1. Report No. FHWA/TX-93/1232-20	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle AN EVALUATION OF EXISTING INCIDENT DETECTION ALGORITHMS		5. Report Date November 1993
		6. Performing Organization Code
7. Author(s) Kevin N. Balke		8. Performing Organization Report No. Research Report 1232-20
9. Performing Organization Name and Address Texas Transportation Institute The Texas A&M University System College Station, TX		10. Work Unit No. (TRAIS)
		11. Contract or Grant No. Study no. 0-1232
12. Sponsoring Agency and Address Texas Department of Transportation: Office of Research and Technology Transfer P.O. Box 5051 Austin, TX 78763		13. Type of Report and Period Covered Interim: September 1990-November 1993
		14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

Several algorithms have been proposed for automatically detecting incidents using freeway detector data. Some are comparative algorithms that compare measured traffic conditions to preestablished thresholds. Other use statistical procedures to detect significant changes in traffic patterns over time. Still others use complex theoretical models to predict future traffic conditions using current traffic measures and historical trends. The structure of an algorithms affects its performance in terms of detection rate, false alarm rate, and detection time.

No single algorithm appears to be superior in terms of its reported performance, data requirements, ease of implementation, ease of calibration, and operational experience. Using the results from both off-line and on-line evaluations reported in the literature, most algorithms appear to achieve the same level of detection and produce similar false alarm rates, when properly calibrated. Detection times for most algorithms are also similar.

Given the results of the evaluation and the sites visits, it is recommended that TxDOT consider the following incident detection algorithms in the initial implementation of their freeway surveillance and control centers:

- Modified California Algorithm #7
- Modified California Algorithm #8
- McMaster Algorithm

17. Key Words Incident Detection Algorithms, Incidents, Traffic Management	18. Distribution Statement No Restrictions. This document is available to the public through the NTIS: National Technical Information Service 5285 Port Royal Road Springfield, VA 22161		
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 100	22. Price

Form DOT F 1700.7 (8-72)   Reproduction of form and completed page is authorized

AN EVALUATION OF EXISTING INCIDENT DETECTION ALGORITHMS

by

Kevin N. Balke, P.E.
Assistant Research Engineer
Texas Transportation Institute

Research Report 1232-20
Research Study 0-1232
Study Title: Urban Highway Operations Research
and Implementation Program

November 1993

TEXAS TRANSPORTATION INSTITUTE
The Texas A&M University System
College Station, TX 77843-3135

IMPLEMENTATION STATEMENT

This report provides recommendations of three candidate incident detection algorithms for consideration by TxDOT for the inclusion in the initial implementation of their freeway surveillance and control centers. The report provides information on the use and effectiveness of existing incident detection algorithms. It also contains information on the data required to operate and calibrate the recommended incident detection algorithms.

DISCLAIMER

The contents of this report reflect the views of the author who is responsible for the facts and the accuracy of the data presented herein. The contents do not necessarily reflect the official view or policies of the Texas Department of Transportation (TxDOT) or the Federal Highway Administration (FHWA). This report does not constitute a standard, specification, or regulation nor is it intended for construction, bidding, or permit purposes. The engineer in charge of the project was Mr. Kevin Neil Balke, (P.E.# 66529).

ACKNOWLEDGMENTS

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

LIST OF FIGURES

LIST OF TABLES

SUMMARY

The Texas Department of Transportation (TxDOT) is currently developing the system architecture to support their freeway surveillance and control centers. These centers will be designed to perform many functions including the automatic detection of congestion and capacity-reducing incidents. One remaining issue to be decided in the development phase of these centers is which incident detection algorithm should be used when the centers are first implemented in the various metropolitan areas in Texas. This report provides an evaluation of the existing incident detection algorithms currently presented in the literature, and provides recommendations as to which algorithms should be considered by TxDOT for inclusion in the initial implementation of their freeway surveillance and control centers. This research focuses on existing incident detection algorithms reported in the literature: no new algorithms were developed as part of this research.

Several algorithms have been proposed for automatically detecting incidents using freeway detector data. Some are comparative algorithms that compare measured traffic conditions to preestablished thresholds. Others use statistical procedures to detect significant changes in traffic patterns over time. Still others use complex theoretical models to predict future traffic conditions using current traffic measurements and historical trends. The structure of an algorithm affects its performance in terms of detection rate, false alarm rate, and detection time.

Site visits were also performed at seven operating freeway surveillance and control centers operating in the United States and Canada. The purpose of these site visits was to obtain firsthand knowledge of the type and effectiveness of incident detection algorithms currently being used in many of the operating surveillance and control centers. The site visits revealed that all seven of the control centers are either using or have used a modified version of the California incident detection algorithm at some point. However, only three are still currently using a modified version of the California algorithm. Three locations have stopped using an incident detection algorithm altogether, citing the high false alarm rates and other faster means of detection (i.e., cellular telephones and closed circuit television) as being reasons for discontinuing the use of an incident detection algorithm in their system. Only one visited location (Toronto, Ontario) is using an algorithm other than a modified California algorithm. This location began using the

McMaster algorithm in an operational capacity in late 1992. Initial impressions of the algorithm performance in an operational setting are favorable.

No single algorithm appears to be superior in terms of its reported performance, data requirements, ease of implementation, ease of calibration, and operational experience. Using the results from both off-line and on-line evaluations reported in the literature, most algorithms appear to achieve the same level of detection and produce similar false alarm rates, when properly calibrated. Detection times for most algorithms are also similar.

Given the results of the evaluation and the site visits, it is recommended that the TxDOT consider the following incident detection algorithms in the initial implementation of their freeway surveillance and control centers:

- Modified California Algorithm #7
- Modified California Algorithm #8
- McMaster Algorithm

These algorithms are recommended because of the ease that they can be implemented and because they require only limited amounts of on-line complex calculations. When properly calibrated, they should perform adequately and can be adapted to the different operating conditions that exist in the various cities where TxDOT will be implementing systems. Consideration should be given to combining the modified California algorithm into a detection system where one of two algorithms can be selected based on prevailing traffic conditions. Unfortunately, as with any algorithm, these algorithms require extensive calibration, with data required for each detection area to properly calibrate the algorithm.

1. INTRODUCTION

The Texas Department of Transportation (TxDOT) is currently designing complex freeway surveillance and control centers to be installed in many major metropolitan areas in Texas. The purpose of these centers is to improve traffic operations on the freeway system by performing many functions, including the following:

- detecting the presence of congestion and lane blocking incidents;
- dispatching personnel to clear incidents and accidents from the freeway;
- implementing control strategies (such as ramp metering) to regulate traffic entering the freeway; and
- providing motorists with information about the cause of the congestion, expected delays and alternative routes around the congestion.

One issue to be determined by TxDOT in the design of their system is the selection of an incident detection algorithm to use in the initial implementation of the system. Many incident detection algorithms have been developed and reported upon in the literature. Each algorithm uses different techniques for detecting the presence of capacity-reducing incidents. For example, some algorithms compare the measured loop occupancy levels at a single or group of detector stations to preestablished thresholds. Other algorithms monitor how traffic measures change over time. There is no clear winner as to which algorithm or detection philosophy is best for a single situation. The Texas Transportation Institute was asked by TxDOT to conduct an analysis of the existing incident detection algorithms and provide recommendations as to which algorithms should be considered in the initial implementation of TxDOT's freeway surveillance and control centers. Specifically, the questions to be addressed in this research were as follows:

- What incident detection algorithms are currently being used in operational freeway surveillance and control systems in the United States and Canada?

- How effective are these algorithms at detecting incidents in an actual operating system?

- What kind of operational problems are caused by these algorithms?

- What incident detection algorithm(s) should TxDOT use (at least initially) when implementing their freeway surveillance and control system?

Objectives

The objectives of this research were as follows:

1. Using the literature, assess the existing incident detection algorithms in terms of their reported operational performance, ease of calibration, ease of implementation, and data requirements;

2. Determine which algorithms, if any, are currently being used in select freeway management systems in the United States and Canada; and

3. Recommend which of the currently available incident detection algorithms should be considered by TxDOT for possible inclusion into the initial implementation of their freeway surveillance and control systems.

Scope

The scope of this research was limited to a review of available incident detection algorithms reported in the literature or in operation in existing freeway management centers in the United States and Canada. The research included algorithms that appeared promising but not yet implemented in an actual freeway management center. No new incident detection algorithms were developed as part of this research.

The study was limited to a review of incident detection algorithms that use data from inductive loop detectors only. Although the report does contain a section on other potential means of detecting incidents (such as video imaging or the use of automatic identification systems), a detailed assessment of these techniques was not performed.

Furthermore, the assessment of the performance of the incident detection algorithms was based on the results published in the available literature. No attempt was

made to use actual field data to compare the performance of the algorithms. Since algorithm performance is very dependent on the design of the system and how well the algorithm is calibrated for the system, the research assumes that the results published in the literature by other authors are accurate and objective.

Organization of Report

This report consists of three additional chapters. Chapter 2 discusses the theoretical aspects of the available incident detection algorithms. Chapter 3 provides a summary of on-site field observations that were performed at seven operating freeway surveillance and control systems in the United States and Canada. Chapter 4 provides an assessment of the performance and implementation aspects of the various incident detection algorithms. In Chapter 5, three incident detection algorithms are recommended for consideration by TxDOT in the initial implementation of their freeway surveillance and control systems.

2. REVIEW OF EXISTING INCIDENT DETECTION ALGORITHMS

Many computer algorithms have been developed to detect incidents in freeway surveillance and control systems. Some algorithms compare direct measurements of traffic to preestablished thresholds. Others use statistical procedures to detect changes in traffic conditions over time. Still others use complex theoretical models to predict expected traffic conditions given current conditions and historical trends. The structure of an algorithm can greatly influence its performance in terms of detection rate, false alarm rate, and detection time.

In this chapter, existing incident detection algorithms are reviewed. The review focuses on the following key elements:

- the underlying theory of each algorithm,
- the data required to operate each algorithm, and
- the reported performance of each algorithm in an operational setting.

However, before the each algorithm can be assessed, it is important to understand the traffic patterns that result when incidents occur under different operating conditions on a freeway. It is also important to have an understanding of traffic and operational situations that can cause incident detection algorithms to generate false alarms.

Incident Traffic Patterns

An incident is defined as any non-recurrent event which causes a temporary reduction in the capacity of a freeway or an abnormal increase in demand on a freeway (1). Incidents can be predictable (such as construction or maintenance operations and special events) or unpredictable (such as accidents, stalled vehicles, weather, etc.) The purpose of an incident detection algorithm is to automatically identify the occurrence of unpredictable incidents that affect the capacity of a freeway (specifically accidents and stalled vehicles) so that appropriate response and clearance procedures can be executed to minimize the effects of the incident on traffic operations. The goal is to identify incident locations as quickly as possible.

Typically, when an incident occurs on a freeway, the capacity of the freeway is reduced. The amount of the reduction depends on several factors, including the following:

- the time at which the incident occurred (i.e., whether the incident occurred peak versus off-peak travel demand periods),
- the location of the incident (i.e., whether the incident is on the shoulder or in the travel lanes),
- the number of lanes that are blocked,
- the duration of the incident, and
- the severity of the incident.

Table 2-1 shows the magnitude of capacity reductions for several typical incident situations occurring on the Gulf (I-45 South) Freeway in Houston, TX.

Table 2-1. Typical Reductions in Capacity for Different Incident Types (2).

Incident Situation	Amount of Capacity Reduction (Percent)
Normal Flow (three lanes - no incident)	-
Stall (one lane blocked)	48
Non-injury accident (one lane blocked)	50
Accident (two lanes blocked)	79
Accident on shoulder	26

However, the effects of an incident are not solely dependent on the magnitude of the capacity reduction. The nature of the incident and the traffic conditions that prevail at the time of the incident also influences its effect on traffic operations. The difference between the incoming traffic demand and the resulting capacity dictates the traffic patterns

6

that develop when an incident occurs on a freeway. In general, there are five basic incident situations that create distinctive patterns in traffic detector data (3):

Incidents in Uncongested Freeway Sections

● **The capacity at the incident site is less than the oncoming traffic demand.** Under this situation, a queue would develop upstream of the incident since the oncoming traffic demand is greater than the number of vehicles that can pass through the incident site. The queue propagates upstream of the incident site as more vehicles enter the congested area. Because not as many vehicles are getting past the incident site, a region of light traffic moves downstream at the same time as the queue begins to build upstream of the incident. This type of traffic pattern is the most distinctive of all the possible patterns that can develop; therefore, it is the easiest traffic pattern that can be detected by an algorithm. Figure 2-1 illustrates this type of traffic pattern.

● **The capacity at the incident site is greater than the oncoming traffic demand.** This type of traffic pattern is typically associated with incidents that have been moved to the shoulder. As shown in Figure 2-2, traffic flow past the incident site is not greatly impacted. Measurements from the loop detectors show that traffic is basically the same as before the incident occurred. Only minor queues (and possible no queues) form in the immediate area of the incident. Depending on how close the incident is to a detector station, queues may not extend over the detectors. Therefore, this type of incident pattern is more difficult to distinguish than the one above. Most incident detection algorithms cannot detect this type of incident pattern when it occurs.

● **The traffic demand is so light that the incident has no measurable effect of traffic patterns.** In this case, the light traffic demand prevent queues and congestion from forming at the incident site. Since there is no congestion or queuing, delays to motorists are minimal. This type of traffic pattern typically occurs under low traffic volumes (such as at night). Because traffic is not significantly impacted, most algorithms are not capable
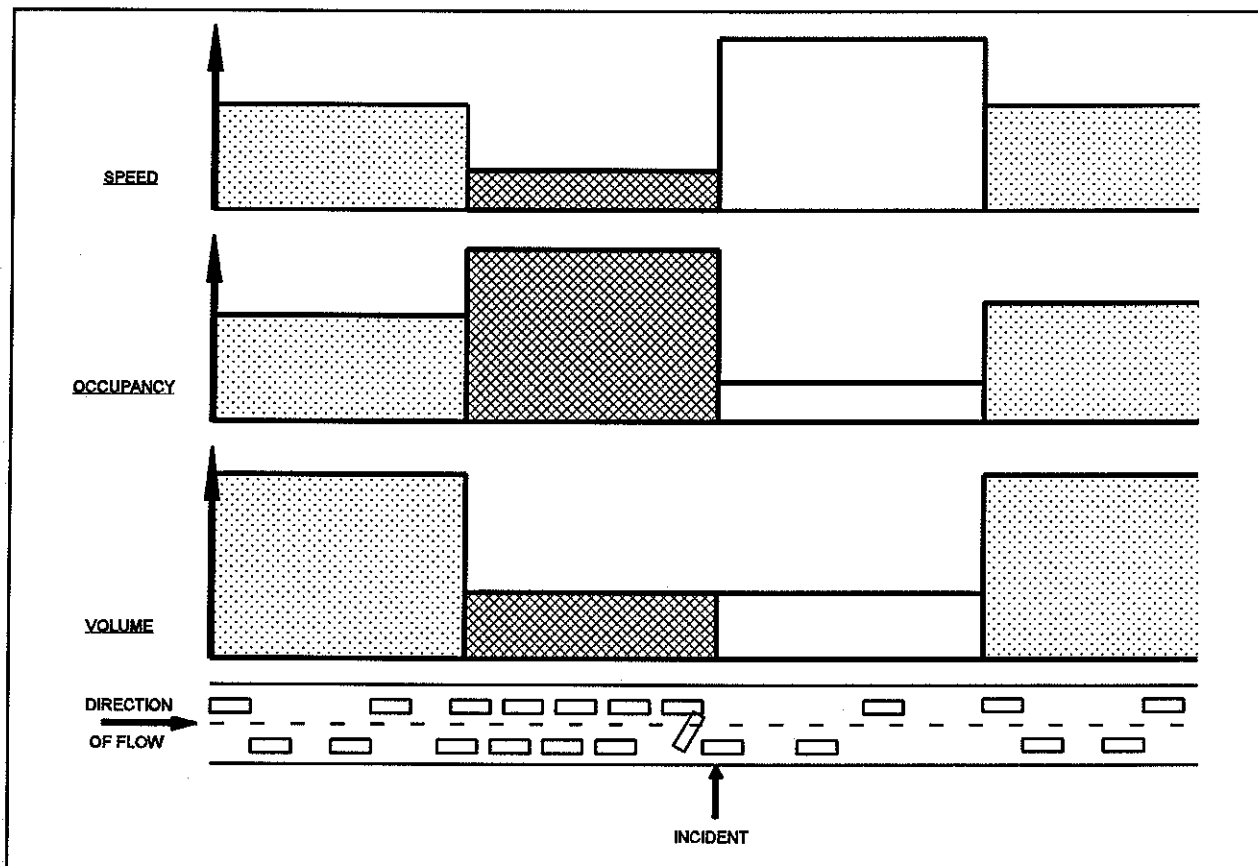
Figure 2-1. Typical Traffic Pattern When Demand Exceeds Capacity During Incident Conditions (37).

of detecting incidents that occur under this situation. However, attempts have been made to develop algorithms that can detect incidents under low-volume conditions. These algorithms and their performance are discussed later in this chapter. The typical traffic patterns associated with this particular situation is shown in Figure 2-3.

Incidents in Congested Freeway Sections

●   **The capacity at the incident site _is less_ than the volume of traffic downstream of the site.** This situation typically occurs during heavy traffic conditions where traffic is congested prior to the incident. In this situation, the incident meters traffic entering the segment of freeway downstream of the incident. Because the demand in the downstream section has reduced,

8
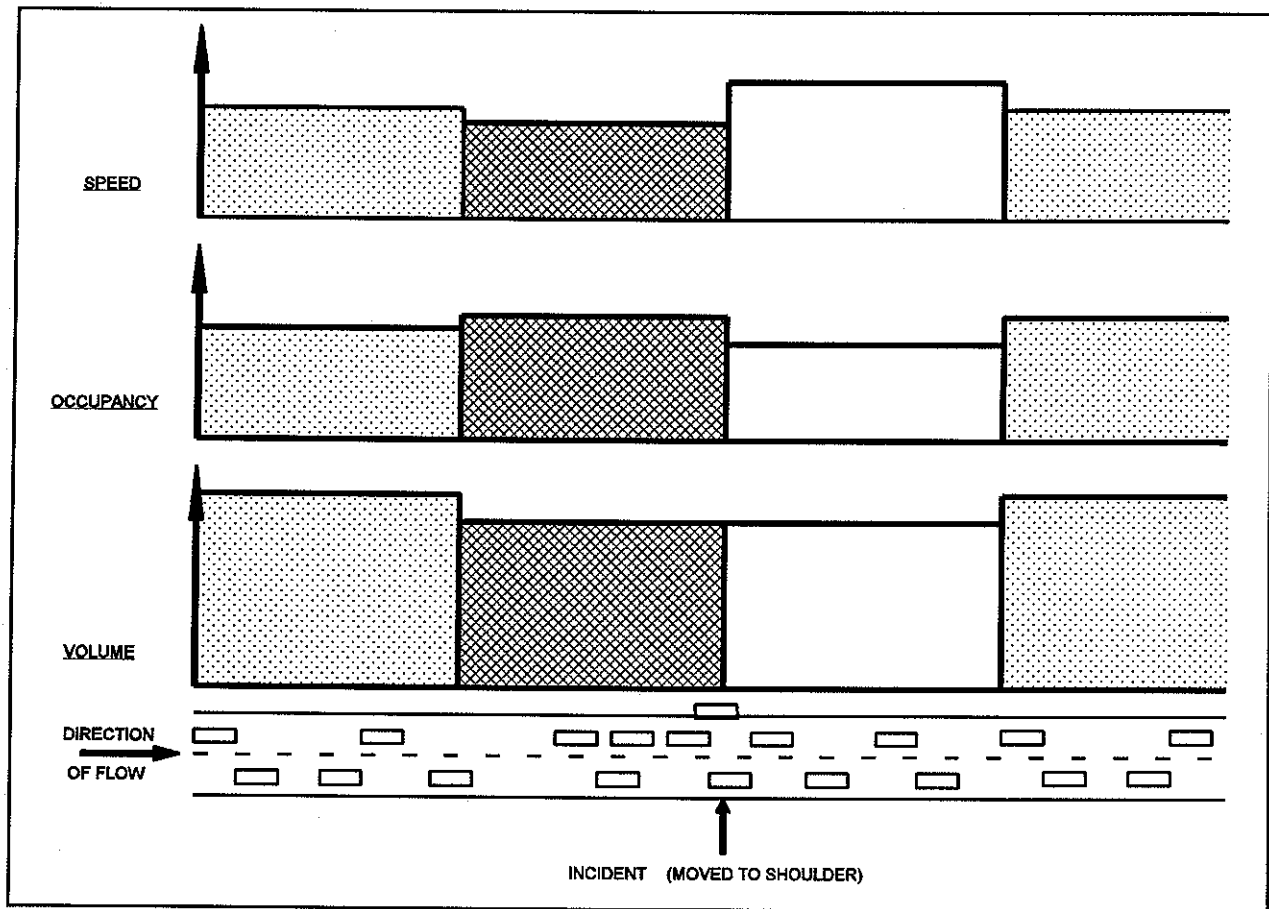
Figure 2-2. Typical Traffic Pattern When Capacity is Greater Than Demand During Incident Conditions.

the congestion downstream of the incident begins to slowly clear, while upstream of the incident, congestion persists. Incidents that occur under these situations may be detected by some algorithms but only after a considerable delay. This situation is illustrated in Figure 2-4.

