Available online at www.sciencedirect.com
SCIENCE DIRECT®

ELSEVIER

Transportation Research Part C 14 (2006) 68–80

TRANSPORTATION RESEARCH PART C

www.elsevier.com/locate/trc

Towards universal freeway incident detection algorithms

Kun Zhang *, Michael A.P. Taylor [1]

Transport Systems Centre, University of South Australia, Adelaide SA 5001, Australia

Received 28 October 2004; received in revised form 14 March 2006; accepted 25 May 2006

Abstract

This paper reports the intensive test of the new transport systems centre (TSC) algorithm applied to incident detection on freeways. The TSC algorithm is designed to fulfil the universality expectations of automated incident detection. The algorithm consists of two modules: data processing module and incident detection module. The data processing module is designed to handle specific features of different sites. The Bayesian network based incident detection module is used to store and manage general expert traffic knowledge, and to perform coherent reasoning to detect incidents. The TSC algorithm is tested using 100 field incident data sets obtained from Tullamarine Freeway and South Eastern Freeway in Melbourne, Australia. The performance of the algorithm demonstrates its competitiveness with the best performing neural network algorithm which was developed and tested using the same incident data sets in an early research. Most importantly, both the detection rate and false alarm rate of the TSC algorithm are not sensitive to the incident decision threshold, which greatly improves the stability of incident detection. In addition, a very consistent algorithm performance is achieved when the TSC algorithm is transferred from Southern Expressway of Adelaide to both Tullamarine Freeway and South Eastern Freeway of Melbourne. No substantial algorithm retraining is required. A significant step towards algorithm universality is possible from this research.

Keywords: Automated incident detection; Bayesian networks; Advanced traffic management system; Algorithm transferability

1. Introduction

Effective freeway incident detection and management are well-recognized key components of any potentially successful advanced traffic management system. The implementation of traditional rule-based automated incident detection (AID) algorithms were hampered by limited performance reliability, substantial implementation needs, and strong data requirements (Chassiakos and Stephanedes, 1993). More advanced approaches, such as neural networks (Dia and Rose, 1997; Cheu and Ritchie, 1995), filtering techniques (Chassiakos and Stephanedes, 1993), and catastrophe theory (Hall et al., 1993; Gall and Hall, 1990; Persaud

* Corresponding author. Tel.: +61 8 8302 1990; fax: +61 8 8302 1880.
E-mail addresses: kun.zhang@unisa.edu.au (K. Zhang), map.taylor@unisa.edu.au (M.A.P. Taylor).
[1] Tel.: +61 8 8302 1861; fax: +61 8 8302 1880.

0968-090X/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.trc.2006.05.004

and Hall, 1989), were then used to improve AID algorithm performance. The big challenge to these algorithms was to meet the universality requirements for which the advanced traffic management systems called. Hence, it is usually difficult to transfer a well-performed such algorithm from site to site. Quite recently, an important step towards algorithm universality was made by Abdulhai and Ritchie (1999), and a unified list of universality requirements was suggested in their work. To enhance freeway incident detection and to fulfil the universality expectations for AID algorithms, the Bayesian network approach was used to develop the transport systems centre (TSC) algorithm (Zhang and Taylor, 2004; Zhang and Taylor, 2002). The purpose of this paper is to report the testing results of the TSC algorithm using a large set of field incident data. The TSC algorithm demonstrates a very stable performance and strong transferability.

This paper is organized in five sections. The first section introduces the attributes possessed by the potentially universal freeway incident detection algorithms. Then the Bayesian network based TSC algorithm is described in Section 2. In Section 3, the TSC algorithm is tested using a large number of field incident data sets, and its performance is evaluated. The TSC algorithm transferability and competitiveness is discussed in Section 4. In Section 5, the conclusions are drawn and the future research directions are recommended.

2. Universality requirements

For a freeway incident detection algorithm to be universal, it needs to possess a set of suitable capabilities and attributes. One possible unified list of universality requirements was suggested by Abdulhai and Ritchie (1999). These attributes may be categorized into the following groups:

Performance

- High detection rate.
- Low false alarm rate.
- Short mean time to detect.

Transferability

- Transferable detection logic. The logic or theory on which the algorithm is built should not be constrained spatially, temporally or in any other manner that would limit transferability to other locations.
- Transferable training and calibration parameters. An algorithm trained with data from one site should be usable in other new environments with as little performance deterioration as possible.

Decision support

- Accounting for prior probabilities of incidents. The algorithm should incorporate into an incident alarm decision the predicted prior probability of occurrence of an incident.
- Capable of producing the posterior probability of an incident. The algorithm should be capable of producing a probabilistic estimate of the certainty associated with an incident alarm.
- Capturing incident duration.
- Estimated incident severity.

Implementation

- Reasonable algorithm implementation requirements.
- Fast training and calibration.
- Minimal initial training data requirements. High quality, detailed real incident data are not only very sparse but also very difficult to obtain. A successful algorithm should be capable of being up and running using minimal incident data, and then improved with time in service, as more data become available.

Flexibility

- Flexibility in working with different surveillance system designs and technologies. Successful field implementation of the algorithm should not be limited to specialized surveillance system designs, including sensor technology, spacing and placement.

