A distributed wireless sensor network system for transportation safety and security

Mashrur Chowdhury[*a], Kuang-Ching Wang[b], Ryan Fries[a], Yongchang Ma[a], Devang Bagaria[b]

[a]Department of Civil Engineering, Clemson University, Clemson, SC 29634
[b]Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634

ABSTRACT

Given the anticipated increases in highway traffic, the scale and complexity of the traffic infrastructure will continue to grow progressively in time and in distributed geographical areas. To assure transportation efficiency, safety, and security in the presence of such growth, it is critical to identify an infrastructure development methodology that can adapt to expansions while assuring reliable operation for both centralized monitoring and distributed management. In this paper, a wireless sensor network design methodology is presented, aimed at providing effective distributed surveillance, anomaly detection, and coordinated response. The proposed methodology integrates state-of-the-art traffic sensors, with flexibly programmable controller devices that can integrate with the available traffic control equipments. The system methodology provides a paradigm in which sensors and controllers can be progressively incorporated and programmed to autonomously coordinate with peer sensors and a hierarchy of controllers to detect, notify, and react to anomalous events. Since the system can tolerate failure of parts of the system, as the network connectivity continues to increase, the proposed sensor network will have positive implications on evacuation plans during natural disasters or terrorist attacks. To illustrate the design methodology and usage, a simulated system along a freeway corridor in South Carolina was constructed in an integrated microscopic traffic and wireless sensor network simulation platform, in which distributed incident detection and response functions were implemented. The test results, including detection and false alarm rates and wireless communication latencies, are analyzed to identify insights of the system's operation and potential enhancement strategies.

Key words: Transportation Security, Intelligent Transportation Systems, Integrated Simulation Platform

1.0 INTRODUCTION

Ensuring the efficiency of the nation's highway transportation infrastructure in the coming decades without costly expansion is a challenge of importance. Increasing population, vehicles, and the excessive traffic induced by urban sprawl has overburdened the existing highway system. Recent threats of terrorism also revealed the highway system's many vulnerabilities and the pressing needs for solutions that jointly assure transportation capability, safety, and security.

Many cites around the world have been using a variety of technologies and systems to better manage and control their surface transportation network under the intelligent transportation systems (ITS) umbrella. As is commonly accepted by the transportation communities, widely and densely deployed traffic sensors for highway traffic surveillance and control are the key component for a majority of ITS functions, such as traveler information, real time traffic management, incident management, natural and human hazard evacuation.

Currently, the majority of roadside sensors are connected by copper wires, fiber-optic cables, or a cellular wireless network to a centralized control center. At the center, human operators are responsible for continuously monitoring and analyzing a large amount of data from video cameras and other sensors. The human decision makers must choose the right strategy by analyzing the sensor information, and then inform the field personnel and/or remotely configure traffic control equipment using the communication infrastructure.

[*]mac@clemson.edu; phone 1 864 656 3313; fax 1 864 656 2670

Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense VI, edited by Edward M. Carapezza, Proc. of SPIE Vol. 6538, 653807, (2007)
0277-786X/07/$18 · doi: 10.1117/12.722629

Several problems arise from the existing sensor network methodology. First, the required dedicated communication infrastructures are prohibitively expensive, particularly as a system grows in coverage and number of sensors increases. Inevitably, this growth limits the possibility of wide deployment extending to broader suburban and rural areas. From a security perspective, the communication and control center infrastructure is also vulnerable to terrorist attacks and natural disasters. Furthermore, the collection and processing of mass data at a centralized location incurs substantial latencies, reinforcing the geographical scope within which acceptable real-time response is possible. Finally, human operators who monitor the sensors endure high working stress, which in turn decreases the system reliability.