● **The capacity at the incident site _is not less_ than the downstream traffic volume.** This type of situation is typically associated with secondary incidents that occur in queues caused by other incidents. Most of the time, the effects of these incidents are localized (see Figure 2-5). Since traffic is already congested, traffic queues and shock waves do not propagate upstream to a detector station. As a result, the second incident does not

9
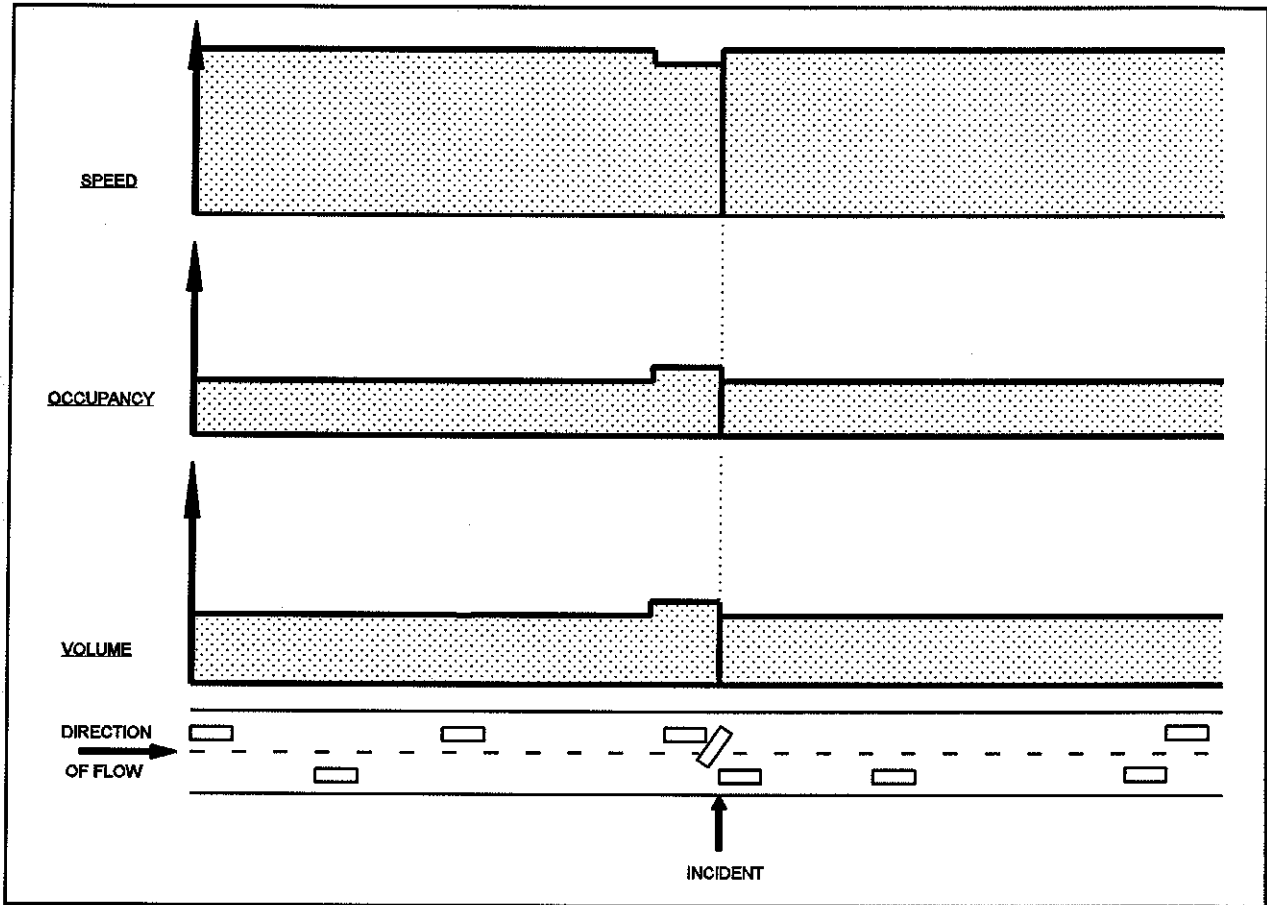
Figure 2-3. Typical Traffic Pattern When Incident Occurs in Low Volume Conditions.

typically result in a noticeable difference in traffic conditions. For this reason, some algorithms may not detect incidents that occur under this situation until the congestion from the first incident has cleared.

As indicated above, not all types of incident patterns can be readily detected by all incident detection algorithms. Some algorithms can detect certain types of incident-induced traffic patterns better than others. Currently, there does not appear to be an incident detection algorithm that can detect all incidents under all conditions. Furthermore, the ability of an algorithm to detect an incident is also influenced by the duration of the incident, the spacing between detector stations, the location of the incident relative to the detector stations, and the operating conditions that existed at the time the incident occurred.
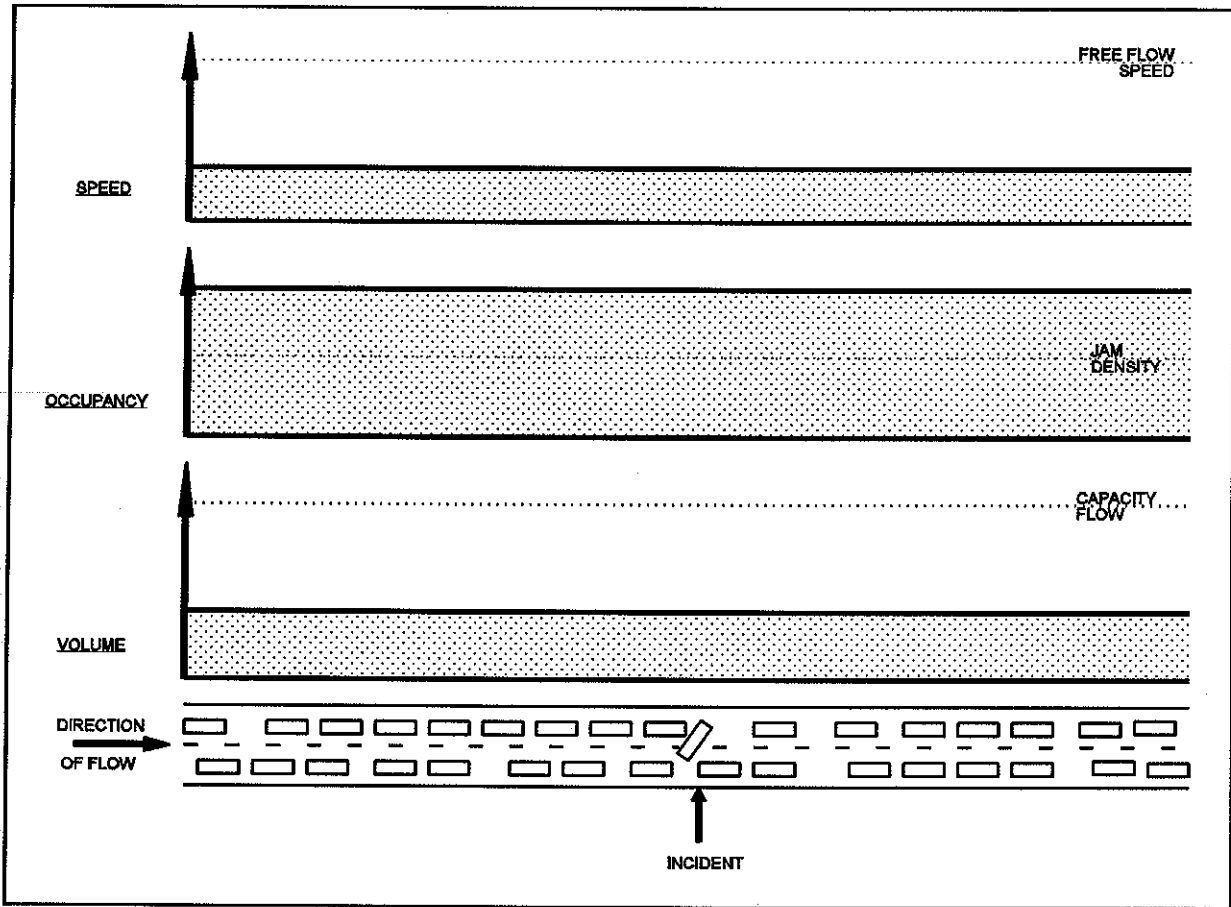
Figure 2-4. **Typical Traffic Pattern When Capacity at Incident Site is Less Than Volume Downstream of Incident.**

Situations That Cause False Alarms

The inability to quickly detect incidents under different traffic patterns is one difficulty facing existing incident detection algorithms. Another difficulty is limiting the number of times that an algorithm issues an incident alarm when an incident does not actually exist (i.e., a false alarm).

One common problem that can create false alarms are malfunctioning loop detectors (3). When this occurs, the detector station can falsely report a high occupancy rate. Most freeway surveillance and control systems include tests that check the validity of incoming detector data before it is used in the algorithm.
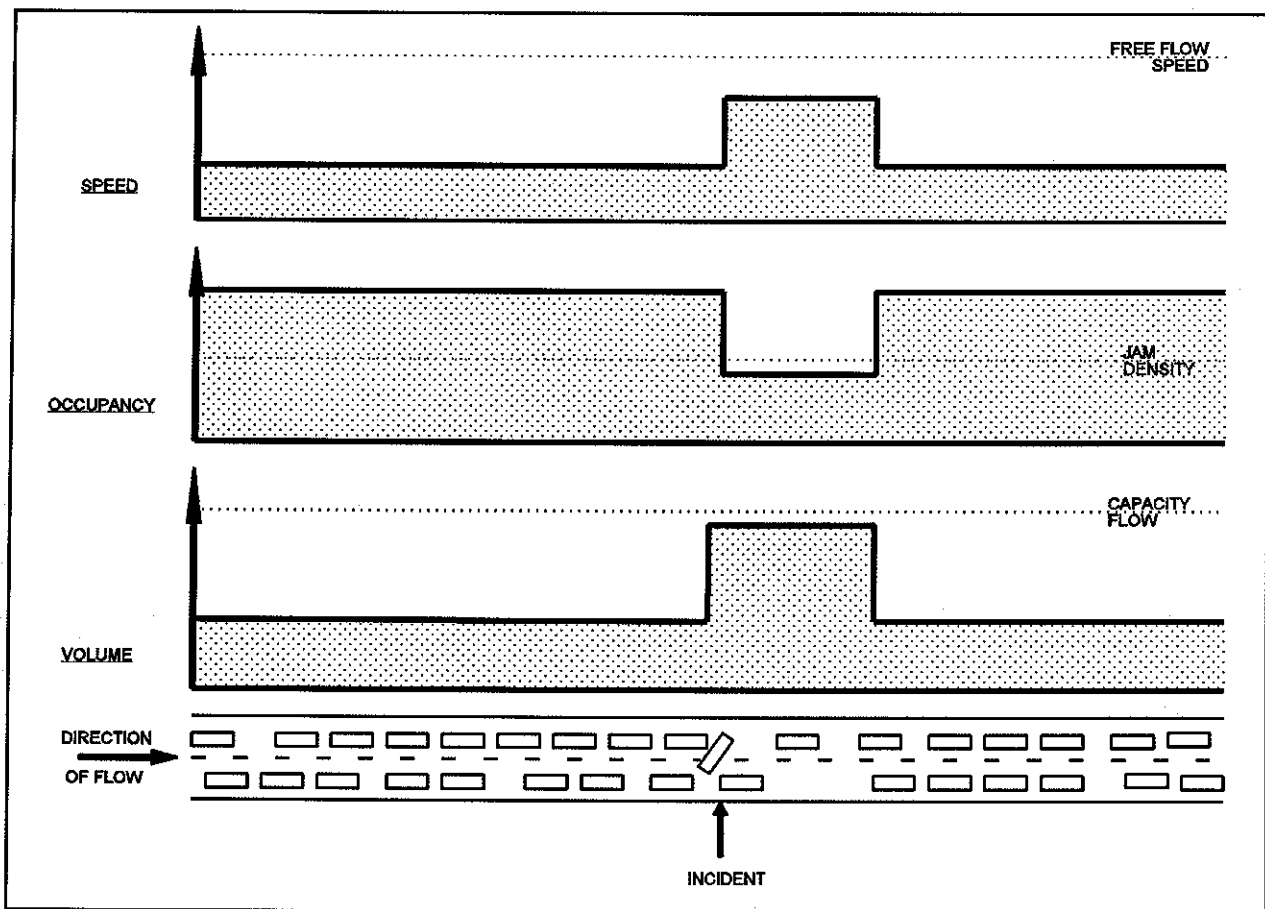
Figure 2-5. **Typical Traffic Pattern When Capacity is not Less Than Volume Downstream of Incident.**

There are also patterns in incident-free traffic that tend to mimic traffic patterns associated with incidents (3). False alarms can also be generated when individual vehicles create isolated variations in speed. This type of pattern can be caused by trucks or other slow-moving vehicles in the traffic stream, and is a prevalent cause of false alarms in most incident detection algorithms. The pattern manifests itself as a compression wave that propagates in the opposite direction of the flow of traffic. It causes a false alarm to be sounded because the station-to-station differences in traffic conditions are similar in magnitude to that generated by incidents.

A third common situation that tends to cause incident detection algorithms to produce false alarms is associated with abnormal geometries (3). Abnormal geometries, such a sharp horizontal curves or severe vertical grades, can cause speeds to decrease

on a freeway, particularly on freeways with heavy truck traffic. Freeway-to-freeway interchanges where one or more lanes are dropped or shared can also be as source of speed variations. Heavy demand on the exit ramps can cause differences in occupancies between two detector stations to appear as incidents to some detection algorithms. Proper calibration of the algorithm to account for the different operating characteristics of traffic at these locations may help to reduce the number of false alarms.

A final situation that can cause some incident detection algorithms to produce false alarms is typically associated with bottleneck areas (3). Bottlenecks occur when traffic demands exceed the physical capacity of the freeway, thereby causing congestion and delays. Most incidents are temporary and unexpected bottlenecks. However, bottleneck congestion is recurrent, occurring at the same location at the same time each day. A typical location where bottleneck congestion can occur is at high volume entrance ramps where entering traffic demand exceeds the capacity of the freeway. This situation creates the high occupancy values and detector-to-detector differences in traffic parameters that are used in incident detection algorithms.

Relationship Between Detection, False Alarms, and Time to Detect

As shown in Figure 2-6, a tradeoff exists between the number of incidents that can be detected by an algorithm, the number of false alarms that an algorithm produces and the time required to detect an incident (3). For the most part, the detection rate and the false alarm rate are directly related. Algorithms that are set to detect a large percentage of the incidents also tend to produce a high number of false alarms. Similarly, algorithms whose sensitivity is reduced to minimize the number of false alarms also tend to miss incidents.

A third variable, the time taken to detect the incident, also influences the detection and false alarm rates. By increasing the time taken by the algorithm to detect an incident, it is possible to both increase the detection rate while, at the same time, reduce the false alarm rate. However, the longer it takes to detect an incident, the greater the impact of the incident on traffic flow. Therefore, to be effective, it is critical that incident detection algorithms achieve a balance between the number of incidents that can be detected, the false alarm rate and the detection time. The most effective algorithms are those that

13
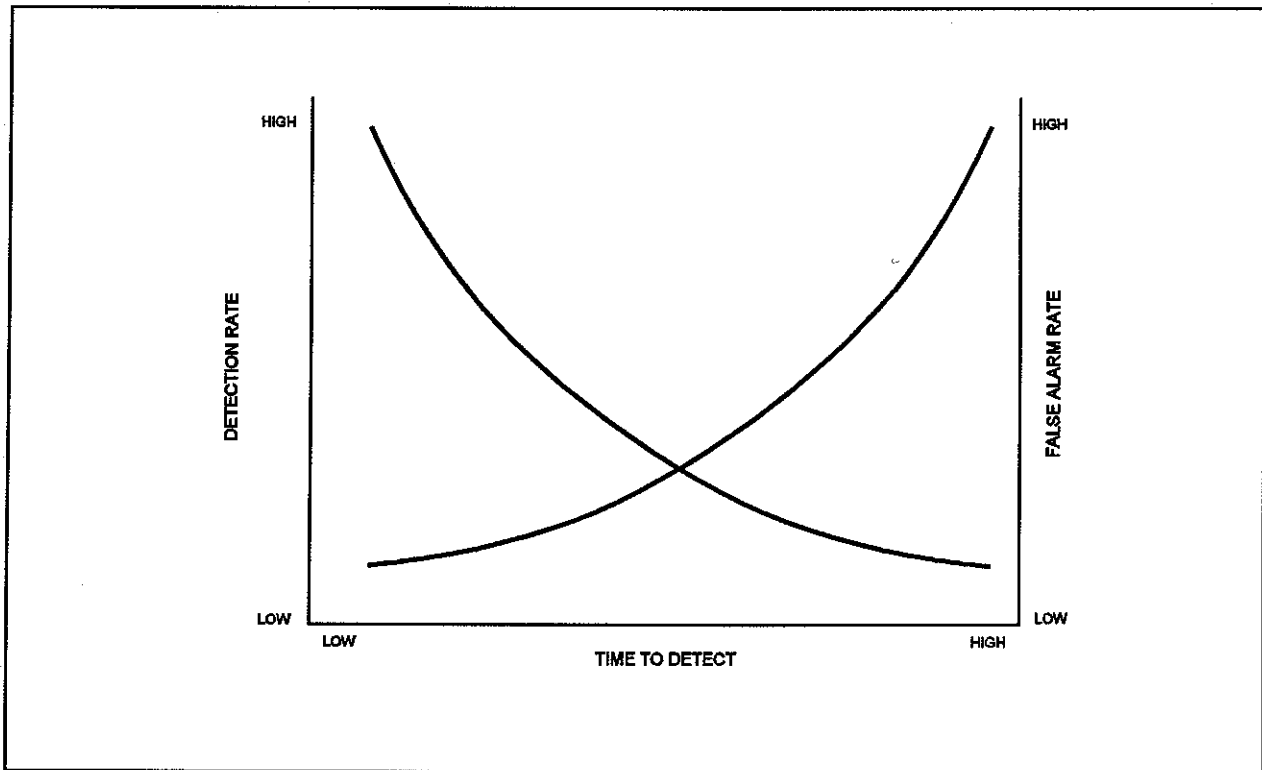
Figure 2-6. Relationship Between Detection Rate, False Alarm Rate, and Detection Time.

maximize the detection rate while minimizing both the detection time and the false alarm rate.

Existing Incident Detection Algorithms

Existing incident detection algorithms can be categorized into one of the five groups listed below. These categories are based on the theoretical approaches that are used to detect incidents.

- Comparative Algorithms,
- Statistical Algorithms,
- Time-Series Algorithms,
- Smoothing or Filtering Algorithms, and
- Modeling Algorithms.

Table 2-2 lists the existing incident detection algorithms contained within each category. The remainder of this chapter is devoted to discussing the existing algorithms in these categories.

Table 2-2. Existing Incident Detection Algorithms.

COMPARATIVE ALGORITHMS	●Basic California ●Modified California ●All Purpose Incident Detection ●Pattern Recognition (PATREG)
STATISTICAL ALGORITHMS	●Standard Normal Deviate (SND) ●Bayesian
SMOOTHING / FILTERING ALGORITHMS	●Exponential Smoothing ●Low-Pass Filtering
TRAFFIC MODEL ALGORITHMS	●Dynamic Model ●McMaster

Comparative Algorithms

Comparative algorithms are the simplest of all the existing algorithms. They rely on the principle that an incident will cause an increase in the loop detector occupancy levels upstream of the incident while, at the same time causing a decrease in the occupancy levels downstream of the incident. Sometimes called pattern-recognition algorithms, comparative algorithms compare the value of a measured traffic parameter (i.e., volume, occupancy, or speed) to a preestablished threshold value. The thresholds are used to define the point that traffic flow becomes congested at a location. An incident is detected when the measured traffic parameter exceeds the established thresholds. Most comparative algorithms perform one or more of the following tests:

- tests to distinguish between incident and bottleneck congestion,
- tests to detect the presence of compression waves in traffic data,
- tests to ensure that incident traffic patterns persist for a specified period (and not caused by short-lived random fluctuations in traffic), and
- tests to determine whether to terminate an incident alarm.

California Algorithm

The California Algorithm is the most widely known (and perhaps most commonly used) comparative algorithm in the United States. It was originally developed for use in the Los Angeles freeway surveillance and control center in the late 1960s. The basic structure of the algorithm compares traffic conditions between two adjacent detector stations using the following three parameters derived from measurement of loop occupancy (3):

- the absolute difference in the measured occupancy between the upstream and downstream detector stations,

- the difference in the measured occupancy between the upstream and downstream detector stations relative to the occupancy level at the upstream station, and

- the relative difference in the measured occupancy from two minutes ago as compared to the current occupancy level at the down stream detector station.

An incident is declared when all three of these traffic parameters exceed the preestablished thresholds. Additional tests, which also compare the difference in occupancy between detector stations, are used to decide whether to terminate an incident alarm after a specified period.

Figure 2-7 shows the basic California algorithm structured as a binary decision tree. A binary decision tree consists of one or more logical decisions grouped together in a tree-like structure. Each logical decision is based upon a comparison of a traffic feature to its corresponding threshold value.