The presence or absence of these attributes will be used to evaluate our proposed TSC algorithm.

3. The Bayesian network based TSC algorithm

To deal with the *performance issue* concerning the existing incident detection algorithms, the proposed TSC algorithm must be capable of (1) effectively storing and managing expert traffic knowledge, and (2) performing coherent and efficient evidential reasoning. In this research, Bayesian networks are chosen as the key technique to develop the TSC algorithm. A Bayesian network is a causal probabilistic network. It builds an environment in which traffic parameters and events act, and simulates the mechanism of the interaction among traffic parameters and events. The ability of Bayesian networks to coordinate bi-directional inferences filled a void in expert systems technology of the early 1980s. Bayesian networks have emerged as a general representation scheme for uncertain knowledge (Pearl, 1988).

3.1. Bayesian network

A Bayesian network consists of a set of variables and a set of directed edges between variables. Each variable has a finite set of mutually exclusive states. The directed edges represent the cause–effect relationship between variables. The variables together with the directed edges form a directed acyclic graph (Jensen, 1996). For each variable A with parents $B_1, \ldots, B_n$, a conditional probability table $P(A|B_1, \ldots, B_n)$ is attached to quantify their causal relationships. A typical Bayesian network is shown in Fig. 1(a).

Let U be a universe of variables. Assume that we have easy access to $P(U)$, the joint probability table, the probability distribution $P(A)$ for any variable A in U is easy to calculate through marginalization

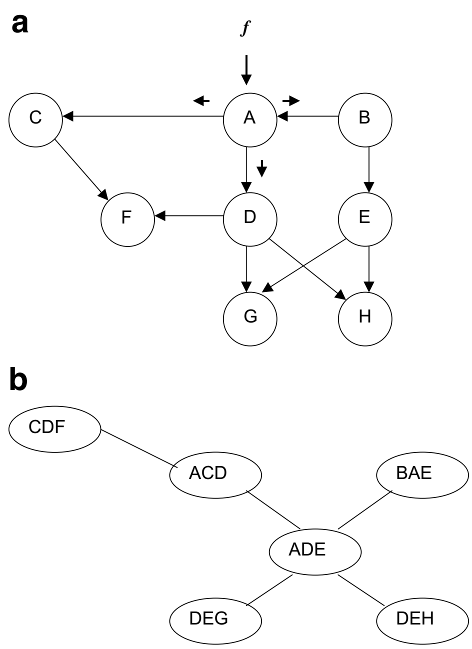

Fig. 1. A Bayesian network (a) and the corresponding junction tree (b).

$$P(A) = \sum_{U \setminus \{A\}} P(U) \tag{1}$$

A Bayesian network over U is a more compact representation of $P(U)$: a way of storing information from which $P(U)$ can be calculated if needed. Let BN be a Bayesian network over $U = \{A_1, \ldots, A_n\}$. If the conditional independencies in the BN hold for U, then $P(U)$ is the product of all conditional probabilities specified in BN (Jensen, 1996)

$$P(U) = \prod_i P(A_i | p(A_i)) \tag{2}$$

where $p(A_i)$ is the parent set of A_i, and $P(A_i|p(A_i))$ is our prior knowledge about A_i in U.

Let A be a variable in U with n states. A finding f on A is a n-dimensional table of zeros and ones ($\underline{f}$). The way that f is entered in the BN can be interpreted as a multiplication of $P(A)$ with the table $\underline{f}$ resulting $P(A, e)$. If new multiple findings $e = \{f_1, \ldots, f_m\}$ are provided, then the findings can be entered into the BN

$$P(U, e) = P(U) \cdot \underline{f_1} \cdots \underline{f_m} \tag{3}$$

and the probability updating in BN can be performed as follows

$$P(U|e) = \frac{P(U, e)}{P(e)} = \frac{P(U, e)}{\sum_U P(U, e)} \tag{4}$$

By using Eq. (1) and the updated probability distribution $P(U|e)$, the posterior probability distribution of any variable A in U, $P(A|e)$, can be calculated. All the probabilistic queries (i.e. finding the most likely explanation for the traffic information received) can be answered coherently using this type of two-way evidential reasoning.

To facilitate probability updating in a Bayesian network, the independence properties of the network are analysed to establish a set of variables (clusters) and to construct a tree over the clusters. Fig. 1(b) is the corresponding junction tree of the Bayesian network which is shown in Fig. 1(a). For each pair V, W of nodes in the junction tree, all nodes on the path between V and W contains their intersection $V \cap W$.

3.2. The TSC algorithm

Each traffic site has its own specific geometric features, travel demands and traffic management schemes. To address algorithm *transferability issue*, modular algorithm architecture is essential, which may include a special module to deal with the specific features of different traffic sites. Meanwhile, the algorithm transferability should focus on the general knowledge base construction and the capability of coherent reasoning for incident detection. The TSC algorithm consists of two modules: (1) data processing module and (2) incident detection module. The data processing module is designed to handle the site specific traffic measurements and normalize them into standard traffic cases. Each traffic case contains the states (instead of absolute values) of selected traffic parameters at each detection interval. The incident detection module employs a Bayesian network to perform universal evidential reasoning to detect incidents. The findings used in the Bayesian network for probability updating is the traffic case information. An incident alarm is issued when the estimated incident probability exceeds the predefined decision threshold. The focus of this module is on expert traffic knowledge storage, updating and coherent reasoning.