In this paper, a methodology is proposed to enable incremental deployment of numerous wireless sensors along highways. By enabling programmable intelligence at each sensor and provisioning distributed controllers to coordinate their observations and decisions, traffic control can take place at unprecedented flexible scopes. Based on the nature of events, response to detected anomalies can take place either at regional levels of various scopes or at the central control center. This ability to detect anomalies at a regional scope reduces or eliminates the need for sending tremendous amounts of data to the control center over the communication infrastructure. To accomplish a regional scope, the sensors utilize ad hoc wireless network interfaces to communicate only the processed information with nearby sensors and controllers, relieving the needs of any communication infrastructure. Sensors and controllers carry out distributed algorithms for detection and response, in place of today's centralized solutions. The large number of computing entities (sensors and local controllers) in each area provides redundancy in the decision making process, to tolerate device failures due to aging, attacks, or disasters. Not only is the system capable of proper function due to partial system failures, but the fact that the system is composed of numerous autonomous components will also reduce the terrorist interests of attacking any individual components, the risks decreasing with an increasing system coverage. The proposed sensor network will have positive implications on evacuation plans during natural disasters or terrorist attacks. Motorists are expected to be able to acquire instantaneous evacuation instructions from the distributed highway controllers, which can be the coordinated decision among controllers of multiple highways derived with minimal operator intervention.

Despite existing knowledge in the separate domains of wireless sensor networking and transportation engineering, it has not been addressed how a distributed wireless sensor system can be practically implemented for traffic control. To plan, deploy, and operate such a network as a distributed autonomous system, we propose a hierarchical, distributed, and collaborative system paradigm within which collaborative decision making algorithms can be developed for automated highway surveillance and control. To illustrate the design methodology, a simulated system along a freeway corridor in South Carolina is constructed in an integrated microscopic traffic and wireless sensor network simulation platform, in which distributed, collaborative incident detection and response functions were implemented. The test results, including detection and false alarm rates and wireless communication latencies, are analyzed to identify insights of the system's operation and potential enhancement strategies.

2.0 BACKGROUND

State-of-the-art ITS systems around the world have been built with the focus of observing and controlling traffic operations from a central location[1,2,3,4,5]. Surface traffic control agencies deploy many sensors along the highway and establish traffic management centers (TMC's) to collect these sensor data for making centralized control decisions. Substantial investments have been made to connect all sensors to central or regional control centers using dedicated communication links. Roadside sensors transmit data to TMC's following predetermined schedules. Loop detectors and video cameras have been the primary sensing devices in use.

For freeway management, human operators detect abnormal conditions through surveillance reports or screening sensor data. Incidents are resolved by dispatching human response teams, rerouting upcoming traffic, and re-timing traffic signals[6]. The centralized control methodology imposes enormous responsibility on operators and critical dependency on an extensive communication backbone that are costly and limited in reliability, both of which are security liabilities during emergencies such as evacuations.

Despite the centralized monitoring and control practice, decentralized and hierarchical control methods have long been used for traffic signal control[7]. Traffic engineers carefully group traffic signals on closely related road segments, such

that their signal timings are consistently controlled to minimize wait time and optimize road capacity. By extracting hierarchical traffic characteristics from intersection sensor data, numerous real-time signal timing adaptation methods have been studied.

In early 1980s, the UK Transportation Research Laboratory (TRL) developed and implemented a global, real-time, rule-based expert system named as SCOOT[8]. A huge rule base is maintained for the traffic signal network, with which SCOOT performs global optimization on signal timing to minimize delays. Unfortunately, SCOOT's global optimization approach is known to be slow and unable to deal with local changes in real time.

The Sydney Coordinated Adaptive Traffic System (SCATS)[9], developed by Australian transportation authority in the late 1970s, is a distributed hierarchical system that optimizes traffic signal timing using volume data detected by sensors at signal stop-lines. The system aims to optimize the traffic flow based on optimizing individual *regions* in the network. Trained specialists are often needed to properly define the region boundary and offset parameters for each region.