16

```
                    ┌─────────────────────┐
                    │   OCCDF ≥ THRES. 1  │
                    └─────────────────────┘
           TRUE        /            \      FALSE
                      /              \
          ┌──────────────────────┐   ┌───┐
          │   OCCRDF ≥ THRES. 2  │   │ 0 │
          └──────────────────────┘   └───┘
     TRUE    /            \  FALSE
            /              \
  ┌───────────────────┐   ┌───┐
  │  DOCCTD ≥ THRES. 3│   │ 0 │
  └───────────────────┘   └───┘
  TRUE  /        \  FALSE
       /          \
    ┌───┐        ┌───┐
    │ 1 │        │ 0 │
    └───┘        └───┘
```

OCCDF = DIFFERENCE IN OCCUPANCY

ODDRDF = RELATIVE DIFFERENCE IN OCCUPANCY

DOCCTD = TIME DIFFERENCE IN OCCUPANCY AT DOWNSTREAM STATION

0 = INCIDENT-FREE STATE

1 = INCIDENT STATE
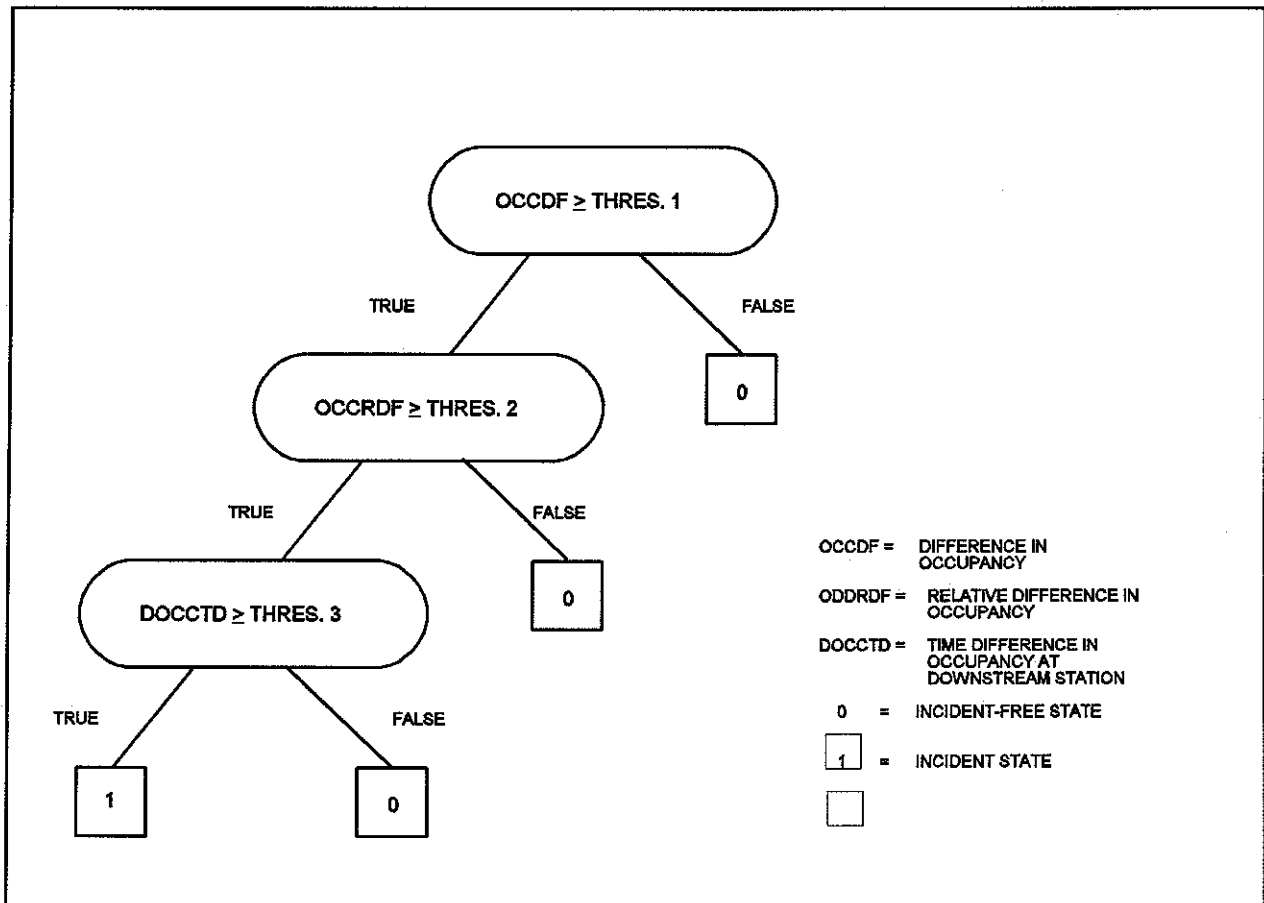
Figure 2-7. Structure of Basic California Incident Detection Algorithm (3).

Modified California Algorithm

In late 1973, FHWA awarded a contract for a research study to develop improved incident detection algorithms (3). This research study was initiated because of the high false alarm rate produced by many of the incident detection algorithms then in use in existing surveillance and control centers (4). The research identified and tested ten modified versions of the California algorithm. Besides using different traffic variables, two additional features were employed in these modified algorithms to reduce false alarm rates: persistence checks and compression wave tests. As previously discussed, incident free-data contains many flow disturbances (or inhomogeneities) which mimic incident conditions. These disturbances are short-lived, typically lasting only one or two execution

17

cycles of the algorithm. To combat these short-lived disturbances, Payne et al. (3) included additional tests that required traffic discontinuities to persist for a specific time before an incident alarm was sounded, thereby increasing the detection time. These persistence checks were found to be sufficient to eliminate most short-lived disturbances.

Compression waves in heavy traffic also tend to produce false alarms in many incident detection algorithms. Compression waves occur in heavy traffic where stop-and-go traffic conditions create large sudden increases in occupancies. These surges in occupancies move through the traffic stream from 5 to 15 mph (8 to 24 kmph) in the direction counter to the traffic flow. They are detected by monitoring traffic data for a large increase in occupancy at a station followed by a similar increase in occupancy at the next upstream station within the interval required for the compression wave to reach the upstream station.

Payne et al. (3) conducted an evaluation of the ten versions of the California algorithm using data obtained from the Los Angeles and Minnesota freeway surveillance systems. A total of 153 incident and 30 incident-free data sets were used in the evaluation. Performance characteristic curves of the detection rate and the false alarm rate were developed to evaluate each algorithm. All except one of the modified versions of the California algorithms use traffic variables derived from occupancy measurements as the primary parameters evaluated in the algorithm. These occupancies are one-minute averages for a detection station. In the exception, a speed measurement derived from volume and occupancy was used as a third traffic parameter.

Of the ten algorithms, two were reported by Payne et al. (3) as providing the best overall results: Algorithms #7 and #8. In Algorithm #7, the third parameter of the basic California algorithm was replaced with a measurement of the current downstream occupancy level. This variable was added so that compression waves could be more readily identified. A persistence check was also added that required incident conditions at a detection station to last for more than two iterations of the algorithm before an alarm was sounded.

Algorithm #8 uses a suppression feature that delays sounding an incident alarm for five minutes after a compression wave has been detected. While the algorithm appears complex (it involves 21 individual decisions), most are simple comparisons of occupancy-

18

related traffic variables to preestablished thresholds. The decision trees for both these algorithms are shown in Figure 2-8 and 2-9, respectively.

All Purpose Incident Detection Algorithm

The All Purpose Incident Detection (APID) algorithm was developed for use in the COMPASS advanced traffic management system implemented in the Metropolitan Toronto area (5, 6). One of two algorithms used in the system, the APID algorithm incorporates the major elements of the California algorithms into a single structure. The algorithm consists of the following major routines:

- a general incident detection algorithm for use under heavy traffic conditions,
- a light volume incident detection algorithm,
- a medium volume incident detection algorithm,
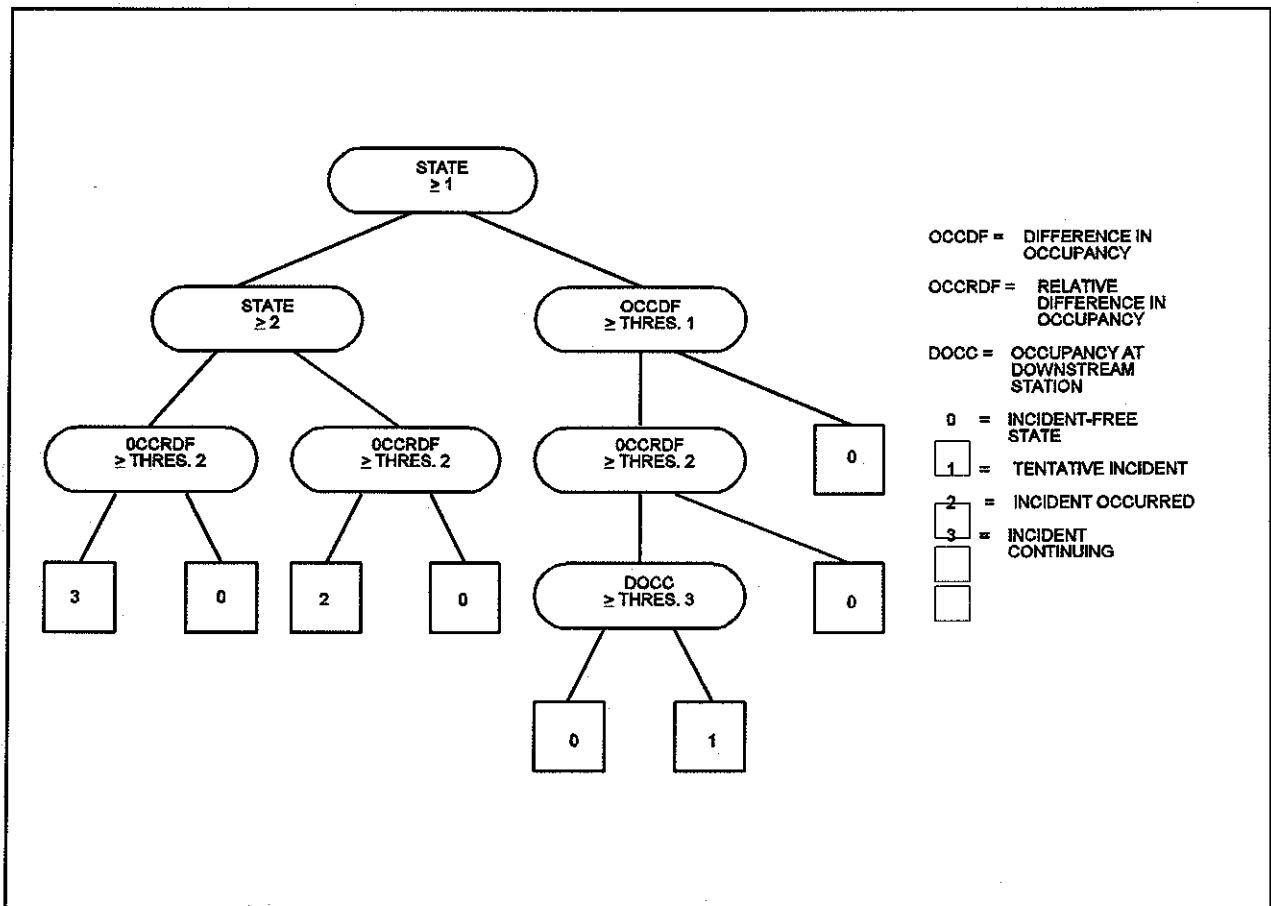
Figure 2-8. Decision Tree for Modified California Algorithm #7 (3).

19

STATE | DESIGNATES
0 | INCIDENT-FREE
1 | COMPRESSION WAVE DOWNSTREAM IN THIS MINUTE
2 | COMPRESSION WAVE DOWNSTREAM 2 MINUTES AGO
3 | COMPRESSION WAVE DOWNSTREAM 3 MINUTES AGO
4 | COMPRESSION WAVE DOWNSTREAM 4 MINUTES AGO
5 | COMPRESSION WAVE DOWNSTREAM 5 MINUTES AGO
6 | TENTATIVE INCIDENT
7 | INCIDENT CONFIRMED
8 | INCIDENT CONTINUING

Figure 2-9. Decision Tree for Modified California Algorithm #8 (3).

20

- an incident termination detection routine,
- a routine for testing for the presence of compression waves, and
- a routing for testing for the persistence of incident conditions.

The primary advantage of this algorithm over the other versions of the California algorithm is that different algorithms are used depending on existing traffic conditions. An initial test defines the existing current traffic conditions on the freeway. The test uses occupancy levels at a detection station to determine the most appropriate incident detection algorithm to use. Traffic conditions are classified as heavy, medium, or light. Different algorithms (which check different traffic parameters) are selected based upon the prevailing traffic conditions on the freeway. If the traffic conditions are defined as "heavy," the algorithm uses the basic California algorithm (discussed above) to detect incidents between detector stations. For medium traffic conditions, two different traffic parameters are used: the relative spatial difference in occupancies ($OCCRDF(i,t)$) and the relative temporal difference in speed ($SPDTDF(i,t)$). (Note: the algorithm that was used during light volume conditions was not defined in the literature). Persistence checks and compression wave tests are also performed under each traffic volume condition before a confirmed incident alarm is issued to the operator.

A two-week on-line evaluation of the APID algorithm was performed on the Burlington Skyway in Ontario, Canada. During this evaluation, the APID detected 66 percent of the total 29 incidents that occurred on the freeway. However, this sample included several minor incidents that did not cause significant disruptions to traffic. If these incidents are removed from the data base, the APID achieved a detection rate of 86 percent. The average detection time achieved during the evaluation period was 2.5 minutes. The algorithm reportedly experienced a false alarm rate of approximately 0.05 percent during the evaluation period.

As a result of the two-week evaluation plus actual on-line operational experience, it was concluded that the APID algorithms worked best under heavy traffic volume conditions. The performance of the algorithms in terms of missed incidents and false alarms is not as good under low volume conditions as under heavy volume conditions. Therefore, it was concluded that another algorithm (such as a double exponential smoothing algorithm that is discussed below) should be used during light traffic conditions.

Pattern Recognition Algorithm

The Pattern Recognition (PATREG) Algorithm was developed by the Transport and Road Research Laboratory (TRRL) as part of their Automatic Incident Detection (AID) system (7). It is used in conjunction with another algorithm, HIOCC (discussed later), to detect the traffic disturbances following an incident on high-speed facilities in England. Comparing detector data from two consecutive detector stations, the PATREG monitors detector data for significant changes in speed of individual vehicles between the two detector stations. The speed of an individual vehicle is calculated based on the assumption that under steady-state, incident-free conditions, a particular traffic pattern observed at an upstream detector station can also be observed, after a delay, at a downstream detector. Under ideal conditions, the delay before the pattern is observed at the downstream station is equal to the travel time between the two detector stations. By determining the amount of delay that occurs before the same traffic pattern appears at a downstream detector station, the average speed of traffic in each lane can be estimated. The estimated speed is then compared to predetermined upper and lower speed thresholds that have been developed for that particular lane. If the estimated speed in a lane falls outside the threshold value during a pre-set number of consecutive intervals (that acts as a persistence check), then an alarm is sounded.

A limited off-line evaluation of the performance of the algorithm was conducted using data from England and 12 staged incidents in France. The evaluation showed that the algorithm did not perform well once traffic volumes exceeded 1500 vehicles per hour per lane (vphpl). It is believed that when traffic becomes heavy, traffic patterns become too random to be recognized by the detection algorithm. The algorithm was unable to detect any of the staged incidents.

Statistical Algorithms

Algorithms in this category use standard statistical techniques to determine whether observed detector data differ statistically from estimated or predicted values. Algorithms in this category include the Standard Normal Deviate and the Bayesian algorithms.

Standard Normal Deviate

The Standard Normal Deviate (SND) algorithm was developed by the Texas Transportation Institute in the early 1970's for use in the initial surveillance and control center installed for the Gulf Freeway (I-45 South) in Houston, TX (8). The algorithm is based on the premise that a sudden change in a measured traffic variable suggests that an incident has occurred on the freeway. Using this premise, the algorithm evaluates trends in selected traffic variables (i.e., either occupancy or energy) to determine when they deviate more rapidly than the expected.

The algorithm computes the standard normal deviate of the control measure. A standard normal deviate (or SND) is the number of deviations a particular value of a variable is away from the mean of that particular variable. It is equivalent to placing confidence intervals on the measured traffic variable. The SND reflects the degree to which the observed field measurement (e.g., the one minute average of loop occupancy) has changed during a given interval compared to the average trend measured during several previous intervals (e.g., three minutes). Measured SND values are compared to critical values that define thresholds for detecting incidents. An SND value greater than the critical SND value indicates that a major change in operating conditions has occurred on the freeway. An SND value less than the critical SND value implies that measured traffic conditions are not statistically different from past trends.

Two operational strategies were developed for implementing the SND model in an actual freeway surveillance and control center. The first requires that only the present minute SND value to be critical. The second operating strategy requires that two successive SND values be critical. In actuality, the second SND value is used as a persistence check.

A moving average technique was used to compute the mean of the control variable. The performance of the algorithm was evaluated using two time bases. The first method used data from the previous three-minute sampling periods to compute the mean and standard deviation of the control variable. The second method considered parameters from the previous five minutes.

The SND model was evaluated using data from the Gulf Freeway in Houston, TX. Incidents were observed manually using video surveillance cameras. When an incident was observed, data about the incident were recorded in a log book at the surveillance center. A computer program was also started that recorded the loop detector data. The evaluation of the performance of the algorithms then occurred off-line. Data were collected from a total of 35 incidents. Data from three A.M. peak periods (7-8 a.m.) where no incidents occurred were used to evaluate the false alarm rate of the algorithm. Because of the tradeoff between detection capabilities and false alarms, an SND value that achieved results approaching a 90 percent detection rate and a 1 percent false alarm rate was used to determine the critical SND value

When only one SND iteration value was required to be critical, the algorithm achieved an 86 percent detection rate when both occupancy and energy were used as control variables. The performance of the occupancy variable was considered better, however, because of the lower frequency of false alarms. Changing the time bases (from a three-minute moving average to a five-minute moving average) did not greatly affect the performance of the algorithm in terms of detection rate or false alarm rate.

When two successive SND values were required to be critical before an alarm was issued, a higher percentage of incidents were detected using occupancy than energy. When a five minute moving average of the incoming traffic data was used to compute the mean and the standard deviation, this approach detected 92 percent of the 35 incidents with an average detection time of 1.1 minutes. The false alarm rate was computed to be 1.3 percent during the peak period. Both time bases, however, resulted in a lower false alarm rate than when only one SND was required to be critical.

Bayesian Algorithm

Levine and Krause (9) proposed an algorithm that uses Bayesian statistical techniques to compute the probability that an incident signal is caused by a lane-blocking incident after accounting for the previous incident and nonincident signals produced by the algorithm. The algorithm actually uses the relative difference the occupancies (OCCRDF) used in the California algorithm as the traffic measure. However, unlike the California

24

algorithm, the algorithm applies Bayesian statistics to compute the conditional probability that the relative difference in the occupancy is caused by an incident. Bayesian theory assumes that frequency distributions of the upstream and downstream occupancies during incident and incident-free conditions can be developed. Using historical data on the frequency of the capacity-reducing incidents for a section of freeway, the probability of an incident occurring on a section of freeway can be derived. Similarly, the probability of not having any capacity-reducing incidents can also be derived from historical occupancy data. Given these probabilities, Bayesian concepts are applied to find the probability that an incident has occurred given that the relative difference in occupancy has exceeded an established threshold.

In theory, the probability that an incident occurred between two detector stations can be determined for a series of incident indications. For example, Bayes theory can be applied to compute the probability that an incident has occurred given that two of the last three signals from the algorithm showed no incident has occurred in the section. Because the probability is assigned to this occurrence, the operator can estimate the likelihood that an incident signal is a false alarm or actual incident.

To implement this algorithm, three data bases are needed:

- traffic occupancy and volume data during incident conditions,
- traffic occupancy and volume data during incident-free conditions, and
- historical data on the type, location, and effects of incidents.

These data are required for each section in which the algorithm will be used. The first two are required to develop the frequency distributions used to calculate the conditional probabilities. The third is needed to develop the historical probabilities of capacity-reducing incidents occurring in a section of freeway. The probability of an incident occurring at a given detector station at a specified minute in time is given by the following ratio:

$$\frac{A}{B \cdot C}$$

where,

25

A =   the average number of incidents occurring in the study section in the total
      period,
B =   the total number of detectors in the study section, and
C =   the number of minutes used in the study period.

Levine and Krause (9) evaluated the performance of the Bayesian algorithm using off-line data from Chicago, Illinois. A total of 17 incidents representing the afternoon rush-hour on dry-weather weekdays and two hours of incident-free data taken at 15 subsystems were analyzed. Levine and Krause reported that one hundred percent of all the incidents were detected with a 0.0 percent false alarm rate. The structure of the algorithm requires a minimum mean time of detection of at least four minutes.

Levine and Krause (9) also compared the performance of the Bayesian algorithm with three versions of the California algorithm (specifically the original California algorithm, Algorithm #7, and Algorithm #8). Using the off-line data, Levine and Krause found that Bayesian algorithm compares favorably with the other algorithms. However, both Algorithms #7 and #8 detect incidents 2 to 2.5 minutes faster than the Bayesian algorithm. Results from an on-line comparison of the Bayesian algorithm and a modified version of the California algorithm (Algorithm #7) are shown in Table 2-3.