3.2.1. Data processing

The schematic diagram (Fig. 2) shows the procedure of traffic data processing. The first part of data processing, we call it *Pre-process*, has two basic functions: eliminating the random fluctuation from raw traffic measurements and identifying a possible compression wave.

Inspired by the good performance of the DELOS algorithms (Chassiakos and Stephanedes, 1993), smoothed traffic data instead of raw traffic measurements are used to generate traffic cases. The raw traffic measurements are smoothed over a time window (n, k), which incorporates the present $(t + k)$ and the past $(t - n)$ time intervals. The moving average is selected

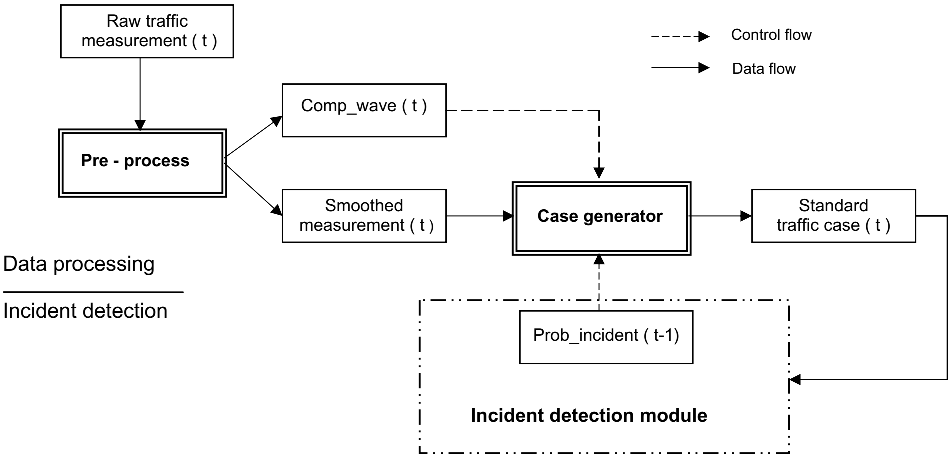

Fig. 2. Data processing and traffic case generation.

$$S_i(t) = \frac{1}{L}\sum_{a=0}^{L-1} M_i(t-a) \tag{5}$$

where $S_i\,(t)$ is the smoothed traffic measurement at time t and detector station i, $M_i\,(t)$ is the traffic measurement at time t and detector station i, and $L = k + 1$, k measurement value after t, or $L = n + 1$, n measurement value before t.

In this study we use the traffic measurements obtained at the previous two intervals ($n = 2$) for smoothing.

A compression wave on freeway is better represented by the high occupancy values experienced by the downstream detector station (Payne and Tignor, 1978). In the data processing module, both the downstream occupancy and the relative temporal difference of the downstream occupancy are compared against predefined thresholds. A binary number of 1|0 is then generated for each time interval with 1 representing a possible compression wave. We use the variable ***Comp_wave*** (***t***) to store this binary sequence. When a compression wave is detected at several consecutive detection intervals, incident detection on this section of the freeway will be suspended for certain time (e.g. 5 min) to allow the wave to pass through.

The second part of data processing can be treated as a traffic *case generator*. As shown in Fig. 2, smoothed traffic measurements (link average) are used as the source to generate traffic case. The control variable ***Prob_incident*** (***t*** − ***1***), which is the incident probability estimate generated by the incident detection module at $t - 1$, determines which traffic parameters should be selected for the current traffic case generation. Meanwhile, the other control variable ***Comp_wave*** (***t***) determines whether the incident detection should be suspended or not. Only the selected traffic parameters are compared against the predefined thresholds to ascertain their states (e.g. volume is high, medium, or low). These selected parameters with their states at each detection interval are then used by the incident detection module as new findings to detect incidents. The idea of using the states instead of absolute values of traffic measurements for incident detection is that the knowledge base for incident detection can be managed and used independently from traffic data processing which contains distinct site specific features. Therefore, the incident detection process can be performed in a universal way.

3.2.2. Incident detection

3.2.2.1. The Bayesian network for incident detection. The core part of the incident detection module is the Bayesian network shown in Fig. 3. The Bayesian network consists of two traffic events (incident: ***Inc1_1***, congestion: ***Con1_1***) and seven traffic parameters (volumes: ***Vol1_1*** and ***Vol2_1***, occupancies: ***Occ1_1*** and ***Occ2_1***, speeds: ***Spd1_1*** and ***Spd2_1***, and occupancy difference between upstream and downstream: ***D_occ1***). They are all state variables. The pointed links between traffic events and parameters represent their cause–effect relationships. This network continuously looks at the variation of spatial traffic patterns and updates the probability distribution of both incident and congestion through two-way evidential reasoning.

