffic conditions being not normal exceeds 0.5.

In this study, we evaluate the performance of our proposed model for detecting both intruded and nonintruded traffic scenarios through the use of four performance metrics - sensitivity, specificity, accuracy, and F1 score. The accuracy values range from 0.59 to 0.76 for no fusion, while the range increases to 0.65 to 0.83 for two-sensor fusion. Notably, our proposed system demonstrates overall superior performance with accuracy ranging from 0.72 to 0.85 across all three sensors. While our system is capable of detecting most normal and intruded traffic conditions accurately in our simulation, it should be noted that the dynamic nature of traffic conditions can result in false positives and false negatives. Table II demonstrates that none of the evidence pieces achieves

superior performance in terms of all metrics, as there may be certain situations where our system may not accurately detect normal traffic conditions.

TABLE II
PERFORMANCE

Fusion	Scenario	Accuracy	Precision	Recall	F1-Score
None	1	0.74	0.87	0.75	0.80
	2	0.63	0.80	0.63	0.71
	3	0.76	0.87	0.77	0.82
	4	0.60	0.79	0.60	0.68
	5	0.69	0.85	0.69	0.76
	6	0.59	0.76	0.60	0.67
Two	1	0.83	0.92	0.83	0.87
	2	0.68	0.85	0.67	0.75
	3	0.83	0.91	0.84	0.88
	4	0.72	0.89	0.70	0.78
	5	0.72	0.83	0.76	0.79
	6	0.65	0.85	0.62	0.72
Three	1	0.84	0.92	0.84	0.88
	2	0.72	0.87	0.71	0.78
	3	0.83	0.95	0.80	0.87
	4	0.74	0.85	0.77	0.81
	5	0.85	0.95	0.83	0.88
	6	0.73	0.89	0.70	0.78

IV. CONCLUSION

Our proposed anomaly detection system for ITS relies on real-time and historical observations of traffic parameters such as traffic flow, average vehicle speed, and phase time. We created simulation scenarios on the SUMO platform with real road networks in Melbourne CBD and actual data from transportation authorities. Due to the dynamic characteristics of traffic data, there are lots of outliers and noise in the data. We used Kalman filer, Dempter-Shafer decision theory, and Shannon entropy for information fusion and handling uncertainty. We assessed our system's ability to detect traffic signal intrusion using standard performance metrics, including accuracy, sensitivity, specificity, and F1-score. The accurate detection of both normal and intruded traffic conditions is critical for effective traffic management and road safety. Our proposed model presents a promising solution for achieving this goal by leveraging data from multiple sensors using information fusion to provide a more comprehensive understanding of traffic conditions. While our results indicate overall superior performance for our proposed system, there are certain limitations that should be taken into consideration. For instance, our simulations may not fully capture the complexity of real-world traffic conditions, which may impact the accuracy of our results. Additionally, our study only considers a limited number of performance metrics, and further research is needed to explore the effectiveness of our model from other perspectives, such as computational efficiency and scalability.

REFERENCES

[1] S. Tammishetty, T. Ragunathan, S. K. Battula, B. Varsha Rani, P. RaviBabu, R. Nagireddy, V. Jorika, and V. Maheshwar Reddy, "Iot-based traffic signal control technique for helping emergency vehicles," in *Proceedings of the First International Conference on Computational Intelligence and Informatics: ICCII 2016*. Springer, 2016, pp. 433–440.

[2] K. A. Perrine, M. W. Levin, C. N. Yahia, M. Duell, and S. D. Boyles, "Implications of traffic signal cybersecurity on potential deliberate traffic disruptions," *Transportation research part A: policy and practice*, vol. 120, pp. 58–70, 2019.

[3] G. Turner, G. Chen, and Y. Zhang, "A visual analytics approach for anomaly detection from a novel traffic light data," *Electronic Imaging*, vol. 2021, no. 1, pp. 330–1, 2021.

[4] Y. Xiang, T. Chen, Y. Li, Y. Tian, W. Niu, E. Tong, J. Liu, B. Jia, Y. Wu, and X. Huang, "Predicting congestion attack of variable spoofing frequency for reliable traffic signal system," in *Security and Privacy in New Computing Environments: 4th EAI International Conference, SPNCE 2021, Virtual Event, December 10-11, 2021, Proceedings*. Springer, 2022, pp. 219–237.

[5] A. Chowdhury, G. Karmakar, J. Kamruzzaman, and T. Saha, "Detecting intrusion in the traffic signals of an intelligent traffic system," in *International Conference on Information and Communications Security*. Springer, 2018, pp. 696–707.

[6] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2014.

[7] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, Y. Xiong, and X. Cui, "Attacks and countermeasures in the internet of vehicles," *Annals of Telecommunications*, vol. 72, no. 5-6, pp. 283–295, 2017.

[8] F. Han, L. Lin, and S. Li, "Invulnerability analysis in intelligent transportation system," *International Journal of High Performance Systems Architecture*, vol. 7, no. 4, pp. 197–203, 2017.

[9] R. Kolandaisamy, R. Md Noor, I. Ahmedy, I. Ahmad, M. Reza Z'aba, M. Imran, and M. Alnuem, "A multivariant stream analysis approach to detect and mitigate ddos attacks in vehicular ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[10] N. Huq, R. Vosseler, and M. Swimmer, "Cyberattacks against intelligent transportation systems," *TrendLabs Research Paper*, 2017.

[11] H. Alnabulsi and R. Islam, "Protecting code injection attacks in intelligent transportation system," in *2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*. IEEE, 2019, pp. 799–806.

[12] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, "Attacks on self-driving cars and their countermeasures: A survey," *IEEE Access*, vol. 8, pp. 207 308–207 342, 2020.

[13] G.-h. Han, X.-r. Chen, Y. Yu, and Y.-q. Li, "A study of microscopic traffic simulation based on sumo platform," *computer engineering and science*, vol. 34, no. 7, pp. 195–198, 2012.

[14] VicRoads, "Vicroads traffic data," https://www.data.vic.gov.au/data/dataset/traffic_signal_strategic_monitor_detector_data, 2019, (Last accessed on: 20/02/2023).

[15] Department of Transport, "Department of transport open data hub," 2020. [Online]. Available: https://vicroadsopendata-vicroadsmaps.opendata.arcgis.com/

[16] S.-L. Sun and Z.-L. Deng, "Multi-sensor optimal information fusion kalman filter," *Automatica*, vol. 40, no. 6, pp. 1017–1023, 2004.

[17] A. Chowdhury, G. Karmakar, J. Kamruzzaman, and S. Islam, "Trustworthiness of self-driving vehicles for intelligent transportation systems in industry applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 961–970, 2020.

[18] Y. Wu, F. Meng, G. Wang, and P. Yi, "A dempster-shafer theory based traffic information trust model in vehicular ad hoc networks," in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*. IEEE, 2015, Conference Proceedings, pp. 1–7.

[19] A. Rényi, "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, 1961, pp. 547–561.