Table 2-3.   Results from On-line Comparison of Bayesian and a Modified California Algorithm.

Algorithm	Detection Rate (Percent)	False Alarm Rate (Percent)
Bayesian	40	
		80
Algorithm #7	46	69

Time Series Algorithms

This type of algorithm assumes that traffic follows a predictable pattern over time. Using historical data that has been collected over time, short-term (i.e., one or two time slices ahead of the current time) prediction of future traffic conditions can then be made. Incidents are detected by comparing observed traffic parameters with values that have been predicted using the time series model. An incident is declared when the difference between the observed and predicted values falls outside an acceptable range.

Figure 2-10 illustrates the general approach used by time series models to detect incidents. A traffic parameter (in this case occupancy) is monitored over time (represented as a solid line in Figure 2-10). Using time series statistical techniques, a relationship is developed to predict future values of the traffic parameter. Confidence intervals (represented by the dashed line in Figure 2-10) are then placed on the predicted traffic variable. An incident alarm is sounded when the observed data crosses outside the confidence interval.

Several different techniques have been used to predict time-dependent traffic variables, including the following:

- ARIMA Algorithm, and
- High Occupancy Algorithm

Time Series ARIMA Algorithm

Ahmed and Cook (10) applied Box-Jenkins techniques to analyze the time series patterns of detector data from several freeway systems in the United States. Using a total of 166 data sets from surveillance centers in Los Angeles, Minneapolis and Detroit, they found that traffic flow on a freeway could be represented by an Autoregressive Integrated Moving-Average (ARIMA [0,1,3]) time series model. The model implies that differences in a traffic variable measured in the current time slice (t) and the same traffic variable in the previous time slice (t-1) can be predicted by averaging the errors between the predicted and observed traffic variable from the last three time slices. Under nonincident conditions, these errors are assumed to follow a random pattern.

27
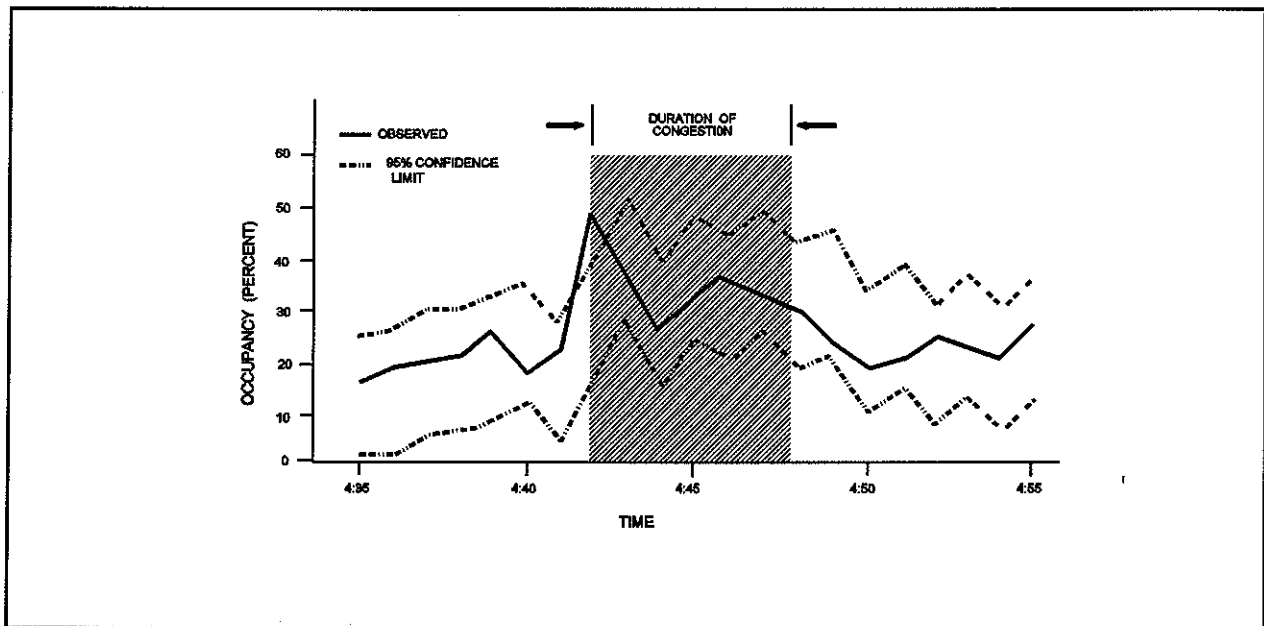
Figure 2-10. General Approach of Time Series Detection Algorithms (11).

Once an appropriate ARIMA model that represents normal traffic operations has been developed, the model can then be used to develop short-term forecasts (one or two time-slices into the future) of the traffic variables. Confidence intervals can also be assigned to the forecast variable, usually two standard deviations away from the corresponding forecast value. Incidents are detected if the observed occupancy values fall outside the established confidence interval (11).

In their research, Ahmed and Cook tested the application of the ARIMA(0,1,3) model to predict traffic patterns on different freeways. Although some differences exist in the specific form of the time series equation, the general ARIMA model is transferable to different freeways within the system. Ahmed and Cook attributed these differences in specific ARIMA models to variations in flow and specific geometric conditions of particular freeways.

Although occupancy was used in the original developing and testing of the ARIMA model, there is no theoretical limitation to other traffic parameters (such as volume or speed) being used in the algorithm. To apply the Box-Jenkins technique in an operational setting, data must first be collected in time series form (i.e., measurements indexed in

28

time). Then using time series statistical techniques, a candidate model that represents the observed time series pattern is developed. The autocorrelation functions (the correlation of a traffic parameter with its own past) and the cross-correlation functions (the correlation of a traffic parameter with another variable's present and past values) are then compared to the candidate model to determine how well the predicted model "fits" the observed data (12).

Ahmed and Cook (11) performed an off-line analysis of the algorithms using 1642 minutes of occupancy observations associated with 50 incidents. These data were recorded for a 2 mile (3.2 km) section of the Lodge Freeway in Detroit. Confidence limits were computed using both parameters estimated from incident-free historical data and parameters that are dynamically estimated from the data in real-time. At a 100 percent detection rate, the false alarm rate was 2.6 percent when constant model parameters were used and 1.4 percent when variable estimates of the model parameters were used. In terms of detection time, the average time to detect an incident using constant-parameter and variable-parameter estimates were 0.58 and 0.39 minutes, respectively.

It should be noted that the ARIMA algorithm was evaluated under heavy and moderate traffic flow conditions (1200-2000 vphpl) only. The literature is unclear on how the algorithm would perform under light volume conditions where the effects of incidents are not as pronounced.

High Occupancy Algorithm

The High Occupancy (HIOCC) algorithm also monitors detector data for changes in traffic conditions over time (7). Developed for use in England, HIOCC inspects occupancy data from individual loop detectors for the presence of stationary or slow-moving vehicles. An alarm is sounded when several consecutive seconds of high occupancy values are observed by the algorithm.

The algorithm examines the individual pulses from the detectors. A computer scans each detector in the system once every tenth of a second to test if the detector is occupied. At the end of each second, the number of times a detector was occupied is computed. The resulting value is termed the instantaneous occupancy. Several

29

consecutive values of instantaneous occupancies are then examined to see if they exceed a predetermined threshold. A threshold value of 10 lasting two or more seconds is equivalent to a loop occupancy level of 100 percent, and an incident alarm is then sounded.

After an alarm has been sounded, the occupancy level is artificially raised to a higher level, usually 90 percent. This is to prevent the alarm from switching on and off due to random fluctuations in traffic. The alarm is ended when the occupancy level falls to the level that existed before the initial alarm was sounded.

An off-line evaluation of the algorithms was performed using queue data from the England and 12 staged incidents in Paris. From the evaluation, it was determined that the detection threshold could be set at 70 percent for two seconds without producing any false alarms. Using a 100 percent occupancy threshold for two seconds, the HIOCC algorithm was successful at detecting all occasions when queues formed at the sites in England and each of the 12 staged incidents in Paris. The response times for the detection of the staged incidents ranged from 20 to 130 seconds.

Smoothing/Filtering Algorithms

As shown in Figure 2-11, loop detector data viewed over time tends to fluctuate with many sharp peaks and valleys. These fluctuations are more pronounced when loop data are compiled over short periods (i.e., less than one minute). Sometimes, the fluctuations are caused by noise in the communication medium, but more often than not, they are caused by random impulses in the traffic stream. It is these fluctuations that are primarily responsible for causing false alarms with most incident detection algorithms. To eliminate false alarms, most algorithms use persistence checks or tests for compression waves to delay sounding an alarm until detection thresholds are exceeded for a specified period. This, however, can cause significant time required to detect an incident.

Smoothing and filtering techniques are designed to remove the short-term inhomogeneities from traffic data that cause false alarms so that the true traffic patterns are "more visible" to the detection algorithm. Smoothing is a mathematical technique (usually an exponential function) for producing a weighted average of a traffic variable.

This approach reduces the impacts or "smooths" the effects of outliers. Filtering algorithms use a linear filter that allows the low-frequency components (i.e., wide fluctuation in a traffic variable characteristic of an incident condition) of the detector data to pass while removing the undesirable high-frequency (i.e., a sharp fluctuation in traffic characteristic or random noise) portions of the detector data. Smoothing and filtering techniques are extremely useful when detector data includes impulse noise that hide incident patterns. Both types of techniques for processing detector data are discussed below.

Exponential Smoothing Algorithms

Exponential smoothing algorithms use short-term forecasting techniques to detect irregularities in a time series pattern of traffic data (13). Using past observations, forecasts
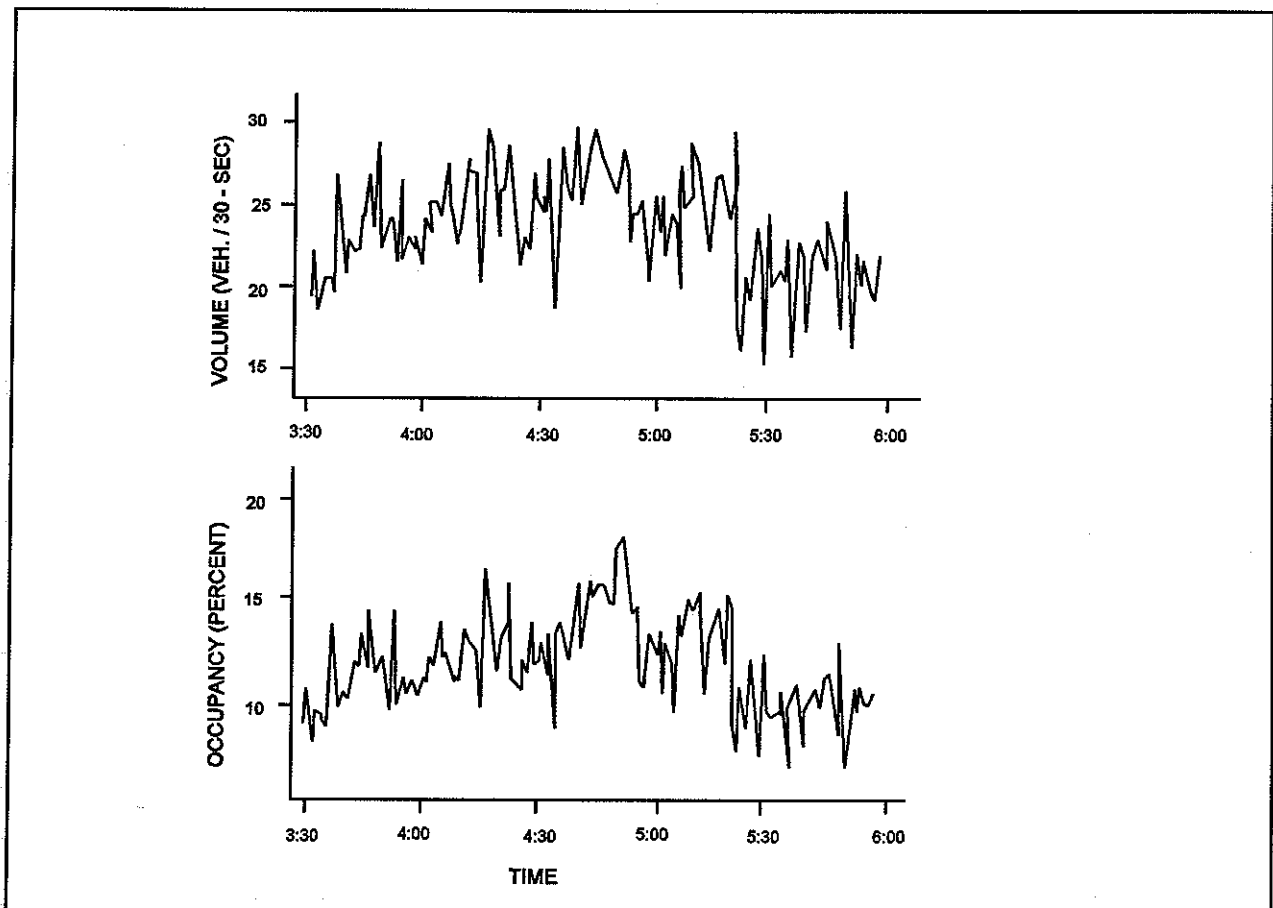
Figure 2-11. Example of Typical Freeway Volume and Occupancy Data (15).

31

of future traffic conditions are made with the more recent observations receiving greater weight than older observations. By using weighted averages of the incoming traffic data, the effects of observed outliers and random fluctuations can be reduced, thereby producing a forecast that more closely resembles the true traffic condition on the freeway.

Mathematically, most smoothing algorithms used for incident detection purposes can be expressed as either as a single or double exponential smoothing function. A smoothing constant is used to affect the degree that past observations influence the forecast value. With a large smoothing factor, more weight is given to the most recent observations. A smaller smoothing constant places less weight on more recent observations, which slows the response of the algorithm to observed changes in detector data.

Incidents are detected using a tracking signal, which is the algebraic sum (to the present minute) of all the previous errors (i.e., the difference between the predicted traffic variable and the observed traffic variable) divided by the current estimate of the standard deviation. Under nonincident conditions, the tracking signal should dwell around zero since the value of the predicted traffic variable should be equal (theoretically) to the value of the measured (or observed) traffic variable. However, when an incident occurs, the predicted traffic variable and the measured traffic variable are not equal, causing the tracking signal to deviate significantly from zero. An incident alarm is sounded when the tracking signal exceeds an established threshold. The threshold can be set either as a function of the variability of the data, or to minimize the likelihood of false alarms.

Cook and Cleveland (13) applied an exponential smoothing technique to develop a total of thirteen incident detection algorithms These algorithms use control variables derived from traffic measures from either a single detector station (station algorithms) or for two adjacent detector stations (subsystem algorithms). All these variables are direct measures (or can be derived from direct measures) of one-minute averages of volume, occupancy, and/or speed from loop detectors.

These algorithms were evaluated using a total of 50 lane blocking incidents (including 18 accidents, 28 stalls and breakdowns, two instances of debris on the roadway, and two short-term maintenance operations) from the Lodge Freeway in Detroit. In only one of these incidents was more than one lane blocked, and the freeway was never

32

completely blocked. In two-thirds of the cases, the lane next to the median, where there was no shoulder refuge for vehicles, was blocked. The average duration of the blockages was 6.1 minutes, with times ranging from 1 to 19 minutes.

Of the thirteen algorithms studied, Cook and Cleveland (13) found that the three best exponential algorithms were the station occupancy, station volume, and the station discontinuity algorithms. Overall, the exponential station occupancy algorithm performed better than all the other algorithms evaluated, detecting 46 of the 50 incidents (92%) at a false alarm rate of 1.87 percent and a mean detection time of 0.74 minutes after the onset of congestion. All 50 incidents were detected at a 6 percent false alarm rate. In terms of detection time, the station occupancy algorithm experienced shorter detection times than any of the other algorithms evaluated. Detection times varied from 0.35 to 1.46 minutes depending upon the false alarm rate.

Low-Pass Filter

Filtering algorithms mathematically remove inhomogeneities from incoming detector data to produce a smoothed moving average of the measured traffic variable (in this case loop occupancy) (14, 15). The filter (called a low-pass (LP) filter) removes the sharp fluctuations (or high-frequency components) that are characteristic of noise in the data while allowing the wide fluctuations (or low-frequency components) typically associated with incident conditions to "pass" through the filter. The filter takes the form shown in the following equation:

$$y_t = \sum_{k=0}^{M} \frac{1}{M+1} x_{t-k}$$

where,

y_t = the smoothed or filtered traffic variable,

x_{t-k} = the observed traffic variable in t-k intervals, and

M = the maximum number of intervals over which the data is filtered.

An example of the effects of filtering detector data is shown in Figure 2-12.

33
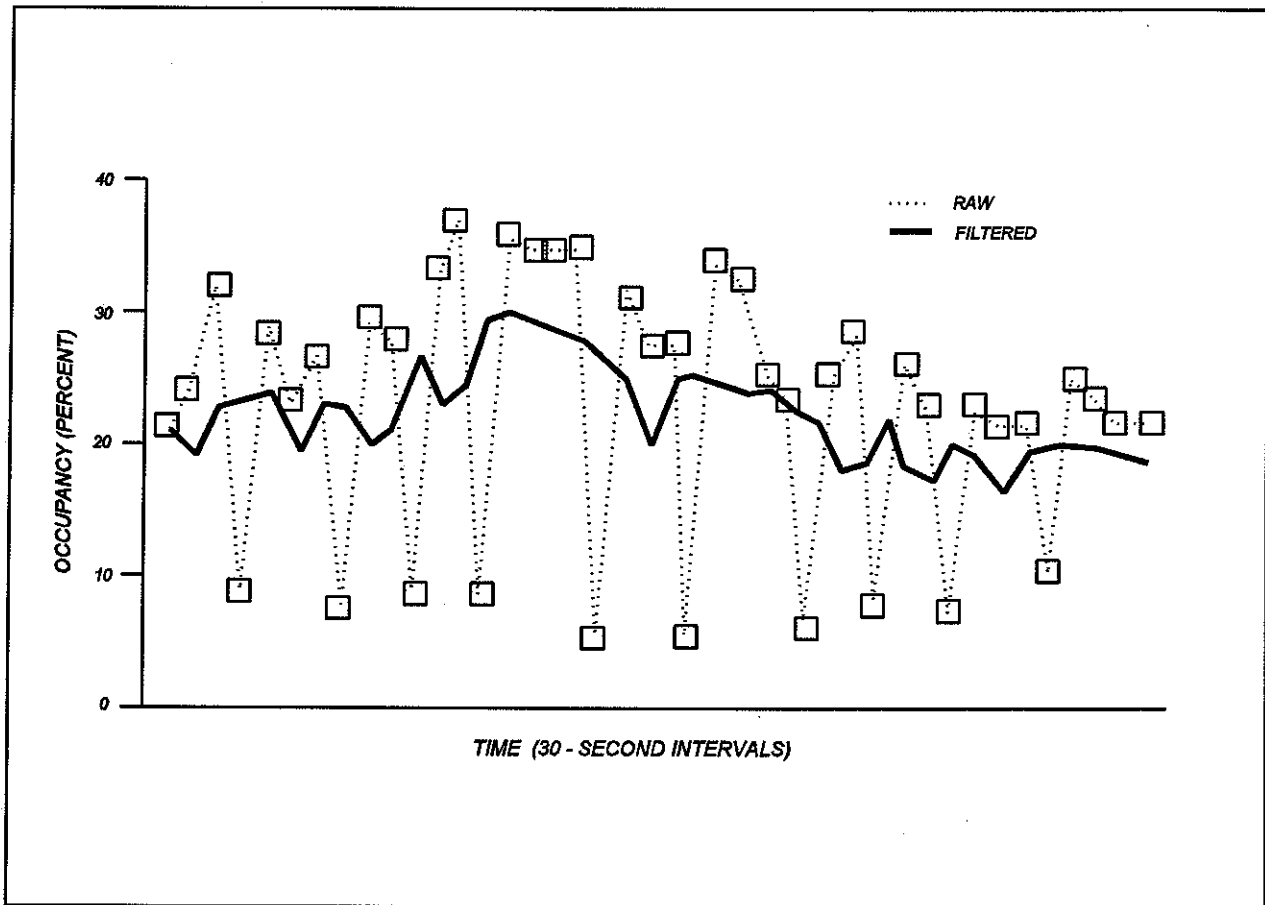
Figure 2-12. Effects of Using a Low-Pass Filter on Detector Data (15).

Stephanedes and Chassikos (14, 15) use this technique to develop an incident detection algorithm. The algorithm is based on a simple comparison of the occupancy levels at two adjacent loop detector stations. Using occupancy data compiled every 30 seconds as an example, a low-pass filter is applied to the difference in occupancy between two adjacent detector stations to obtain a 3-minute moving average. Since all random fluctuations have been theoretically removed by the filter, a high value of the filtered occupancy should be indicative of congestion caused by either a bottleneck or an incident. To distinguish between incident and bottleneck congestion, a second filter is used. The second filter is designed to examine an additional 5-minute time average of the spatial difference in occupancy prior to the first three minutes.

Stephanedes et al. (15) compared the performance of the filtering model with the performance of the California-type algorithm (both the basic California and Algorithm #7),

34

the SND model and the double exponential smoothing algorithm. Operating characteristic curves depicting the detection and false-alarm rates accomplished by the algorithms at specific threshold values were developed. A total of 140 hours of traffic data from 5.5 miles (9 km) of freeway in the Minneapolis areas was used. Thirty-second occupancy and volume data were obtained from 14 detector stations located in the study area. The data set contained a total of 27 capacity-reducing incidents.