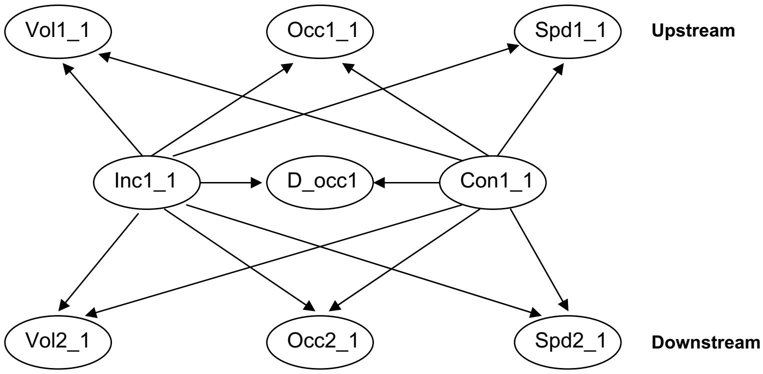

Fig. 3. The Bayesian network for incident detection.

As shown in Fig. 3, the connections between any parent node (***Inc1_1*** or ***Con1_1***) and the rest of the nodes (child nodes) are diverging connections. The states of these two parent nodes are unknown and will be determined by the available states of traffic parameters. These two conditions indicate that all child nodes in the Bayesian network are *d-connected*, which means a finding (current state of a traffic parameter) at any child node can be propagated throughout the entire network. Therefore, each and every piece of traffic information can be made use of to update the incident probability and to estimate the probability distributions of the traffic parameters with unknown states.

Evidential reasoning in the Bayesian network is made efficient enough for real time application by using Hugin propagation (Jensen, 1996). Firstly, the Bayesian network is transformed into a junction tree. Then, a node (e.g. *Rt*) in the junction tree is chosen as a root. Whenever the Hugin propagation takes place, the function *CollectEvidence* (*Rt*) is called first, which is followed by a call of the function *DistributeEvidence* (*Rt*). This two-way message passing scheme guarantees that each finding obtained from any node will be used to update the probability distributions of the entire network. When the calls are completed, the table that contains updated probability distribution of each node is normalized so that it sum to one. The Hugin Development Environment (Hugin, 2003) is used in this research to develop the application programs for incident detection.

Since the different traffic parameters (occupancy, volume and speed) operate in different ways during the transit period from free flow condition to incident-induced congestion condition or vice versa (Persaud and Hall, 1989), it is crucial to select the most reliable and relevant traffic parameters for incident detection under different traffic conditions. This is the reason why the control variable *Prob_incident* $(t-1)$ is introduced into the traffic case generation. In the TSC algorithm, the traffic condition has two states: incident free (*state 0*) and suspect incident (*state 1*), which is determined by the incident probability at the previous interval. *State 1* is divided further into *state 1a* (suspect incident) and *state 1b* (true incident) for incident reporting purpose. Suppose the current state of traffic is *0*, the available states of all traffic parameters will be used to identify the possible incident. When traffic condition shifts from state *0* to state *1* as the result of the incident detection at the previous time interval, only the selected traffic parameters with their states are used for incident decision making. This function is fulfilled by the dynamic control of traffic case generation, which is shown in Fig. 2. Meanwhile, the Bayesian network supports such reasoning using partially collected findings.

The traditional rule-based algorithms detect incidents through two sequential steps: identifying traffic congestion, then, finding out the causes of the congestion (incident induced or not). In case the traffic volume does not greatly exceed the remaining roadway capacity at the time of incident, the first step of congestion identification would take a very long time. Meanwhile, the persistence test performed by the algorithms would post extra delay on incident detection time. In the TSC algorithm, both congestion identification and incident pattern recognition are fulfilled through one step reasoning using the Bayesian network. The states of all selected traffic parameters are considered simultaneously, and the estimated congestion probability at current detection interval is incorporated into incident decision making. It needs to be emphasized that the Bayesian network does not require every node to have a renewed state at each detection interval, and evidential reasoning can be performed using partially collected findings. This flexibility of the Bayesian network approach opens an opportunity for other information (e.g. probe travel time) that cannot supply continuous report at each detection interval to be used (when available) by the TSC algorithm to enhance its performance.

3.2.2.2. Incident report. This procedure is designed to estimate incident probability at each detection interval and issue an incident alarm when its value exceeds the decision threshold. As shown in Eq. (6), both the current Bayesian network outputs $(I(t), C(t))$ and the final estimate of incident probability at the previous two intervals $(\widehat{I}(t-1), \widehat{I}(t-2))$ are used to calculate the current incident probability $\widehat{I}(t)$. The coefficients $(\alpha, \beta i)$ are not fixed, they are determined by $I(t), C(t)$ and $\widehat{I}(t-1)$ at each detection interval.

$$\widehat{I}(t) = \alpha * C(t) + \beta 1 * I(t) + \beta 2 * \widehat{I}(t-1) + \beta 3 * \hat{I}(t-2) \tag{6}$$

where $I(t)$ is updated incident probability at time t, $C(t)$ is updated congestion probability at time t, $\widehat{I}(t)$ is the final estimate of incident probability at time t for incident report, and $\alpha \in [0,1]$, $\beta i \in [0,1]$, $\alpha + \beta 1 + \beta 2 + \beta 3 = 1$.