At every detection rate, the performance of the filtering algorithm was superior to that of the California-based algorithms. At an 80% detection rate, the filtering algorithm achieved a false alarm rate of approximately 0.3%, whereas Algorithm #7, the next best performing California-based algorithm, achieved a 0.6% false alarm rate. Stephanedes reported that the filtering algorithm also achieved comparable mean detection times. Although the structure of the algorithm imposes a three minute delay, the detection times were within one minute of the other algorithms. The main limitation of the algorithm is that it cannot separate other traffic phenomena, (such as compression waves) that can also create temporal changes in the traffic stream, from incident data.

Traffic Models

Traffic modeling approaches for detecting incidents use complex traffic flow theory to describe the behavior of traffic during incident conditions. Models are used to predict the performance of traffic under incident conditions. Algorithms then compare observed traffic parameters to traffic parameters predicted by the model. The two algorithms that use this approach are the Dynamic model and the McMaster incident detection algorithms.

Dynamic Model

One reported problem with many existing incident detection algorithms is that they do not account for the dynamic nature of traffic. To address this problem, Willsky et al. (16) developed an algorithm that uses macroscopic traffic flow models to capture the dynamic nature of freeway traffic. At the heart of the algorithm is the fundamental velocity-density and flow-density relationships depicted in Figure 2-13. The algorithm assumes that traffic flow can be modeled using these relationships.
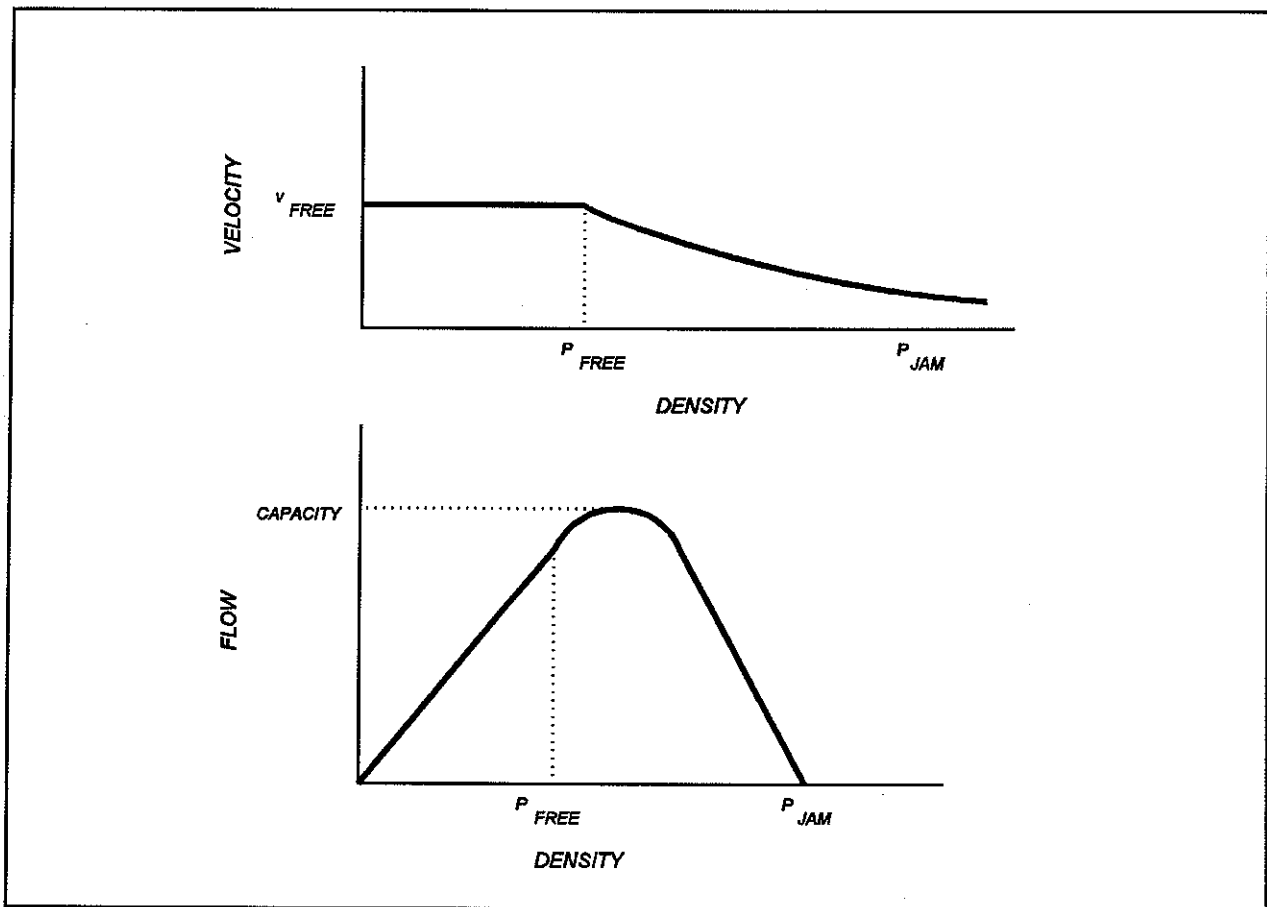
Figure 2-13. **Fundamental Traffic Flow Relationships Used in the Dynamic Model Algorithm (16).**

The algorithm uses two statistical hypothesis testing techniques for examining the flow-density relationships in observed traffic data: the Multiple Model (MM) method and the Generalized Likelihood Ratio (GLR) method. The MM method is used to identify a linear system of equations that represent traffic flow conditions on a freeway. Using these equations, the conditional probability of the validity of the observed data "fitting" a flow-density model indicative of incident conditions is determined. The value of the conditional probabilities is used as the control measure for detecting incidents. A high conditional probability implies that the observed traffic data indicates that an incident has occurred on the freeway.

Incident conditions are also detected monitoring detector data for abrupt system changes. The algorithm assumes that abrupt changes in the freeway system (such as

36

those caused by incidents) follow a predictable pattern (or "signature") in a stream of detector data. To detect system changes, the algorithm uses the GLR, which measures the likelihood that the observed flow-density pattern is indicative of an incident condition, as the control variable. Incident conditions are said to exist on a freeway when the maximum likelihood ratio exceeds a specified threshold.

This algorithm is based on a dynamic theoretical model of traffic flow developed by Payne (17). The model, designed to capture both the flow fluid and car-following aspects of freeway traffic, is used to describe the relationship between velocity, density, and flow. To use the algorithm, estimates of these parameters are obtained from detector data. Unfortunately, presence detector data provide time-averaged information about travel conditions at a fixed location. Therefore, measured loop detector data must be converted from a time-based average to a spatial-based average. Willsky et al. provide procedures for converting loop detector data to spatial averages.

The performance of the algorithm has been tested using only simulated traffic conditions. The performance of the algorithm was evaluated over a wide range of traffic flow (900 vphpl to 2000 vphpl) and detector noise conditions. Under these simulated conditions, the algorithm performed relatively well. No false alarms or incorrect detections were observed. The response time of the detection system was also relatively small. However, the algorithm has not been tested using real detector and incident data.

Mc Master Algorithm

The McMaster algorithm is a single-station incident detection algorithm (18, 19, 20). It uses the speed-flow-occupancy relationship to determine when traffic conditions change at a detection station. It is based on the premise that while speed experiences a sharp change when traffic conditions move from uncongested to congested conditions, flow and occupancy change smoothly. Therefore, the algorithm uses historical data from a detector station to determine the flow-occupancy relationship as traffic operation change from uncongested to congested flow. It was derived based on observations by Persaud and Hall (19) that found the relationship between flow and occupancy (or volume and occupancy) clustered tightly about a line. This line can be used to identify when traffic operations on a freeway transition from uncongested to congested flow.

VOLUME (VEH. / 30 SECS)

35

30   STATE 1   STATE 4

25

20   g(OCC) V_{CRIT}

15

10   STATE 3

5   STATE 2

0   OCC $_{CRIT}$

0   10   20   30   40   50   60   70   80   90   100

30 - SECOND OCCUPANCY (%)
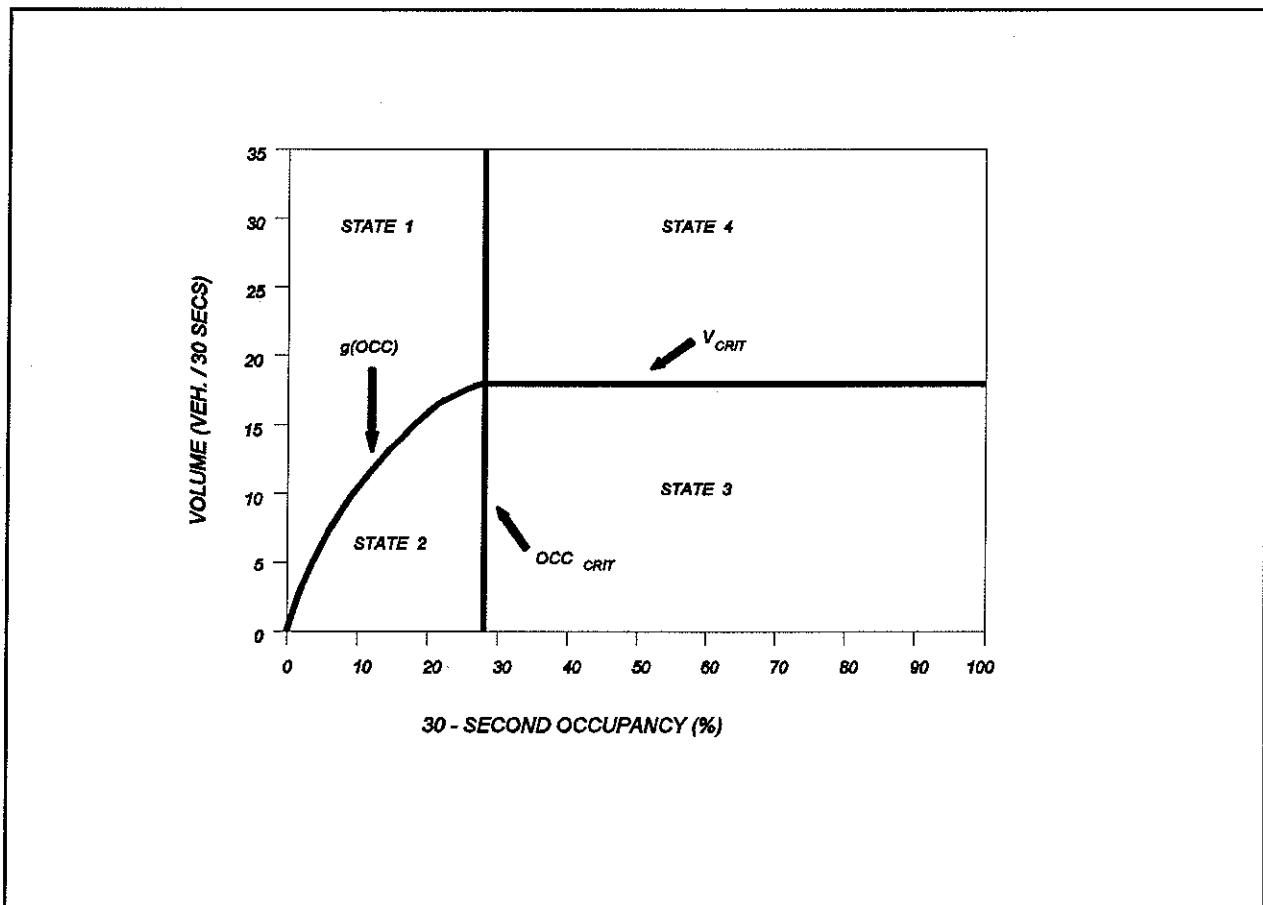
Figure 2-14. Flow-Occupancy Template for McMaster Algorithm (18).

The algorithm assumes that traffic operations at a single detector station can be classified into states based on volume and occupancy measurements made at the station. Figure 2-14 illustrates a typical volume-occupancy template that is used to determine traffic states in the algorithm. The template is composed of four areas, which are divided by the lower bound of the uncongested data (LUD), the critical occupancy (OCRIT), and the critical volume (VCRIT). Area 1 (the area above the LUD curve and to the left of OCRIT) defines an uncongested traffic state (i.e., high flow rates with low occupancies). The area below the LUD and VCRIT curves and to the left of OCRIT (Area 2) represents congested traffic flow conditions while the area to the right of OCRIT and below VCRIT (Area 3) represents traffic conditions that are heavily congested. The area to the right of OCRIT but above VCRIT (Area 4) reflects traffic operations that might appear downstream of a permanent bottleneck in a section of freeway operating at or near capacity.

To detect incidents, the algorithm employs two tests. The first test is used to determine whether traffic at a detector station is congested. Raw loop detector data are compared against the appropriate template developed for that particular station. If traffic conditions fall below the LUD curve (i.e., into Areas 2 or 3) for longer than three consecutive intervals (30 seconds each), the station is considered congested. The logic used to determine the state of traffic at a detector station is shown in Figure 2-15.

If the algorithm detects congestion at a station, it then attempts to identify the cause of the congestion by evaluating the traffic state at a downstream detector station. If traffic conditions downstream of the detector station are relatively clear (i.e., in Areas 1 or 2), then it is likely that an incident happened between the two detector stations. The logic used in the algorithm for determining the cause of congestion at a detector station is shown in Figure 2-16.

The algorithm uses volume and occupancy measurements from a single detector station to identify traffic conditions on the freeway. Raw measurements of flow and occupancy are directly compared to template values for each station. Although the algorithm was initially developed to use 30 second flow and occupancy values, there is no theoretical reason data compiled at a different rate cannot be used in the algorithm.

To calibrate the algorithm, the LUD curve, OCRIT, and VCRIT must all be defined. The LUD curve is calibrated manually with approximately three days of incident-free data. A standard quadratic function is used to fit the LUD directly to the flow-occupancy boundary. Visual inspection is used to determine if any aspects of the curve needs to be modified (intercept, slope, curvature). Once the curve has been established, the relevant coefficients for the equation are then adjusted. While the procedure is not easily automated, experience has shown that proper calibration of a station can be accomplished in less than two hours (20).

The other parameters (VCRIT and OCRIT) are also decided manually. OCRIT is defined as the occupancy at which the highest observed volume occurred. To properly establish VCRIT, recurrent congestion must occur at a detector station.

Both off-line and on-line evaluations of the performance of the McMaster Algorithm have occurred and were reported in the literature (18). The off-line evaluation used 39

39
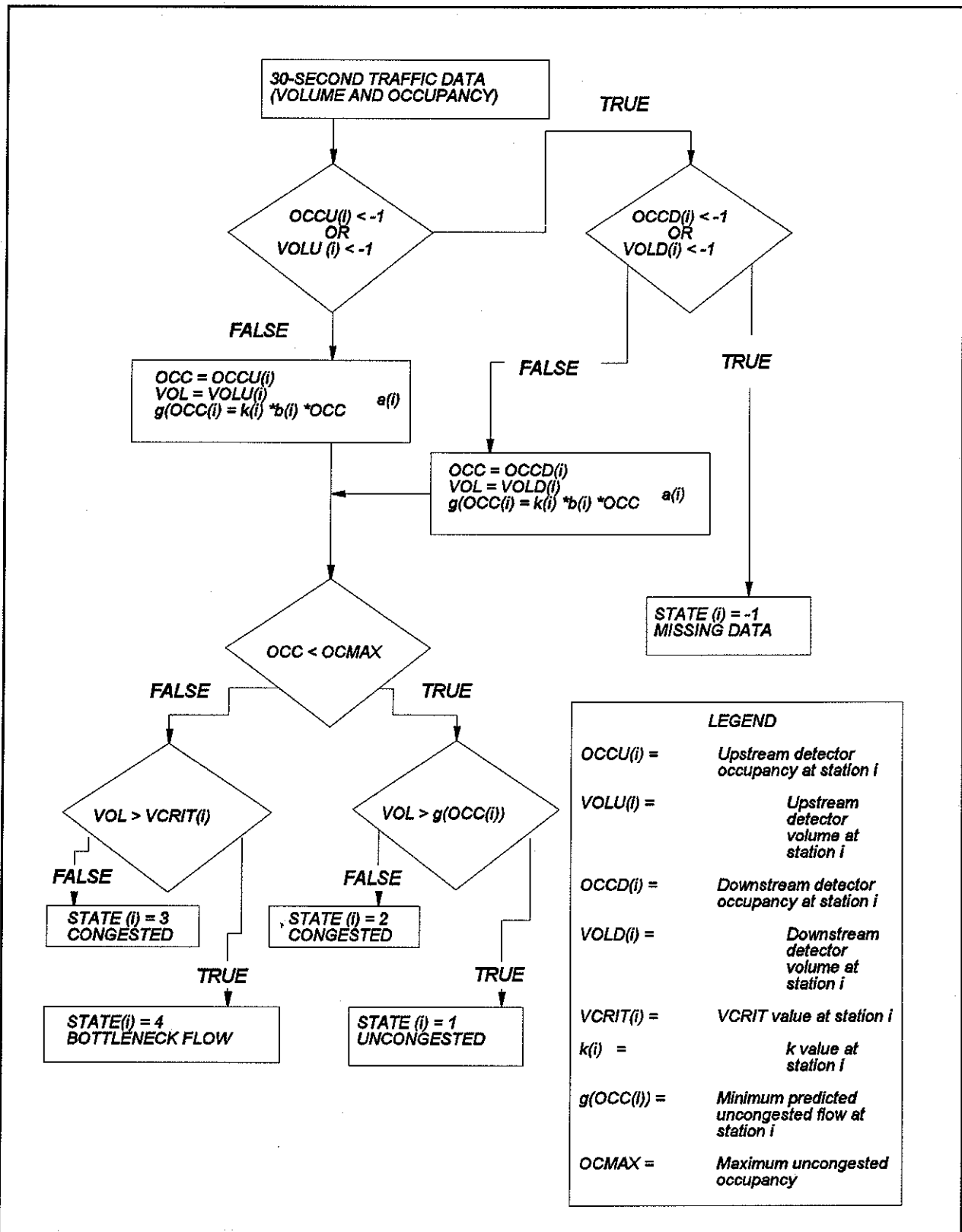
Figure 2-15. Logic for Determining Traffic States with McMaster Algorithm (18).
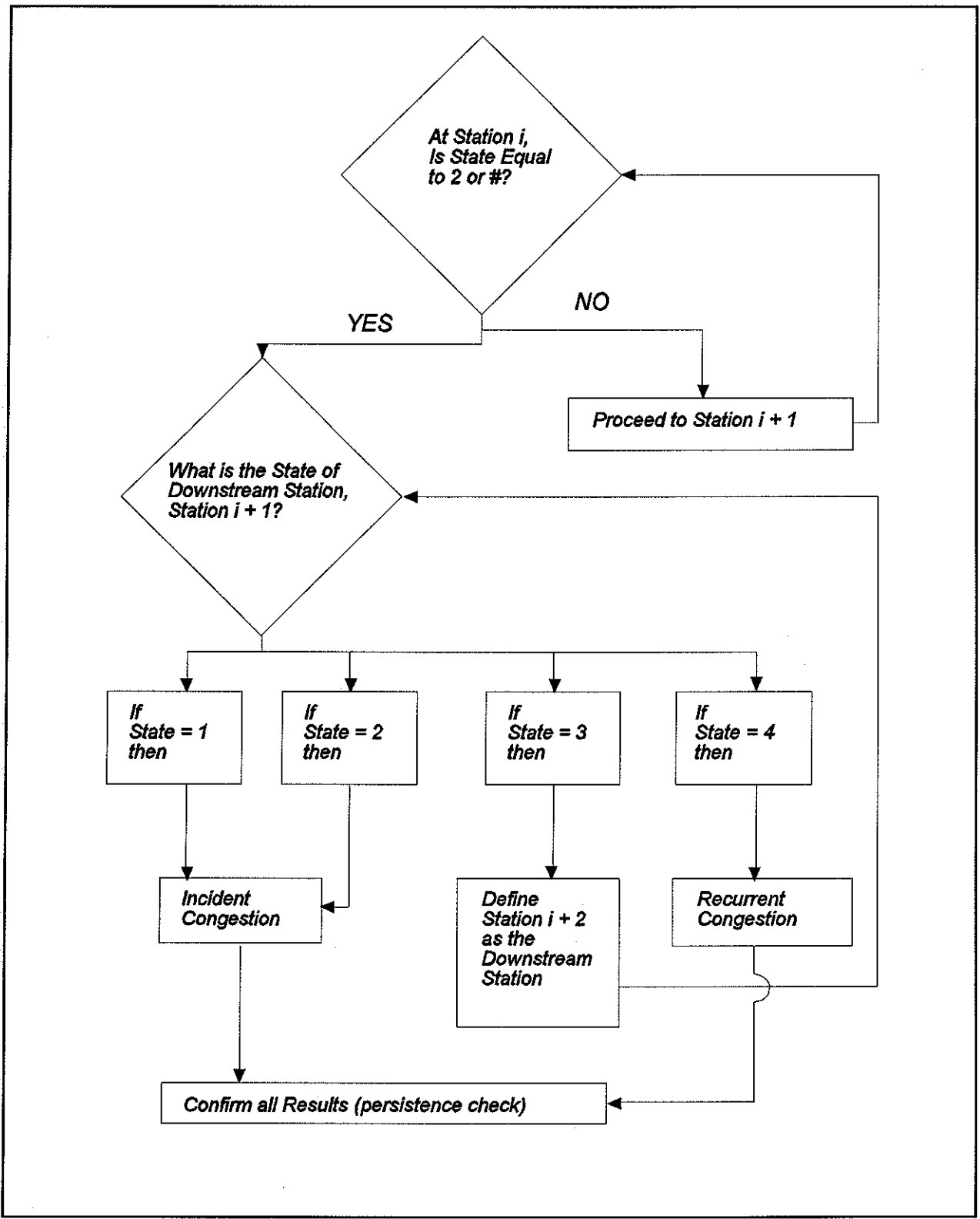
Figure 2-16. Logic used in the McMaster Algorithm for Determining the Cause of Congestion ([18]).

days of data from the Mississauga Freeway Traffic Management System (FTMS). In these 39 days, a total of 28 incidents were detected by control center personnel. The algorithm detected 15 of the 28 incidents (a detection rate of 62 percent). By deleting seven incidents that the author claims had no affect on traffic, the detection rate was 88 percent. The average detection time for these incidents was 2.2 minutes. The reported false alarm rate was 0.0012 percent.