A typical output of the TSC algorithm is shown in Fig. 4. The incident data set No. 42 from Tullamarine Freeway is used to produce this result. This incident occurred during an inter-peak period, which involved a four-car crash. Each bar in the figure represents the estimated incident probability $(\widehat{I}(t))$ at time interval t. The two arrows mark the incident starting time and termination time respectively. If the decision threshold is set to 60% ($iP = 60\%$, this value may vary according to different objectives of field AID application), the TSC algorithm picks up this incident three minutes after its occurrence time, and the certainty associated with this incident alarm is 74%. The severity of this incident can be directly estimated from the absolute value of the algorithm output. In addition, the incident duration can be estimated from the time-profile of the algorithm output, which is 27 min in this case. The above *decision support* functions are embedded in the TSC algorithm.

3.2.3. Algorithm training

The TSC algorithm training is performed at two different stages: algorithm development (stage 1) and algorithm implementation (stage 2).

Stage 1: The major task of training is to construct a general knowledge base for incident detection. The knowledge base refers to the CPTs of the Bayesian network. The Bayesian network is partitioned into several small clusters of nodes first, which contains parent–child node pairs (e.g. ***Inc1_1***, ***Con1_1*** and ***Vol1_1***). For each cluster of nodes, every piece of knowledge concerning the relationship between certain traffic parameter and events under incident and incident-free conditions is then translated into subjective detection rules. Finally, these rules are quantified and converted into the entries of CPTs that are attached to the nodes of that cluster.

Stage 2: The focus of training is given to the choice of thresholds for traffic parameters (i.e. volume, occupancy and speed), which only involves the data processing module. Thresholds are used to determine the state of each traffic parameter (e.g. volume is high, medium or low). The precision of the threshold settings is not critical compared with the CPTs of the Bayesian network. Hence, traffic operators' experiences on the targeted freeway section are good enough for setting these values.

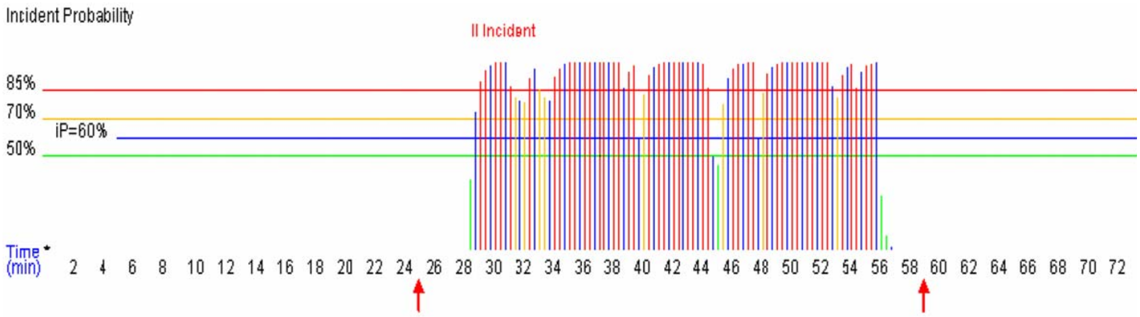

Fig. 4. A typical output of the TSC algorithm.

The Bayesian network is transparent and its CPTs are fully accessible. Any dynamic changes of traffic conditions, which might be caused by transport policy changes, road network upgrading or the implementation of new traffic control strategies, can be effectively dealt with at any stage of the algorithm implementation through updating certain CPT entries of the Bayesian network, especially when the effects or impacts of such changes could be well predicted. This feature can be viewed as subjective algorithm training, and the choice of thresholds for traffic parameters can be treated as subjective algorithm adaptation to the targeted traffic environment. To further enhance the performance of the algorithm, objective Bayesian network adaptation using field incident data (given that quality incident data are available) can be performed. By setting experience tables of each CPT, the extent of knowledge base modification is well controlled during each Bayesian network adaptation.

The knowledge base used by the TSC algorithm are general expert knowledge rather than a large collection of diverse incident patterns. Meanwhile, the successful incident detection does not largely rely on the precisely calibrated thresholds but on the coherent reasoning performed in the Bayesian network. Therefore, the substantial *algorithm implementation* needs in terms of skills required for implementation, high quality incident data and training time are dramatically reduced.

4. TSC algorithm performance

4.1. Incident data

Incident data used for the TSC algorithm testing were collected on Tullamarine Freeway and South Eastern Freeway (SEF) of Melbourne in an early research (Dia and Rose, 1997). These data were used in that research to develop and test the best performing neural network based MLF algorithm. The Tullamarine data consist of 85 usable lane-blocking incidents, and 60 of them form Dia's original training data set. The SEF data contain 15 incidents. These 15 incidents plus the 25 incidents from the Tullamarine data form the original validation data set. The characteristics of the full set of 100 incidents are listed in Table 1.

4.2. Performance measures

The direct performance measures used to evaluate the TSC algorithm include the detection rate (DR), the false alarm rate (FAR) and the mean time to detect (MTTD). The DR is defined as

$$\mathrm{DR} = \frac{\text{number of detected incidents}}{\text{total number of incidents in the data set}} \times 100\% \tag{7}$$

The FAR is defined as

$$\mathrm{FAR} = \frac{\text{number of false alarms}}{\text{total number of applications of the algorithm}} \times 100\% \tag{8}$$

The definition of the FAR can be easily translated into the actual number of false alarms per hour per km, which is consistent with the earlier work (Chassiakos and Stephanedes, 1993; Hall et al., 1993; Payne and Tignor, 1978).

Table 1
Tullamarine Freeway and South Eastern Freeway incident characteristics

Study site	Number of incidents	Incident characteristics							
		Time of occurrence		Severity			Duration		
		Peak	Off-peak	1 lane affected	2 lanes affected	3 lanes affected	<30 min	30–60 min	>60 min
Tullamarine	85	24	61	3	64	18	21	30	34
SEF	15	2	13	1	14	0	3	4	8
Total	100	26	74	4	78	18	24	34	42

The MTTD is defined as

$$\mathrm{MTTD} = \frac{1}{n}\sum_{i=1}^{n}(t_{\text{detect}} - t_{\text{on-set}}) \tag{9}$$

where t_{detect} is the time interval that an incident is detected by the algorithm, $t_{\text{on-set}}$ is the time interval that an incident actually occurs, and n is the number of correctly detected incidents. Both the DR and FAR measure the effectiveness of an algorithm, and the MTTD reflects the efficiency of the algorithm.

Abdulhai and Ritchie (1999) elicited operational constraints and criteria from freeway operation personnel in order to assist in evaluating AID algorithm performance. Traffic management centre personnel put more emphasis on the high DR, which is consistent with the prime objective of incident detection.

4.3. TSC algorithm performance

The TSC algorithm was originally developed on Southern Expressway (SX) in Adelaide using simulated incident data (Zhang and Taylor, 2004). The Southern Expressway is a novel one-way reversible direction expressway. Under the prevailing tidal flow nature, the SX is designed to operate northbound in the morning and southbound in the evening to relieve peak flow traffic on an alternative arterial route (Main South Road). To compare the congestion parameters and emissions of the two routes, and to investigate the impact of the advanced traffic management implementation on the SX in the early research (Woolley et al., 2001), the SX micro-simulation model was constructed using the Paramics software package and was validated using field operational data. We use the SX model to generate incident data for the TSC algorithm development.

To adapt the TSC algorithm to Tullamarine Freeway, 10 incidents from the Tullamarine data are chosen to re-train the algorithm in this research. The selected incidents belong to north-bound traffic (from Melbourne CBD) between detector stations S3 and S6 (shown in Fig. 5). Four of them occur during peak periods. Inci-

Fig. 5. Schematic of the sections of Tullamarine Freeway used in the study, showing detector stations S3, S4, S5 and S6.

Table 2
The TSC algorithm performance

Data set	Decision threshold, *iP* (%)	Incident detection performance			
		Detection rate		False alarm rate (%)	Mean time to detect (s)
		No.	%		
100 incidents					
Tullamarine (85) SEF (15)	55	92/100	92	0.143	158
	60	92/100	92	0.103	165
	70	92/100	92	0.087	175

dent duration varies from 14 min to 113 min. We examine five of these incidents to set up the initial thresholds for traffic parameters. The other five incidents are used to test the thresholds and fine-tune the data processing module. As an alternative, this task could be fulfilled by an experienced traffic operator from site without using the field incident data.

As discussed in Section 3.2, the TSC algorithm has a modular architecture. The incident detection module only contains general expert traffic knowledge about incidents which could be shared with other freeways. We directly transfer the original incident detection module (including the Bayesian network and its CPTs) of the algorithm from SX to Tullamarine Freeway without any retraining. The resultant TSC algorithm, the original incident detection module plus the updated data processing module, is then tested using both the Tullamarine and SEF incident data. No further retraining is performed when the algorithm is transferred from Tullamarine Freeway to SEF. The algorithm testing results are shown in Table 2.

A very good DR of 92% is achieved. Most excitingly, the DR is not sensitive to the decision threshold (*iP*). When $iP > 55\%$, a stable DR is obtained. This result could be explained by (1) the knowledge base of the TSC algorithm contains general expert traffic knowledge rather than specific incident patterns, and (2) the evidential reasoning performed by the Bayesian network is similar to an experienced operator's reasoning process but more consistent and coherent in terms of the way by which incident probability is estimated.

The FAR produced by the algorithm under three different *iP* values is reasonably low. The FAR is slightly affected by the decision threshold, decreasing with increasing value of *iP*. The above results indicate that the strong positive correlation between the DR and FAR which is currently experienced by existing AID algorithms is greatly mitigated. The TSC algorithm improves the stability of automated incident detection.