On-line testing of the algorithm was also conducted using data from the Mississauga FTMS for a total of 64 days. During this time, the operators reported 230 incidents. All but 28 of the incidents were not included in the evaluation because they did not have a significant impact on traffic. Of the 28 remaining incidents, nineteen were successfully detected by the algorithm for a detection rate of 68%. The mean detection time for all incidents was 2.1 minutes. The average detection time for the lane blocking incidents was 1.4 minutes. Similar false alarm rates as those reported in the off-line evaluations were achieved during the on-line evaluation.

Low-Volume Incident Detection Algorithms

Most of the existing algorithms reported problems detecting incidents under low volume conditions. This is because most algorithms are monitoring traffic data for flow discontinuities, queues, or congestion that result when the capacity of the freeway is reduced below demand levels. However, incidents that occur during low volume conditions, such as those that occur late at night between the hours of 1:00 a.m. and 5:00 a.m., seldom reduce the capacity below demand levels. As a result, incidents that occur during low volume conditions seldom generate the level of congestion and queuing that is typically associated with incidents that occur at medium or high traffic volume conditions, and the same general concepts that are used to detect incidents during heavy traffic conditions may not be applicable during light traffic conditions.

Several algorithms have been designed specifically for detecting incident under low volume conditions. One algorithm, developed by TTI, uses an input-output analysis of individual vehicles on section of freeway to detect incidents during light flow conditions (21). The algorithm is based on the time and speed of vehicles entering to predict an exit

42

time of vehicles in a section of freeway. Exit times are predicted using the following equation:

$$t_e = t_i + d/v$$

where,

t_e = the time (in seconds) of the vehicle exiting the freeway section,
t_i = the time (in seconds) of the vehicle entering the freeway section,
d = the length of the freeway section, and
v = the speed of the vehicle as it enters the freeway section.

The algorithm assumes that the speed of the vehicle remains constant as it travels through the freeway section.

As vehicles enter a freeway section, the earliest and latest times that they are expected to arrive at the downstream detector station are determined. Vehicles are placed in one of three accounting intervals based on their projected arrival times. All vehicles whose projected arrival times overlap are placed in the same accounting interval. Each vehicle that exits the freeway section after the earliest projected arrival are counted. When the time-of-day equals the latest projected arrival time, the exit count is compared to number of vehicles assigned to the counting interval. If the exit count is less than the projected number in the accounting interval, an incident is declared. If the exit count is equal to the projected number in the accounting interval, no incident is detected. An unknown situation is declared when the number of exiting vehicles is greater than the expected number for that accounting interval.

The performance of this algorithm was evaluated using five days of data from I-610 North in Houston, Texas. The algorithm was evaluated over a range of traffic volumes (from 100 vph to 1200 vph). The effects of detector station spacing were also examined. Staged incidents were used to evaluate the algorithm. The evaluation found that the algorithm achieved a detection rate between 49 and 78 percent, depending upon the spacing of the detector stations. At lower volume levels (less than 400 vph), the false alarm rate was one per 7 hours of operation. At higher volume levels (between 900 and 1200 vph), the false alarm rate increased to one per 2 hours of operation.

43

A similar approach has been proposed for detecting incidents in the Lincoln and Holland tunnels leading into New York City (22). In the tunnels, lane changing is prohibited and only a small amount actually occurs. Under normal light volume conditions, less than 1 percent of the vehicles can be expected to change lanes. However under incident conditions, it is reasonable to expect that some motorist will change lanes to avoid being delayed. Using these assumptions, an incident detection algorithm was developed that monitors the lanes in which individual vehicles entered and exited the tunnel. Primary indicators that an incident has occurred in the tunnel are the number of vehicles that have changed lanes and the amount of delay individual vehicles experience in the tunnel. Ultrasonic detectors or automatic vehicle identification systems have been proposed to track individual vehicles. Unfortunately, this concept has not been tested in an operational setting.

Advanced Incident Detection Techniques

Several innovative approaches for detecting incidents have also been developed. These approaches use advanced detection technologies and computer programming languages to aid in detecting incident conditions on freeways. While these approaches provide promises for improving incident detection capabilities, they are beyond the scope of this report and are only introduced here to provide completeness.

Artificial Intelligence

Artificial intelligence is an approach used by computer scientists to emulate the human thought process using computational models (23). Artificial intelligence is a mechanism for including inexact reasoning and uncertainty in complex decision-making processes. Because of the complex and dynamic nature of traffic, the application of artificial intelligence for detecting incidents has been explored by several researchers (24, 25, 26).

Two general artificial intelligence approaches have been considered for incident detection: Fuzzy Sets and Neural Networks. Fuzzy sets provide a mechanism for applying inexact or imprecise data to a set of rules, such as threshold values in an incident

detection algorithm. Unlike classical algorithms that require strict (or crisp) adherence thresholds, fuzzy set algorithms allow data that is close (but does not exceed) thresholds to be considered in the detection decision. Therefore, fuzzy sets allow decisions to be made even though data may be inexact or missing. The ability to make decisions based on incomplete data has the potential to significantly improve the performance of many incident detection algorithms.

Neural networks are used to simulate the knowledge reasoning of the human brain. Like the human brain, a computer neural network consists of interconnected elements (called neurons) working in parallel. The neurons not only receive input from other neurons but also communicate its output to other neurons. Because different "paths" can be taken to reach a final decision, the step-by-step processing normally associated with most incident detection algorithms is no longer required. Neural networks also have the ability to "learn" from past trial-and-error processes. Consequently, the potential for improving detection capabilities in an incident detection system is great. Recent research has shown the application of neural networks for detecting incidents to be very promising, particularly with respect to limiting the number of false alarms that typically occur with other approaches for detecting incidents.

Automatic Vehicle Identification Systems

Automatic Vehicle Identification (AVI) systems have also been proposed for detecting incidents on freeways. With AVI, vehicles are equipped with transponders. Each transponder is encoded with a unique identification number. Reading devices are installed either over or next to the freeway. As vehicles pass the reading devices, their identification numbers are broadcast to the readers. By installing multiple reader stations, a vehicle can be tracked as it travels the freeway. Incidents can be detected by monitoring how long it takes for vehicles to travel a section of freeway compared with the expected travel time. This approach has been proposed in many cities in the United States such as Houston, Texas (27).

Video Image Processing

Another approach for detecting incidents that has received considerable attention lately is Video Image Processing (28). With video image processing, measures of traffic

45

performance (such as traffic volumes, traffic densities, queue lengths, etc.) are automatically extracted from a video image using a computer program. Video image processing units can be used in two ways to detect incidents. First, the image processing unit can be used as a loop detector station to provide volume and/or occupancy counts that can be used in conventional incident detection algorithms. The second approach requires the computer to interpret the entire video image to find stationary or slow-moving vehicles. Current leaders in the application of video image processing include the University of Minnesota and Washington State Department of Transportation.

Summary

As discussed above, numerous algorithms have been developed to automatically detect congestion and lane-blocking incidents in freeway surveillance and control systems. These algorithms use a variety of techniques for detecting incidents ranging from simple comparisons of measured traffic relative data to preestablished thresholds to theoretical traffic flow models to predict future traffic conditions based on current observations. Most of these algorithms have been developed and evaluated off-line, using recorded loop detector data from incident and nonincident conditions. Relatively few have been used in an actual operational capacity. Therefore, most remain untested in detecting incidents using live (or on-line) loop detector data. Substantial differences can exist between testing an algorithm in an off-line situation and using an algorithm to detect incidents in a real-world situation. Because of the differences that can exist between theoretical and practical applications, it is important to find out what incident detection algorithms are being used in actual operating freeway surveillance and control centers. The next chapter presents findings of site visits to selected freeway surveillance and control centers in the United States and Canada to determine the use and effectiveness of incident detection algorithms.

3. SITE VISITS TO SELECTED FREEWAY MANAGEMENT SYSTEMS

As part of this research, site visits were conducted at the following freeway management systems:

- Los Angeles, California
- Northern Virginia
- Minneapolis, Minnesota
- Toronto, Ontario
- Seattle, Washington
- Long Island, New York
- Chicago, Illinois

The purpose of the site visits was to obtain in-depth information as to the type and performance of the computer algorithms being used to detect incidents in these freeway management systems. Four of the above sites (Los Angeles, Northern Virginia, Chicago, and Toronto) are currently using algorithms to detect incidents. The other locations (Seattle, Long Island, and Minneapolis) have all discontinued algorithm usage. Site visits to these locations provided insight into why incident detection algorithm usage was discontinued in these freeway management centers.

Another primary objective of the sites visits was to determine, through observation, the role and usefulness of the incident detection algorithm as part of the overall incident detection and management system at these locations. It was felt that a more realistic representation of the performance of the algorithms could only be obtained by actually observing the operations of the control center.

This chapter provides a summary of what was learned from the site visits. Observations from each center visited are provided. General conclusions and comments that can be drawn from the site visits are provided at the end of this chapter.

Los Angeles, California

The freeway surveillance and control system monitors over 264 miles of freeway in the Los Angeles area. It operates 24 hours a day and is staffed by at least two California Department of Transportation (Caltrans) employees and one California Highway Patrol (CHP) officer. The primary responsibility of the Caltrans employees is to operate the ramp

metering and incident management systems. The CHP officer acts as a liaison to coordinate incident response measures between CHP and Caltrans. The officer also monitors CHP's computerized dispatching system (there is a terminal located in the control center) and alerts the Caltrans operators of incidents reported to the dispatch center.

The primary means of obtaining data from the freeways is through loop detectors embedded in the pavement. A single loop detector embedded in each lane provides volume and occupancy data. The spacing of the detectors varies from ½ mile in the core area to one mile or more in the outlying areas. Occupancy and volume data are compiled by Type 170 controllers in 30 second intervals. An average occupancy and volume level is calculated for each detector station. The average occupancy at each detector station is then smoothed with two minutes of previous data.

A wall-sized electronic map and computer graphics displays are used to show the operating conditions of the freeways currently under surveillance. Different colors are used to display the current speed of traffic traveling over the detector stations. The following color codes are used:

- Green -- speeds > 35 mph
- Yellow -- speeds between 20 mph and 35 mph
- Red -- speeds < 20 mph

A flashing red light is used to show when a potential incident has been detected at a station.

Currently, only a small portion of the freeway system is covered with CCTV surveillance. At the time of the site visit, only four CCTV cameras were operational. These cameras were placed at select interchanges that were known problem areas. Caltrans is currently in the process of installing additional CCTV cameras in their system, but only on a limited scale (a total of 17 cameras will be included in the system).

Incident Detection Algorithms

The surveillance and control software has been designed so that one of the following strategies for detecting incidents can be employed:

48

- One algorithm with a single set of threshold values to detect incidents in the entire surveillance area,
- Different algorithms and corresponding threshold values can be used to detect incidents on different freeways or segment of freeways in the surveillance area, or
- Different algorithms and corresponding threshold values can be used to detect incidents in individual zones (a zone being defined as two adjacent detector stations).

Although the same algorithm is used throughout the surveillance area, incident detection is performed on a zone-by-zone basis with threshold values calibrated to specific zones. A flow chart of the automatic incident detection process is provided in Figure 3-1.

Caltrans is currently using two different algorithms in their freeway surveillance system. The algorithms are selected based on measured traffic conditions that exist throughout the surveillance area (29). During periods when traffic is heavy (essentially all daylight periods), Caltrans uses the modified California Algorithm #8 which tests for the presence of compression waves in the traffic stream. During lighter traffic conditions (i.e., late night), Caltrans uses the modified California Algorithm #5 with a three minute persistence check. Decision trees for both of the algorithms are shown in Appendix A.

Currently, both algorithms are operating in their original form (29). No in-house modifications have been made by Caltrans. Although the operators are aware that other incident detection algorithms and theories exist, they currently do not have operational experience with any of these other algorithms.

Once an incident has been detected by the algorithm, it is assigned a log number and priority by the computer (29). Even though the incident has been logged, it is not immediately displayed to the operator as a potential incident. Incident conditions must exist in a zone for a minimum of six cycles (three minutes) before an alarm is displayed to the operator. Adding in the time used by the algorithm, then, the actual detection time could be five to eight minutes.
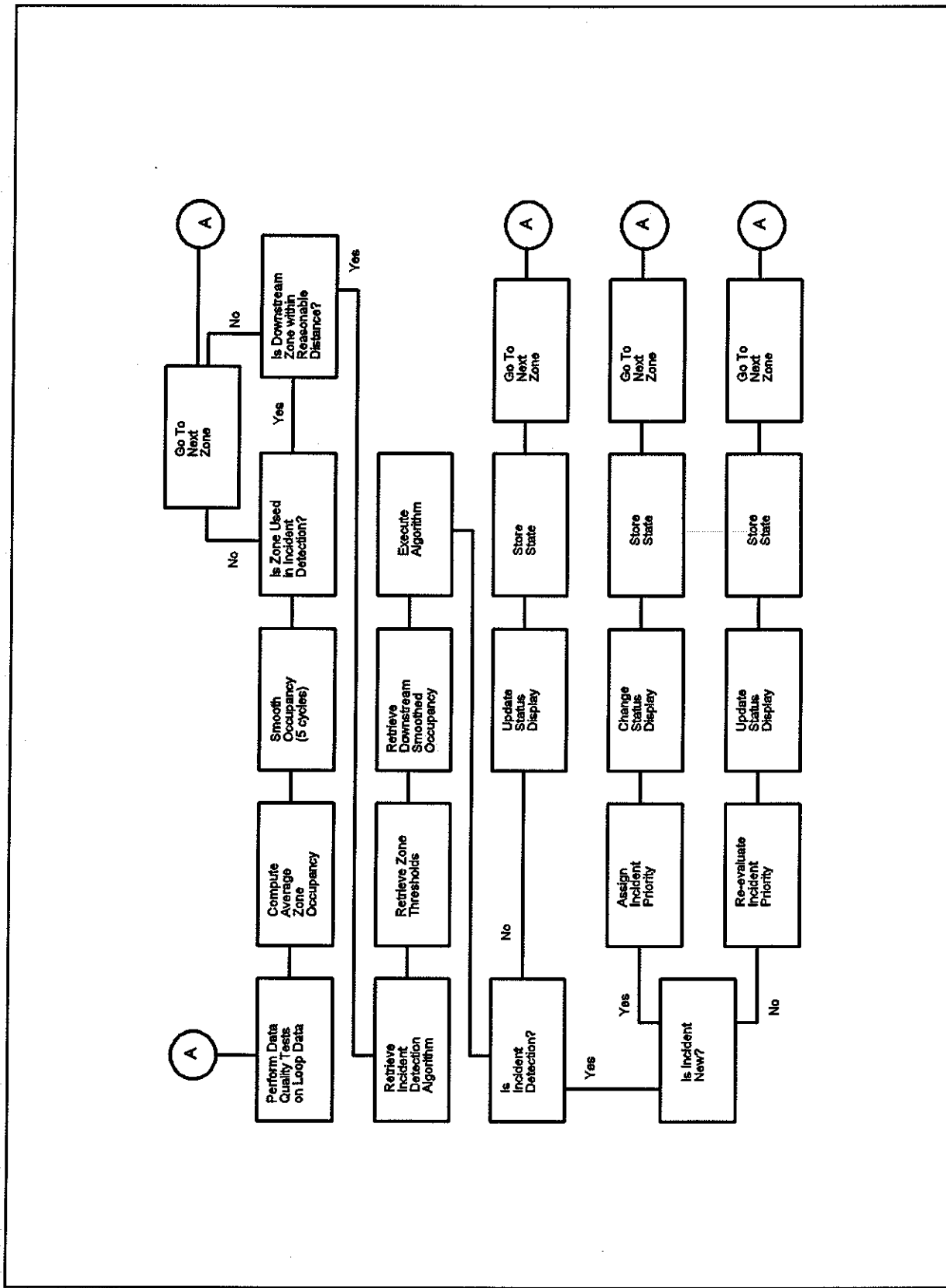
Figure 3-1. Los Angeles Automatic Incident Detection Process.

Severity is estimated by the amount of reduction in capacity that occurs because of the incident. The reduction in capacity is estimated by evaluating the relative difference in the occupancy levels of the upstream and downstream detector stations with respect to the upstream detector station. Nine user-defined threshold values are employed to establish incident priorities. For example, an incident that results in a reduction in capacity of between 90% and 100% is given a Severity 1 rating. A Severity 2 incident is given to an incident that reduces capacity between 75% and 90%. The severity index is used to assign response priorities for the incident management team.

General Observations

In Los Angeles, not all capacity-reducing events are classified as incidents. Minor accidents and stalls that are located on the shoulder are considered part of normal freeway operations. Caltrans policy defines an incident as an event that blocks a lane of traffic for more than two hours. An incident response team is dispatched when requested by CHP or when the incident is anticipated to block a freeway lane for more than two hours. Therefore, the operators, for the most part, do not appear to rely heavily on the incident alarm display and the map display to respond to incidents. The operators rely mainly on the CHP officer and maintenance radio dispatchers to alert them to the presence of incidents.

Seattle, Washington

Traffic conditions on the freeways in the Seattle area are monitored through a system of loop detectors placed in each lane at each detector station. On the average, detector stations are spaced every ½ mile. Each station accumulates loop occupancy and volume data for a 20-second interval. A one-minute moving average of the loop occupancy and volume data is then computed using three consecutive 20 second intervals.

Besides loop detectors, a total of 55 CCTV cameras provide surveillance on approximately 35 miles on I-5, I-90, and SR 520 in the Seattle area. The video images are displayed to operators through a bank of video display terminals in the control center. The

video is used to visually inspect the operations of the various facilities and to verify incidents that are reported by local radio stations, the State Highway patrol, and Washington State Department of Transportation (WsDOT) maintenance forces. The control center also relies heavily on the CCTV surveillance system for detecting incidents.

Loop detector data are transmitted back to the central control center and displayed on a color-graphics terminal. The display shows the level of congestion on the freeways in the Seattle area. Color codes are used to display congestion levels. A green indication over the freeway is used to display free-flowing traffic. Moderate congestion is displayed as a yellow band while heavy congestion is displayed as a red indication. A flashing red indication is used to display stop-and-go traffic and incident locations.

Incident Detection Algorithm

When the system was originally activated in 1981, WsDOT used a modified version of the basic California Algorithm (30). The version that was used was developed in-house and performed the following three comparisons in sequence:

- The difference in loop occupancy levels between upstream and downstream detector stations was compared to a preset threshold value (OCCDF),

- The relative difference in the occupancy levels of the upstream and downstream detector station was compared to a second threshold value (OCCRDF),

- The occupancy level of the downstream detector station was compared to a third threshold value (DOCC).

An incident alarm was sounded if all three of the threshold values were exceeded. A diagram depicting the algorithm logic is shown in Figure 3-2 (30).

Figure 3-2. Decision Tree for Incident Detection Algorithm Used in Seattle.

Currently, though, WsDOT is not using an algorithm to detect incidents in the surveillance area (30). It was felt that the algorithm produced too many false alarms and that other means of detecting incidents were more accurate and faster. Under the current system design, the primary means of detecting incidents in the Seattle area include the following:

- a police computer-aided dispatching (CAD) terminal located in the control center,
- the CCTV system,
- the monitoring of radio scanners, and
- WsDOT maintenance crews traveling the freeway network.

When the algorithm was used, specific threshold values were developed for each detector zone (30). Operational experience with the algorithm showed that roadway geometry appeared to influence the effectiveness and performance of the incident detection algorithm.

WsDOT also experienced problems with calibrating the algorithms (30). It was felt that the algorithm could not be properly calibrated unless an incident occurred in the particular detection area. Since not all detection zones experienced an incident when the algorithm was operational, WsDOT felt that the algorithm was never properly calibrated.

General Observations

At the time of the site visit, WsDOT was in the process of upgrading their computer system and relocating their control center to a new location. The new control center was expected to greatly expand the control functions and surveillance capabilities of the operator. In addition, district dispatching personnel would be physically located in the new control center. Since maintenance forces are one of the primary means of not only detecting but also responding to major incidents, it was expected that the physical presence of the dispatchers in the same area as the control center operators will greatly improve incident detection capabilities and response efficiency.

54

Although WsDOT is currently not using an incident detection algorithm in their system, they anticipate reinstating an incident detection algorithm in their system in the future. They believe that the algorithm could eventually be an important tool in their overall incident management system.