Given the *iP* is set to 60%, the TSC algorithm detects 68% of incidents in less than 4 min, 58% of incidents in less than 3 min, and 39% of incidents in less than 2 min. The overall MTTD is less than 3 min. It is thus reasonable for field application. Note that the estimated incident start time is used to calculate the MTTD in this research instead of using the time that appears in operator's log. As noted in Dia and Rose (1997), the inspection of the log times corresponding to the validation data set (40 incidents) revealed that two incidents were detected by the operators before their impact on traffic was confirmed from the detector data. Only 18.4% (seven incidents) of the remaining 38 incidents were detected by the operators within 3 min of their occurrence. The average time taken by the operators to detect the 38 incidents was 6.9 min after their estimated occurrence times. The MTTD of the TSC algorithm is 2.75 min. This suggests that the TSC algorithm has the potential to provide more than 50% improvement in efficiency compared to the average time taken by the operators to detect incidents.

In addition, the duration of a detected incident can be estimated directly from the time-profile of the TSC algorithm outputs. This study reveals that incident probability is generally below 25% during incident-free periods and jumps up to 60–80% during incident periods.

5. Algorithm transferability and competitiveness

5.1. The TSC algorithm transferability

The TSC algorithm is tested on three different freeway environments including Southern Expressway of Adelaide, Tullamarine Freeway and South Eastern Freeway of Melbourne. The Bayesian network and its

Table 3
The TSC algorithm transferability

Test site	Number of incidents	Incident detection performance			
		Detection rate		False alarm rate (%)	Mean time to detect (s)
		No.	%		
SX ($iP = 85\%$, simulated data)	36	36/36	100	0.07	113
Tullamarine ($iP = 60\%$)	85	77/85	90.6	0.114	181
SEF ($iP = 60\%$)	15	15/15	100	0.022	95

CPTs of the algorithm are the same during all three tests. In addition, an identical data processing module is used for the tests on both Tullamarine Freeway and South Eastern Freeway. The detailed testing results are presented in Table 3.

The TSC algorithm performs consistently in three different freeway environments. It performs even better on South Eastern Freeway when it is transferred from Tullamarine Freeway without any retraining. We think the excellent performance of the TSC algorithm stems largely from its modular architecture which makes the incident detection module universal and independent from the data processing module. Therefore, the general knowledge base of the algorithm can be fully transferred from site to site. The above results demonstrate that algorithm transferability is achievable under the TSC framework.

5.2. Performance comparison

5.2.1. The performance comparison between the TSC and MLF algorithm

The performance comparison is first made between the TSC algorithm and the MLF algorithm which was developed and tested using the Tullamarine and SEF incident data (Dia and Rose, 1997). The original validation data set is used here to test the both algorithms. The validation data set has not been used when we adapt the TSC algorithm to Tullamarine Freeway. The testing results are shown in Table 4.

The DR produced by the TSC algorithm is 92.5%. It is superior to the DR produced by the MLF algorithm (82.5%).

Both algorithms have the low FAR. Note that the FAR of the TSC algorithm presented here is 0.057%, which is twice as low as the value (0.103%) presented in Table 2. When the algorithm is tested using the complete set of 100 incidents (training set: 60 incidents, validation set: 40 incidents), a total number of 39 false alarms is generated. Among these the 24 false alarms are caused by three specific incidents (Incident No. 2: three-car accident, off-peak, duration 50 min; Incident No. 28: two-car accident, peak, duration 22 min; and Incident No. 59: mower rolled down slope, off-peak, duration 110 min). All these three incidents belong to the original training data set. This is the reason why the better FAR is obtained when the validation data set is applied.

The TSC algorithm detects incidents 129 s quicker than the MLF algorithm when the SEF incident data are used. On contrast, the MTTD of the TSC algorithm obtained from Tullamarine Freeway is 21 s longer than

Table 4
Performance comparison: TSC vs MLF

Algorithm	Data set	Number of incidents	Incident detection performance			
			Detection rate		False alarm rate (%)	Mean time to detect (s)
			No.	%		
TSC ($iP = 60\%$)	Tullamarine	25	22/25	88	0.074	209
	SEF	15	15/15	100	0.022	95
	Total	40	37/40	92.5	0.057	163
MLF (DT = 0.64)	Tullamarine	25	19/25	76	0.09	188
	SEF	15	14/15	93.3	0.00	224
	Total	40	33/40	82.5	0.065	203

Table 5
Performance comparison: TSC vs California, McMaster and DELOS

Algorithm	Number of incidents	Incident detection performance		
		Detection rate (%)	False alarm rate (%)	Mean time to detect (s)
TSC ($iP = 60\%$)	100	92	0.103	165
California 7	150	59	0.134	N/A
California 8	150	61	0.177	N/A
McMaster	17 (off-line)	88.2	0.0012	132
	28 (on-line)	68	0.0008	126
DELOS 3.3	27	78	0.174	66
DELOS 3.1	27	78	0.257	66

that of the MLF algorithm. The overall MTTD produced by TSC algorithm is 40 s shorter than that of the MLF algorithm. As mentioned before, all incidents that belong to the original training data set occurred on Tullamarine Freeway. Hence the shorter MTTD is obtained when the MLF algorithm is tested using the Tullamarine data. These findings again demonstrate the better transferability of the TSC algorithm.