Northern Virginia

The general philosophy of incident detection in the Northern Virginia system is to use an algorithm to identify regions of congestion and then decide, through visual inspection with their CCTV system, whether the congestion is a result of an incident or whether it was caused by a normal bottleneck condition (31). If an incident is the cause of the congestion, its location is identified and the capacity of the incident is calculated for use by the ramp metering control and advisory message sign algorithms. If the congestion is a result of a bottleneck condition, the algorithm then calculates the capacity of the bottleneck and uses this value in the ramp metering control algorithm. A computer algorithm is also used to decide when incidents and bottleneck congestion end.

Incident Detection Algorithm

The Virginia system also uses a modified version of the California Algorithm, although not one of the ten modified versions of the algorithm referred to earlier (31). The algorithm was developed by Sperry Systems Management and has two specifically added features. The first feature is that the operator is required to manually enter when an incident has cleared the travel lanes, even though the algorithm contains a test for determining when an incident terminates. This feature was added as a safeguard against the system from falsely indicating that the incident has terminated. A false indication can occur when ramp metering and advisory signing reduce the demand at an incident site to a level that is below the capacity of the incident, thereby clearing the congestion. The other feature that has been added to the algorithm is the ability to use historical data in the algorithm computations if the operator has to take a detector station off-line because of malfunctions.

The detection algorithm consists of two modules: one for detecting incidents and another for identifying bottleneck congestion locations. It differs from the basic California algorithm in that it does not include a test of the relative difference in the occupancy levels between two detection station with respect to time (i.e., DOCCTD). In order for an incident to be declared, the operator must manually confirm the presence of an incident through visual inspection using the CCTV system. Manual confirmation is used to prevent false alarms from triggering unwarranted advisory sign messages and unduly restrictive ramp metering. The bottleneck module compares the average occupancy level at the upstream detector station to a third threshold. Tests for determining when to terminate incident and congestion alarms are also included in the algorithm. A decision tree showing the incident detection process is provided in Figure 3-3.

The algorithm is executed once every minute for every detector station covered by the system. The algorithm uses one-minute average occupancies which are updated every 30 seconds. The loop occupancy data are averaged across all lanes at a detector station.

General Observations

Although specific data on the performance of the algorithm are unavailable, the operators of the Virginia system indicated during the site visit that they were relatively satisfied with the performance of the algorithm. The general feeling was that the algorithm, as calibrated, achieved a good balance between the number of incidents detected, the time to detect incidents, and the rate of false alarms. Currently, Virginia Department of Transportation does not have any plans to abandon their existing algorithms.

However, during the on-site observations, the operators appeared to pay little attention to the incident detection algorithm. Most of the time, the operators were watching the CCTV monitors and reacted directly to the video images displayed in the control room. Even though, the operators occasionally would check the status of the incident display screen, they did not appear to be reacting directly to the information on the terminal. This was because, for the most part, they had already detected the incident using the surveillance cameras.

Figure 3-3. Northern Virginia Incident Detection Process.

Long Island, New York

The INFORM (INformation FOR Motorists) system is a motorist information/ freeway surveillance and control system that operates in a 40-mile long freeway corridor on Long Island, New York. The system provides surveillance and control on a total of 128 centerline miles of highway including two major freeways (the Long Island Expressway and the Northern State Parkway/Grand Central Parkway) as well as many parallel and crossing arterial streets and freeways. Although the system was originally envisioned in the early 1970s, it did not become fully operational until 1988 (34).

The INFORM system was designed primarily to prove the potential applications and effectiveness of motorist information systems. The primary purpose of the system is to alert drivers of impending congestion and delays, and provide them with diversion messages to alternate routes. The management of traffic (in terms of control functions) is a secondary objective.

The individual elements of the system include the following:

- an extensive loop detector surveillance system,
- an extensive network of changeable message signs (over 70 signs total)
- a ramp metering system that controls the operations of 50 ramps in either a manual, time-of-day, or traffic responsive mode, and
- a wall-size board that is used to display to the operator the average link speeds on the facilities.

The system also contains a limited amount of CCTV cameras. At the time of the site visit, only 12 cameras are operational. These cameras were not part of the original design but were added to the system to provide surveillance during a project to reconstruct part of the Long Island Expressway (32).

The electronic surveillance system consists of over 2000 individual inductive loop detectors grouped into approximately 500 detector stations or zones. Besides loop detectors placed in each lane, loops are also placed at or near each entrance and exit ramp in each detection zone. The typical spacing between mainline detection zones is ½ mile. This spacing varies, however, depending upon the spacing of entrance and exit

58

ramps. Paired "speed" trap loop detectors are located approximately every 3 miles. Detector data are compiled locally at each detector zone and then transmitted to the central computer once every minute.

Incident Detection Algorithm

The system began operating originally with a modified version of the California Algorithm to detect incidents. (The exact algorithm that was used at that time was not known by the operators.) New York Department of Transportation (NYDOT) discontinued using the algorithm because it produced too many false alarms (32). Through conversations with operating personnel, it appears that the algorithm was not properly calibrated for the system. Discussions indicated that a single set of threshold values may have been used for the entire surveillance area. No attempt was made to establish threshold values that were specific for particular detection zones. NYDOT does not have any plans to reactivate the algorithms.

Currently, NYDOT relies on the experience of the operators to detect incidents. A large, color-coded wall map is used to display travel speeds on each segment of highway under surveillance. A red indications is displayed to the operators when travel speeds fall below 30 mph. The operators use their experience to evaluate which red indications are "typical" and which are "unusual" for that time-of-day.

As a rule, the operators generally take remedial action only after two or more atypical but consecutive indications on the map are illuminated. If the operator observes an unusual condition, they typically retrieve additional information (such as loop occupancy and volume data) from the system. If the congestion occurs in the area of one of their CCTV cameras, they will use the cameras to investigate the cause of the congestion. The severity of the congestion is estimated by how rapidly delays propagate upstream. In the absence of other sources, the operators monitor police and CB radio scanners to determine the cause of an unusual congestion display. By monitoring the display board, an experienced operator can reliably predict the following (32):

- the nature of the congestion (i.e., whether it is recurring or non-recurring),
- the severity of the capacity reduction,

- the presence of rubbernecking, and
- the amount of delay to be expected based on the location, time of day, and severity of the congestion.

General Observations

Because of the way the INFORM system is designed and operated, the rapid detection of incidents is not critical. INFORM was designed to be a motorist information system. It was never designed or intended to be an incident management system. NYDOT uses its CMSs to inform motorists of impending delays only. NYDOT's operating policy is to not use messages that describe the cause of a delay (i.e., "ACCIDENT", "CAR FIRE", etc.) for fear that these types of messages will peak the interests of some motorists and cause them not to divert from the congested freeway (32). From an operating standpoint, however, the use of an automatic incident detection algorithm was perceived as a beneficial tool to the operators of the INFORM system.

Minneapolis, Minnesota

Minnesota Department of Transportation's (MnDOT) Traffic Management Center (TMC) is the communication and computer center for managing traffic on the freeways in the Minneapolis/St. Paul area. It has been operating in the Minneapolis/St. Paul area since 1972 (33). The TMC is responsible for monitoring and controlling the operations of a total of five interstate highways (I-35W, I-94, I-394, I-494, and I-694) and five State Highways (Trunk Highways 212, 169, 100, 62 and 77). The freeway surveillance and control system includes approximately 308 ramp meters (223 which are centrally controlled), over 100 closed circuit television cameras, and 32 rotating drum changeable message signs.

A system of inductive loops is used to provide the TMC with volume, occupancy, and speed data in the surveillance area. A single loop detector is installed in each lane of the freeway. Data from the loops are averaged across all lanes to develop station averages. Loop data averages are compiled every 30 seconds and then transmitted to the

TMC. Type 170 controllers are used to compile data in the field. Loop detector stations are spaced every ½ mile.

The most impressive feature about the Minnesota system is the amount of video surveillance used in the system. Approximately forty-five percent of the freeways in Minneapolis/St. Paul area are under CCTV surveillance. A total of 108 CCTV cameras provide surveillance on portions of five interstate highways and five state highways.

A redesign of the control room at the TMC was recently completed. The new control room has areas for two independent operator stations, a radio announcer station, and an information officer station. The two operators are responsible for monitoring the forty-eight 17-inch video monitors (each operator monitors twenty-four). Typically, video images from two or three cameras are displayed on each monitor in a sequential fashion. Each operator station is also equipped with a computer graphic terminal which is capable of controlling on-line ramp meters and the changeable message signs. In addition, a large screen computer-generated map is used to display real-time traffic conditions on the freeways in surveillance area. The map display is used by the information officer and the radio operators to broadcast congestion and incident information to motorists. (MnDOT provides live broadcasts from the TMC on a public radio station operated by Minneapolis Public Schools).

Incident Detection Algorithm

When the system originally became operational, a modified version California type algorithm was used to detect incidents. At the time the algorithm was operational, approximately one-half of the current area under surveillance was covered (approximately 150 miles). Use of algorithm was discontinued because of the large number of false alarms generated by the algorithm and because other sources (i.e., the video surveillance system) provided more accurate and faster detection of incidents (33). Through discussions with the MnDOT operating personnel, it appears that one set of threshold values was used for the entire city.

Currently, the primary means of detecting incidents in the coverage area is through the video surveillance cameras. Operators watch the video monitors for tell-tale signs of

incidents (i.e., unusual congestion or light traffic, stopped vehicles, flashing lights, etc.). The general feeling at MnDOT is that this method allows them to detect incidents as quickly and as accurately as an algorithm.

Chicago, Illinois

The Illinois Department of Transportation (IDOT) Traffic System Center provides surveillance and control on over 130 centerline miles on eight freeways in six counties in the Chicago metropolitan area (34). The system was one of the first traffic surveillance and control systems in the United States. Although the control center is staffed only from 5:00 a.m. to 7:00 p.m. on weekdays, the system operates 24 hours a day, 7 days a week.

Approximately 2000 loop detectors provide surveillance capabilities on the eight different freeways. Detector stations are spaced approximately every ½ mile. Each detector station consists of a single inductive loop detector. Loops are placed in only the center lane at each detector station. All the detector stations are monitored centrally by a VAX 11-750 computer system. Loop detectors are polled by the central computer 60 times a second. The central computer then develops 1 minute average occupancies and volumes from the individual pulses. A separate mainframe computer is used to monitor traffic from each freeway under surveillance.

In addition to the surveillance system, IDOT relies heavily on other systems to provide them with traffic and congestion information including the following:

- an extensive freeway service patrol system (over 35 vehicles),
- police patrols,
- maintenance forces,
- aerial surveillance by traffic reporting services,
- the monitoring of CB radio, and
- reports from cellular telephone users.

Incident Detection Algorithm

Although IDOT has experimented with several different algorithms (including the Bayesian and California algorithms), they are currently using a simple comparative algorithm to automatically detect incidents in the surveillance area. Using five minutes worth of data the algorithms compares the one minute average occupancy level at two adjacent detector stations. An incident is declared when the occupancy levels at both detector stations exceed all five of the following conditions,

	Lane Occupancy Levels	
Time	Upstream	Downstream
T	$\geq 30\%$	$\leq 10\%$
T-1	$\geq 30\%$	$\leq 10\%$
T-2	$\geq 28\%$	$\leq 12\%$
T-3	$\geq 26\%$	$\leq 14\%$
T-4	$\geq 24\%$	$\leq 16\%$

Since the algorithm is working with a five minute window of data, the minimum detection time for the algorithm is five minutes. For this reason (and others), IDOT relies on other sources (such as the cellular telephone number, emergency service patrols, CB and police radio monitoring, and operator experience) as the primary means of detecting incidents.

General Observations

It should be noted that the IDOT's philosophy has never been to use a computer algorithm as the primary means of detecting incidents. For this reason, the incident detection algorithm used in the Chicago system is intended to be a secondary means of detecting incidents and a tool for training new operators (34). By design, the algorithm is intended to help the operators spot possible incident locations that have not already been detected by visual patrols or by monitoring the real-time displays. The "alarms" produced by the algorithm are used to alert the operators as to locations that should be monitored more closely.

Because the algorithm is not a primary means of incident detection, statistics on the performance of the algorithm (i.e. detection time, false alarm rate, mean time-to-detect) are not kept by IDOT. Furthermore, IDOT does not classify nonrecurrent congestion as an incident until it is visually confirmed and responded to by the emergency service patrol. In many cases, the initial cause of the congestion either has cleared by the time the patrol arrives or is unknown. Therefore, it is hard for IDOT to classify an alarm as either being the result of an incident or as a false alarm.

Toronto, Ontario

The Ontario Ministry of Transportation has installed a freeway surveillance and control system on the Highway 401 freeway in the Toronto area. Highway 401 is one of the major freeways in the Toronto area and carries approximately 350,000 vehicles per day. It contains both express through lanes and collector lanes. Ingress and egress to the express lanes is provided by slip ramps spaced periodically throughout the length of the freeway. Each section of the collector lanes services three or four entrance and exit ramps to and from the freeway (35).

The freeway management system on Highway 401 became operational in 1990. It provides 24 hour-a-day, 7 day-a-week surveillance on over 27 km (16 miles) of freeway in the Toronto area. It includes over 220 loop detectors, 37 color video surveillance cameras, and 13 LED changeable message signs.

Inductive traffic loops are used to obtain volume, occupancy, and speed data from the freeway. Both single loop and dual loop detectors stations are used in the system to provide traffic data. Because of the greater accuracy and redundancy that is provided using dual loop detector stations, the current design policy for new or replacement loops is to use dual loops. The spacing between detector stations is approximately 600 meters (¼ mile).

The local controller produces aggregate volume and occupancy data across all the lanes at each detector station. The data are then transmitted the central computer once every 20 seconds. Since detector data are checked by the central computer in the next 20 second interval, data used in the incident detection algorithm are 40 seconds old.

When the system originally came on-line, two algorithms were used to automatically detect incidents: the All-Purpose Incident Detection (APID) algorithm and the Double Exponential Smoothing (DES) algorithm. Even though the software has been designed to run up to five different algorithms at a time, only one algorithm can be used to detect incidents in a particular group of detector stations. The software was configured so that different algorithms can be used for different groups of detector stations. The operator selects which algorithm to use for each particular set of detector stations.

Recently, the Ministry has switched to the McMaster algorithm as the primary algorithm used to detect incidents in the main lanes. The Ministry began using the McMaster algorithm in an operational mode late in 1992 (35). Although they have not completed their evaluation, the Ministry is generally pleased with the performance of the McMaster algorithm (35). They feel the algorithm has significantly reduced their false alarm rate over the California algorithm. The Ministry did report that they had problems with the algorithm during one period of inclement weather (a snow storm in January). The storm caused atypical driving patterns on the freeway, which resulted in a high false alarm rate during the storm.

Findings

On-site interviews and observations were conducted at seven freeway surveillance and control centers operating in the United States and Canada. The purpose of the site visits was to obtain a better understanding of the types of algorithms that are being used in these systems to detect incidents, and the role automatic incident detection plays in the entire incident management and freeway management efforts in these cities.

Of the seven locations visited, only four (Los Angeles, Northern Virginia, Chicago, and Toronto) are actively using an algorithm to detect incidents on the freeways covered under their respective surveillance systems. Except for Toronto, all of these systems are using a modified version of the California algorithm. Toronto has recently switched from a family of California algorithms to the McMaster algorithm. Most of these systems did not have quantifiable data on the performance of their algorithms.

For the most part, the operators from these four centers reported they are generally pleased with the performance of the algorithms they are using. However, with the exception of Toronto, on-site observations of the control centers revealed that the operators did not depend heavily on the algorithm to alert the operators to the presence of incidents. For the most part, the operators relied on other mechanisms, such as radio reports or CCTV systems, to alert them of incidents on the freeway.

Three locations (Seattle; Long Island, New York; and Minneapolis) are not using any kind of algorithm to assist them in detecting incidents in their systems. All of these systems were using modified versions of the California algorithm at one time, but have subsequently discontinued its use the algorithms because of the high number of false alarms produced. Both Seattle and Minneapolis depend on their CCTV systems to detect incidents, while the INFORM system relies on the experience of the operators to distinguish between incidents and normal bottleneck congestion.

In general, how an algorithm performs in a system depends upon the role the algorithm is expected to play in the overall incident management/freeway management system. No incident detection algorithm can detect an incident the instant it occurs. Regardless of the type of algorithm or how frequently the algorithm is executed, there is always some delay in detection. Therefore, those agencies that demand rapid detection of incidents with very few false alarms are generally not pleased with the performance of their algorithms. Agencies are generally more pleased with the performance of the algorithms when used as secondary means of detection, where longer detection times and high false alarm rates are not as critical.

Proper calibration of the algorithms also effects performance. Of those systems that have discontinued algorithm use, improper calibration appears to the most prevalent reason why the algorithms generated a high number of false alarms. Most of these systems appeared to be using only one set of threshold values for the entire surveillance area. Since geometric anomalies (i.e., lane drops, severe grades, etc.) affect traffic flow, algorithms must be calibrated on a zone-by-zone basis for them to be of use to the operators.

Extensive amounts of data, effort, and time are required to properly calibrate an algorithm. Even then, it may not be possible to totally eliminate all of the false alarms. Minor fluctuations in traffic caused by slow moving vehicles or inclement weather may interfere with traffic flow enough to trigger false alarms. Furthermore, at least one agency believes that the algorithms cannot be properly calibrated unless an incident occurs in every detection zone.

4. ASSESSMENT OF EXISTING INCIDENT DETECTION ALGORITHMS

In this chapter, a comparative assessment of the existing incident detection algorithms is performed. The assessment focuses on the following major issues that should be considered in the selection of an incident detection algorithm in an operating freeway surveillance and control center:

- the performance of the algorithms as reported in the existing literature,
- the data required to operate the algorithms,
- the ease at which they can be implemented in an freeway surveillance and control center, both from an operators and a system designer standpoint,
- the ease at which they can be calibrated once in an operational setting, and
- the use in operational control centers throughout the United States and Canada.

Again, it should be noted that this assessment is based on data that are currently available in the literature. An actual comparison of algorithm performance (either off-line or on-line) was not performed as part of this study.

Reported Performance

Three major measures are typically used to assess the performance of incident detection algorithms: detection rate, false alarm rate, and detection time. Of these three, detection rate is the primary measure for assessing the ability of the algorithm to detect incident patterns in a stream of detector data. It is typically defined as the percentage of the total number of capacity-reducing incidents that are detected by the algorithm in a specified period.

The false alarm rate, on the other hand, is used to assess an algorithm's ability to distinguish true incident patterns from random fluctuations in detector data. Historically, there are two ways of calculating the false alarm rate for an algorithm. The first is to calculate the false alarm rate as the percentage of incident alarms that are falsely declared to the total number of incident declarations (both true incidents and false alarms) that occurred in a specified period. This is commonly called the on-line false alarm rate and

represents how an operating agencies might typically calculate the false alarm rate of algorithm used in an actual operational setting. The second is to define the false alarm rate as the percentage false alarm signals produced by the algorithm out of all signals (both incident and nonincident). This definition includes not only decisions where an incident alarm was produced (either as a true incident or a false alarm) *but also all decisions where the algorithm determined that no incident was present*. This is typically called the off-line false alarm rate and is used by many research to assess the performance of their algorithms. Typically, the off-line false alarm rate is significantly less than the on-line rate.

Detection time is typically defined as the time between when an incident occurs and when it is detected by the algorithm. However, because of the way data were collected, the reported detection time in some studies is actually the time between when an incident is observed by an operator and the time detected by the algorithm. In these cases, the time between when the incident occurred and recorded by the operator is not known. It is possible considerable delays can occur between when the incident occurs and when it is recorded by the operator.

There is no single study that compares the performance of all the existing algorithms using the same set of data. Furthermore, very few of the algorithms have actually been evaluated in an on-line study. Therefore, results from different studies have been used to assess the performance of the different algorithms. Unfortunately, the algorithms are seldom evaluated under similar operating conditions.

Table 4-1 presents the best detection rate, false alarm rate, and detection time for each of the existing algorithms. The performance measures shown in the table represent an off-line evaluation. This table is intended for illustrative purposes only and should not be used for direct comparisons. Because of the differences in the way that performance measures are computed in some studies, a direct comparison of the performance of the algorithms is not possible. Also, note that performance data from the PATREG, HIOCC, and Dynamic Model algorithms are not included in the table because they were not evaluated using the same performance measures as the other algorithms.

Table 4-1.   Reported Best Performance of Existing Incident Detection Algorithms.

Algorithm	Detection Rate	False Alarm Rate	Average Detection Time
California			
Basic	82%	1.73%	0.85 mins
Algorithm #7	67%	0.134%	2.91 mins
Algorithm #8	68%	0.177%	3.04 mins
APID	86%	0.05%	2.5 mins
Standard Normal Deviate	92%	1.3%	1.1 mins
Bayesian	100%	0%	3.9 mins
Time-Series ARIMA	100%	1.5%	0.4 mins
Exponential Smoothing	92%	1.87%	0.7 mins
Low-Pass Filter	80%	0.3%	4.0 mins
McMaster	68%	0.0018%	2.2 mins

From this table, it can be seen that there is little difference in the performance of existing incident detection algorithms. The detection rate of all of the algorithms ranged between almost 70 and 100 percent, with the majority of the algorithms achieving detection rates between 85 and 95 percent. The false alarm rates were reported to be below 1.5 percent for most of the algorithms. It is important to remember that actual performance in the field may vary tremendously from that reported in the literature.