5.2.2. Performance comparison with the California, McMaster and DELOS algorithms

It is difficult to directly compare the performance of the TSC algorithm with the widely used algorithms (i.e. California, McMaster and DELOS) using the Tullamarine and SEF incident data. Certainly, it would be time consuming in order to calibrate these algorithms properly. But more importantly, the best performance of these algorithms was usually found at the original site where they were developed (Abdulhai and Ritchie, 1999; Chassiakos and Stephanedes, 1993). Thus, we use the best results of these algorithms, which were published in the literature (Chassiakos and Stephanedes, 1993; Hall et al., 1993; Payne and Tignor, 1978), to make performance comparison. Table 5 shows the performance differences among these algorithms.

Table 5 suggests that the TSC algorithm performs better than the other algorithms in terms of the DR.

The FAR of the TSC algorithm remains the same level as that of the California and DELOS algorithms. The FAR of the McMaster algorithm is not comparable to rest of the algorithms, because the traffic data used to calculate the FAR of the McMaster algorithm cover 16 h of operation per day (from 6:00 am to 10:00 pm). These data are thus not incident specific traffic data which normally cover the incident periods and the reasonable short periods immediately before and after the incident.

The MTTD used by the McMaster and DELOS algorithm is defined as the difference between the time when an incident is detected by the algorithm and the time when the operator identifies the incident. This definition is different from the one we use to evaluate the TSC algorithm. Operators need some time to detect incidents after they occur. In the Melbourne case, the average time taken by the operators to detect the 38 incidents (which belong to the validation data set) is 6.9 min after their estimated occurrence times (Dia and Rose, 1997). If the operator's detection time is taken into account, the TSC algorithm will detect incidents much faster.

6. Conclusion

The aim of this research is to evaluate the performance of the TSC algorithm using field incident data. A total of 100 lane-blocking incidents observed on the Tullamarine Freeway and South Eastern Freeway in Melbourne are used. The testing results demonstrate the competitiveness of the TSC algorithm with the best performing neural network algorithm MLF which was developed using the same incident data. The testing results also reveal that both the DR and FAR produced by the TSC algorithm are not sensitive to incident decision threshold. The positive correlation between the DR and FAR is greatly mitigated. This unique feature improves the stability of automated incident detection.

The TSC algorithm is significantly easy to train in a subjective way without employing a large set of field incident data. Operators' experiences about a specific freeway environment are good enough to adapt the TSC algorithm to the site. This capability stems largely from the modular architecture of the algorithm and its general knowledge base for incident detection, which is clearly demonstrated in both algorithm performance test and transferability test. An important step towards algorithm universality has therefore been possible in this research.

In this research, only lane-blocking incidents are used to test the performance of the TSC algorithm. Our future research will focus on the extensive testing of the algorithm using different types of incidents which are collected from other freeway environments. Meanwhile, to explore the data fusion potential of the Bayesian network by incorporating other traffic information (e.g. probe travel time) into the TSC algorithm will be the next step of algorithm performance enhancement.

Acknowledgements

The authors would like to thank Hussein Dia and VicRoads for kindly providing the Tullamarine Freeway and South Eastern Freeway incident database and MineLab Electronics Pty Ltd for their financial support for this research project.

References

Abdulhai, B., Ritchie, S.G., 1999. Enhancing the universality and transferability of freeway incident detection using a Bayesian-based neural network. Transportation Research 7C, 261–280.

Chassiakos, A.P., Stephanedes, Y.J., 1993. Smoothing algorithms for incident detection. Transportation Research Record 1394, 9–16.

Cheu, R.L., Ritchie, S.G., 1995. Automated detection of lane blocking freeway incidents using artificial neural networks. Transportation Research 3C, 371–388.

Dia, H., Rose, G., 1997. Development and evaluation of neural network freeway incident detection models using field data. Transportation Research 5C, 313–331.

Gall, A.I., Hall, F.L., 1990. Distinguishing between incident congestion and recurrent congestion: a proposed logic. Transportation Research Record 1232, 1–8.

Hall, F.L., Shi, Y., Atala, G., 1993. On-line testing of the McMaster incident detection algorithm under recurrent congestion. Transportation Research Record 1394, 1–7.

Hugin 2003. www.hugin.com.

Jensen, F.V., 1996. An Introduction to Bayesian Networks. Springer-Verlag, London.

Payne, H.J., Tignor, S.C., 1978. Freeway incident-detection algorithms based on decision tree with states. Transportation Research Record 682, 30–37.

Pearl, J., 1988. Probabilistic Reasoning in Intelligent Systems. Morgan Kaufmann, San Mateo, CA.

Persaud, B., Hall, F.L., 1989. Catastrophe theory and pattern in 30 second freeway traffic data – implication for incident detection. Transportation Research 23A, 103–113.

Woolley, J.E., Taylor, M.A.P., Zito, R., 2001. Modelling of the Southern Expressway using Paramics mirosimulation software. Journal of the Eastern Asia Society for Transportation Studies 4 (4), 279–295.

Zhang, K., Taylor, M.A.P., 2002. Automated incident detection – Bayesian networks approach. In: Proceedings of the 24th Conference of Australian Institutes of Transport Research, Sydney.

Zhang, K., Taylor, M.A.P., 2004. Incident detection on freeways: a Bayesian network approach. In: Proceedings of the 27th Australasian Transport Research Forum, Adelaide.