Three noteworthy exceptions to this generalization are the modified California Algorithm #7, and the modified California Algorithm #8, and the McMaster algorithm. While these three did not achieve detection rates as high as some of the other algorithms,

they reported producing fewer false alarms. Recall that there is a trade-off between detection rate and false alarm rate. For most algorithms, changes in the algorithm to increase in detection rate also result in increases in the false alarm rate.

It is also important to remember that the structure of a particular algorithm influences the detection times. Some algorithms use special tests (such as persistence checks and compression wave tests) that delay signaling an alarm until incident conditions are detected for a specified number of iterations. For example, the Modified California Algorithm #7 includes a persistence check which requires that threshold values be exceeded for three minutes. This persistence check adds to the overall detection time. In cases where algorithms include persistence and compression wave tests, it is logical for algorithms that include these tests to have higher detection times. Therefore, the high detection times reported for Algorithm #7, Algorithm #8, and the Low-Pass Filter algorithms are to be expected.

The negative effects of including these tests (in terms of increased detection times) are offset by the reduction in the false alarm rate. As shown in Table 4-1, the algorithms with the higher detection times also tend to have a lower false alarm rate. The lower false alarm rate can be directly attributed to the structure of the algorithm for delaying sounding an incident alarm until the algorithm is certain that a true reduction in capacity has occurred.

Data Requirements

From an operational standpoint most of the algorithms require the same amount and type of data, Table 4-2 lists the traffic features that are used in each algorithm as the control variable. As seen from this table, most algorithms use occupancy (or a derivative of occupancy) as the control measure for detecting congested traffic conditions. Occupancy is defined as the percentage of time that a loop detector is occupied by vehicles (35). As such, it is a direct measure of the level of concentration (or congestion) that exists on a freeway. Typically, occupancy values range from 0 percent (the complete absence of vehicles passing over the loop) to 100 percent (a vehicle is completely stopped over the loop). Occupancy levels greater than 30 percent are typical of congested flow conditions.

Table 4-2.   Traffic Parameters Used as Control Variable in Existing Incident Detection Algorithms.

Algorithm	Occupancy	Volume	Speed	Other
California				
Basic	X	-	-	-
Algorithm #7	X	-	-	-
Algorithm #8	X	-	-	-
APID	X	X	X^1	-
PATREG	X	-	-	-
Standard Normal Deviate	X	X	-	Energy^2
Bayesian	X	-	-	-
Time Series ARIMA	X	X	-	-
HIOCC	X	-	-	-
Exponential Smoothing	X	-	-	Station^3 Discontinuity
Low-Pass Filter	X	-	-	-
Dynamic Model	X	X	-	-
McMaster	X	X	X^4	-

[1] Derived from occupancy and volume
[2] Derived as the square of volume divided by the occupancy
[3] Comparison of kinetic energy of individual lanes
[4] Optional parameter

Most algorithms use a 60-second average occupancy value (i.e., loop occupancy levels measured for 60 seconds) as the control variable. Others use a 60-second moving average where occupancy measures are updated every 20 to 30 seconds. Table 4-3 lists the interval and the update cycles of the traffic variable in each of the existing algorithms. As discussed above, the interval over which the traffic variable is averaged often dictates the time required to detect an incident.

Table 4-3. Interval and Update Cycle of Traffic Parameters Used in Existing Incident Detection Algorithms.

Algorithm	Time Interval Over Which Control Variable is Averaged (sec)	Update Cycle (sec)
California		
Basic	60	20, 30, or 60
Algorithm #7	60	20, 30, or 60
Algorithm #8	60	20, 30, or 60
APID	20 to 300	20
PATREG	40	1
Standard Normal Deviate	180 or 300	60
Bayesian	60	20
Time Series ARIMA	20	20
HIOCC	2	1
Exponential Smoothing	60	60
Low-Pass Filter	180	30
Dynamic Model	60	5
McMaster	30	30

Ease of Implementation

The ease at which an algorithm can be implemented into the design and operation of the surveillance and control center should also be considered when selecting an incident detection algorithm. Usually, the incident detection algorithm is only one piece of information that has to be processed by an operator in a traffic control center. Besides monitoring the incident detection algorithm, control room operators are often responsible for operating ramp-metering systems, CCTV systems, and motorist information systems. Because operators are required to make decisions based upon the results of the algorithm, it is important for them to understand how incidents are detected in the algorithm. An operator is more likely to use and make decisions if the algorithm is intuitively easy to understand.

Furthermore, it is also important that the algorithm must be relatively easy to integrate into the proposed design of a freeway surveillance and control center. For TxDOT, the large areas that covered by the surveillance centers and the desire for a distributed computing structure makes it desirable to use an algorithm that performs well (in terms of detection rates, false alarm rates, and detection times) but does not require extensive amounts of computer processing time. Algorithms that have simpler structures (in terms of the number of calculation required during each iteration of the algorithm) are typically easier to implement in a control center.

Unfortunately, there is little quantitative information on how easy it is to implement each of the incident detection algorithms in an actual freeway surveillance and control center. Table 4-4 provides a qualitative assessment of the ease that each algorithm could be implemented in proposed TxDOT design. The assessment is based on judgments relating to the complexity of the design of the algorithm and the amount of processing required by each algorithm. Each algorithm is given a rating of Low, Moderate, High, or Extremely High based on the complexity of the algorithms structure and the perceived ease that the algorithm can be integrated into the proposed structure of the surveillance and control system.

Table 4-4. Perceived Degree of Complexity and Ease of Integration of Existing Incident Detection Algorithms Into TxDOT Freeway Surveillance and Control System.

Algorithm	Degree of Complexity	Ease of Integration
California		
Basic	Low	Easy
Algorithm #7	Moderate	Easy
Algorithm #8	Moderate	Easy
APID	Moderate	Easy
PATREG	Low	Difficult
Standard Normal Deviate	Low	Easy
Bayesian	High	Moderate
Time Series ARIMA	High	Difficult
HIOCC	Low	Difficult
Exponential Smoothing	Moderate	Moderate
Low-Pass Filter	Moderate	Easy
Dynamic Model	Extremely High	Extremely Difficult
McMaster	Moderate	Moderate

Ease of Calibration

Another important factor to consider in selecting an incident detection algorithm is the level of effort required to calibrate the algorithm in an operational setting. Calibration is the process of identifying the relationships in traffic detector data and establishing the thresholds that are used to detect incidents. Each detection for most algorithms is a complex and time-consuming task, requiring extensive amounts of traffic data under both incident and nonincident conditions. Without proper calibration, most incident detection algorithms will not perform to as expected. Improper calibration is one reason some agencies have not been pleased with the performance of the incident detection algorithms in their systems.

No single algorithm is easier to calibrate than the others. All require some degree of calibration and modification. Seldom can traffic relationships and detection thresholds be transferred from system to system without being calibrated to the specific conditions that exist. On occasions, it may possibly to use a single algorithms with a single set of thresholds (perhaps varying by time of day) for a group of detectors and possible a single freeway, but more likely than not detection threshold and traffic relationships will need to be developed for each individual detector station or detection zone on a freeway.

To fully calibrate an algorithm, traffic data from both incident and nonincident conditions are required for each detector station or detection zone included in the incident detection system. Incident data are used to establish trends and identify threshold values under incident conditions. Nonincident data are used to identify areas of peculiar operations and to assess the false alarm rate. Calibration should occur using both off-line and on-line data.

Calibration can be a time-consuming and labor intensive effort. Most algorithms require incident and nonincident data be collected and analyzed from each detection zone. Detection zones with particular geometric and operational characteristics must be considered in the calibration process. Areas that experience unusual traffic operations are identified for testing to find out if the algorithm should be tailored to meet the peculiar operating conditions of traffic in that detection zone. Once the areas the experience peculiar operating conditions have been identified, off-line analyses can be performed to

77

develop specific detection threshold and traffic relationships for these zones. On-line analyses are performed to insure that the algorithm is functioning as expected.

Operational Experience

A final factor to consider in selecting an incident detection algorithm is the experiences other operating agencies have had with the different algorithms in an operational setting. Algorithms that perform well in off-line evaluation may not perform as expected when implemented in the field. Therefore, the experiences that other operating agencies have had with the different algorithms is a valuable source of information.

As discussed in the previous chapter, most of the traffic control centers that are operating today are using (or have used) the some variation of the California algorithm. There are two possible explanations for this. First (and probably foremost) is that many of these centers began operating in the 1970s. At this time, the California algorithms (or one of its variations) was considered the standard algorithm. The second is nature of the algorithms itself. The underlying idea of the California algorithm is easy to understand and makes intuitive sense.

Not all of the operating agencies, however, have been pleased with the performance of the California algorithm in their system. Representatives from many of the agencies reported problems with false alarms. Several operating agencies have stopped using their incident detection algorithms altogether. While there are a number of possible explanations for the false alarm problem, the most probable cause is improper or inadequate calibration.

The only other existing algorithm that is currently being used in an operational setting is the McMaster algorithm. The Ontario Ministry of Transportation has recently begun using the McMaster algorithm in an operational capacity to detect incidents in the Toronto area. They began using the algorithm in late 1992 and have been generally pleased with its performance so far.

Summary

No single algorithms appears to be superior in terms of it reported performance, data requirements, ease of implementation, ease of calibration, and operational experience. Essentially, there is no significant difference between the reported performance of any of the detection algorithms. All of the algorithms tend to acheive detection rates greater than 70 percent, at an off-line false alarm rate of less than 2 percent. Most algorithms, when properly calibrated, best reported detection rate ranged between 85 and 90 percent with false alarm rates well below 1 percent. Although two algorithms reported achieving 100 percent detection rates, one did not function well in an on-line comparison (achieving a 40 percent detection rate with an 80 percent false alarm rate) while the other experienced a relatively high off-line false alarm rate (over 1 percent).

Of all the algorithms, the California algorithms (specifically, Algorithm #7 and Algorithm #8) and McMaster algorithm appear to be the most logical choices for TxDOT to consider in the initial implementation of their freeway surveillance and control system. Both of these types of algorithms have relatively simple structures and should be relatively easy to implement in the TxDOT's control system logic. California algorithms use traffic paratmeters that are derived using simple subtraction and division equations. The McMaster algorithm uses a simple comparison of measured traffic conditions to volume-occupancy curves that has been established for each detector station.

In terms of data requirements, both of these types of algorithms require the same type of data. Both types of algorithms use data that can be directly obtained from loop detectors. The California algorithms use one-minute moving averages of occupancy. This moving average can be updated at either 20, 30 or 60 second cycles. The McMaster algorithm uses both volume and occupancy measures derived from loop detector data. These measures can be 20, 30 or 60 second averages.

5. RECOMMENDATIONS

This report has provided an evaluation of the application and performance of the existing algorithms for detecting incidents on freeways using loop detector data. This evaluation was based on a review of operating performance as reported in the literature and site visits to operating freeway surveillance and control centers in the United States and Canada. Performance measures used in the evaluation included reported detection rate, false alarm rate, detection time, ease of calibration and implementation, data requirements, and actual operating experience.

Based on a review of the reported performance in the literature, and site visits to operating freeway surveillance and control centers, no single algorithm can provide optimum performance under all traffic situations that are likely to occur on a freeway. With all of the algorithms, there is a tradeoff between the number of incidents that are detected by the algorithm and the number of false reports of incidents produced by the algorithm. Algorithms that are set to achieve a high detection rate also achieve a high false alarm rate. As the sensitivity to the algorithm is adjusted to lower the false alarm, the number of incidents that are detected by the algorithm is also reduced. Therefore, expectations of obtaining a 100 percent detection rate with no false alarms with any of the existing algorithms are unrealistic.

It is also unrealistic to expect any of the reviewed algorithms to be able to detect an incident the moment that it occurs. There is always some level of delay associated with all of the existing incident detection algorithms. For the most part, the delay comes from two sources: the physical proximity of the incident to a detector station and the structure of the algorithm. The structure of most algorithms results in a one to three minute delay in detection. Persistence checks and compression wave tests that are used to reduce false alarms often add between three and five minutes of additional delay to the detection time. Many operating agencies reported that they often already knew of an incident through other means (i.e., CCTV surveillance, cellular telephone reporting systems, etc.) before it was detected by the algorithm.

With these limitation in mind, three incident detection algorithms are recommended for consideration for initial implementation in TxDOT's freeway surveillance and control system:

81

- the Modified California Algorithm #7,
- the Modified California Algorithm #8, and
- the McMaster Algorithm

These algorithms are recommended for a number of reasons. First, all three of these algorithms were reported to perform well in both off-line and on-line comparisons in the literature. When calibrated properly, these algorithms can be expected to achieve detection rates in the 70 to 85 percent range with reasonable false alarm rates (less than 1 percent). The modified California Algorithm #7 is a good all-purpose algorithms that can be expected to perform well under most traffic conditions. The modified California Algorithm #8 performs best under high volume conditions. Consideration should be given to incorporating logic (similar to that used by the APID algorithm) in the control system that uses both of the modified California algorithms depending upon the prevailing traffic conditions. Time-of-day changes in traffic conditions are reflected in the flow/occupancy curves developed for each detection station in the McMaster algorithm.

Conceptually, these algorithms are relatively easy to understand and implement from an operator standpoint. These algorithms do not require complicated theoretical relationships or formulas to detect incidents, but use simple comparisons of measured traffic parameters to preset thresholds or relationships to detect the presence of incident conditions. Most of the problems associated with the performance of these algorithms in an operating setting are believed to result from inadequate or improper calibration.

Regardless of the type of algorithm that is selected, calibration is a time-consuming process. With most algorithms, calibration must occur either on a station-by-station basis (as with the McMaster algorithm) or on a zone-by-zone basis (as with the California algorithms). In order for each algorithm to perform adequately, data from both incident and nonincident conditions must be used. It is unrealistic to expect to develop a single set of thresholds or traffic flow curves that can be universally applied to entire area under surveillance. Thresholds for each algorithm need to reflect the actual operating characteristics of traffic passing through each area of detection.

6. REFERENCES

1.   R. A. Reiss and W. M. Dunn, Jr. *Freeway Incident Management Handbook.* Report No. FHWA-SA-91-056. Federal Highway Administration, U.S. Department of Transportation, Washington D.C., July 1991.

2.   M. E. Goolsby. Influence of Incidents on Freeway Quality of Service. In *Highway Research Record 349.* Highway Research Board, National Research Council, 1971.

3.   H. J. Payne, E. D. Helfenbein, and H. C. Knobel. *Development and Testing of Incident Detection Algorithms, Volume 2: Research Methodology and Detailed Results.* Report No. FHWA-RD-76-20. Federal Highway Administration, U.S. Department of Transportation, Washington D.C., April 1976.

4.   S. C. Tignor and H. J. Payne. Improved Freeway Incident Detection Algorithms. In *Public Roads.* Federal Highway Administration, U.S. Department of Transportation, Washington D.C., June 1977.

5.   P. H. Masters, J. K. Lam, and K. Wong. Incident Detection Algorithms of COMPASS -- An Advanced Traffic Management System. *Vehicle Navigation and Information Systems Conference Proceedings.* Society of Automotive Engineers, Inc. Warrendale, PA., October 1991.

6.   *Highway 401 FTMS Software Functional Specifications.* Ministry of Transportation, Toronto, Ontario. February 1978.

7.   J. F. Collins, C. M. Hopkins, and J. A. Martin. *Automatic Incident Detection -- TRRL Algorithms HIOCC and PATREG.* TRRL Supplementary Report 526, Transport and Road Research Laboratory, Crowthorne, Berkshire, 1979.

8.   C. L. Dudek, C. J. Messer, and N. B. Nuckles. Incident Detection on Urban Freeways. In *Transportation Research Record 495.* Transportation Research Board, National Research Council, Washington D.C., 1974.

9.   M. L. Levin and G. M. Krause. Incident Detection: A Bayesian Approach. In *Transportation Research Record 682.* Transportation Research Board, National Research Council, Washington, D.C., 1978.

10. M. S. Ahmed, and A. R. Cook. Analysis of Freeway Traffic Time-Series Data Using Box-Jenkins Techniques. In *Transportation Research Record 722.* Transportation Research Board, National Research Council, Washington D.C., 1977.

11. S. A. Ahmed and A. R. Cook. Application of Time-Series Analysis Techniques to Freeway Incident Detection. In *Transportation Research Record 841.* Transportation Research Board, National Research Council, Washington D.C., 1982.

12. G. A. Davis, N. Nihan, M. Hamed, and L. Jacobson. Adaptive Forecasting of Freeway Traffic Congestion. Presented at the First International Conference on Applications of Advanced Technologies in Transportation Engineering. San Diego, CA. February 1989.

13. A. R. Cook, and D. E. Cleveland. Detection of Freeway Capacity-Reducing Incidents by Traffic-Stream Measurements. In *Transportation Research Record 495.* Transportation Research Board, National Research Council, Washington D.C., 1974.

14. Y. J. Stephanedes, A. P. Chassiakos, and P. G. Michalopoulos. Comparative Performance Evaluation of Incident Detection Algorithms. In *Transportation Research Record 1360.* Transportation Research Board, National Research Council, Washington D.C.,

15. Y. J. Stephanedes, and A. P. Chassiakos. Application of Filtering Techniques for Incident Detection. In *Journal of Transportation Engineering.* Volume 119, No. 1. American Society of Civil Engineers, New York, NY. 1993.

16. A. S. Willsky, E. Y. Chow, S. B. Gershwin, C. S. Greene, P.K. Houpt, and A. L. Kurkjian. Dynamic Model-Based Techniques for the Detection of Incident on Freeways. In *IEEE Transactions on Automatic Control.* Volume AC-25, No. 3. Institute of Electrical and Electronic Engineers, Piscataway, N.J., 1980.

17. H. J. Payne. Models of Freeway Traffic for Control. In *Mathematical Models of Public Systems, Simulation Control Proceedings.* Volume 1, No. 1. January 1971.

18. A. I. Gall and F. L. Hall. Distinguishing Between Incident Congestion and Recurrent Congestion: A Proposed Logic. In *Transportation Research Record 1232.* Transportation Research Board, National Research Council, 1989.

19.   B. N. Persaud, F. L. Hall, and L. M. Hall. Congestion Identification Aspects of the McMaster Incident Detection Algorithm. In *Transportation Research Record 1287.* Transportation Research Board, National Research Council, Washington D.C., 1990.

20.   F. L. Hall, Y.Shi, and G. Atala. On-Line Testing of the McMaster Incident Detection Algorithm Under Recurrent Congestion. Presented at the 72nd Annual Meeting of the Transportation Research Board, Washington D.C., January 1993.

21.   D. B. Fambro, and G. P. Ritch. *Automatic Detection of Freeway Incidents During Low Volume Conditions.* Report No. FHWA/TX-79/23+210-1. Texas Transportation Institute, Texas A&M University System, College Station, TX. September 1979.

22.   H. N. Yagoda, and J. R. Buchanan. A New Technique for Incident Detection in Light Traffic. *ITE 1991 Compendium of Technical Papers.* Institute of Transportation Engineers, Washington D.C., 1991.

23.   E. Charniak and D. McDermott. *Introduction to Artificial Intelligence.* Addison-Wesley Publishing Company, Reading, MA. 1986.

24.   E. C. P. Chang and K. Huarng. Incident Detection Using Advanced Technologies. Presented at the 72nd Annual Meeting, Transportation Research Board, National Research Council, Washington D.C. January 1993.

25.   C. H. Hsiao, C. T. Lin, and M. J. Cassidy. An Application of Fuzzy Set Theory to Incident Detection. Presented at the 72nd Annual Meeting, Transportation Research Board, National Research Council, Washington D.C., January 1993.

26.   R. L. Cheu, S. G. Ritchie, and W. W. Recker. Investigation of a Neural Network Model for Freeway Incident Detection. Presented at the Second International Conference on the Application of Artificial Intelligence Techniques to Civil and Structural Engineering, Oxford England, September 1991.

27.   K. N. Balke and W. R. McCasland. Development and Implementation of Systems to Collect, Analyze, and Disseminate Real-Time Traffic Information: A Private/Public Enterprise. Presented at the 1992 Annual Meeting of IVHS America. Washington D.C., 1992.

28.   P. G. Michalopoulos. Incident Detection Through Video Image Processing. In *Applications of Advanced Technologies in Transportation Engineering.* Proceedings of the Second International Conference. American Society of Civil Engineers, New York, NY. 1991.

29. Personal Communications with Alex Dunnet, California Department of Transportation, 1992.

30. Personal Communications with Mark Morse, Washington State Department of Transportation, 1992.

31. Personal Communications with Jimmy Chu, Virginia Department of Transportation, 1993.

32. Personal Communications with Joe Contegni, New York Department of Transportation, 1993.

33. Personal Communications with Glen Carlson, Minnesota Department of Transportation, 1993.

34. Personal Communications with Tony Cioffi, Illinois Department of Transportation, 1993.

35. Personal Communications with David Tsui, Ontario Ministry of Transportation, 1993.

36. A. D. May. *Traffic Flow Fundamentals.* Prentice Hall, Englewood Cliffs, NJ. 1990.

37. R. Wilshire, R. Black, R. Grochoske, and J. Higinbotham. *Traffic Control System Handbook.* FHWA Report No. FHWA-IP-85-11. Federal Highway Administration, U.S. Department of Transportation, Washington D.C., 1985.