In early 1990s, the University of Arizona developed a real time adaptive control system called the Real-time Hierarchical Distributed Effective System (RHODES)[10]. The system constructs stochastic traffic flow models to predict the expected condition over the next few minutes. While its hierarchical architecture are conceptually applicable to network wide operation, its algorithms demand exponential complexity and network wide real-time communication, thus rendering its practical use to a very limited network scope.

With advances in ad hoc wireless sensor network technology, intelligent sensors have been envisioned to be useful for future traffic control system[11]. Yet, the architecture and design method for such a large scale traffic sensor network has not been addressed in literature. Recently, researchers considered unleashing one level of freedom for the originally wired traffic sensors in California highways by removing the fiber optic cables of some sensors. Instead, TMC maintains links to only a number of gateway devices, while each gateway collects data from their nearby sensors using a multi-hop wireless network forwarding protocol named Power Efficient and Delay Aware Medium Access (PEDAMACS)[12]. PEDAMACS does not alter the centralized control model, since all data are still delivered to TMC's for monitoring and control. In a more confined scope, sensors have been placed on specialized highways and vehicles for automated vehicle steering, which have been highlighted in the 1997 and 2003 automated highway system demos in San Diego, CA.

3.0 METHODOLOGY

3.1 Hierarchical Sensor Network Architecture

The proposed methodology adopts a hierarchical network architecture, which manifests itself in the routing protocol implementation, inherits the hierarchical segment-intersection-network traffic modeling concepts[10]. It is envisioned as follows[1]:

- **Three functional units –** sensors, controllers, and clusters – are defined. Sensors perform sensing along road segments and report data to controllers that are typically located at intersections or interchanges. An ad hoc wireless network is formed connecting all sensors and controllers. A cluster is a logical grouping of controllers and sensors that collaborate to perform a common operation. **Figure 1** illustrates one typical setup of these units.

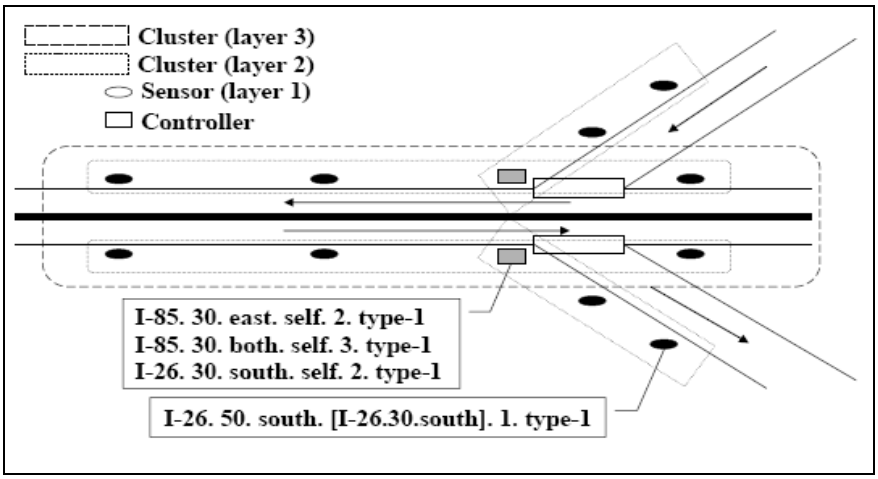

Figure 1: Hierarchical Network Architecture

- **A hierarchical addressing scheme** is used to identify sensors and controllers, inheriting convention of the U.S. highway reference system, where each highway or major arterial road has a unique road identification number (RID) and each location on the road is uniquely identified with its mileage from the road's starting point. The address format is shown in Equation 1.

[RID, Mileage, Direction, Cluster ID, Level, Class] (Equation 1)

A device can have one or multiple addresses according to whether it is located along one or between multiple highways (at an intersection or interchanges), respectively. Equation 1 also specifies the side of a road (bi-directional traffic sensors), the cluster(s) identifying the anomaly, such as a traffic incident), the levels of sensors and controllers involved in the detection and verification, and the one or multiple sensor classes involved (i.e. flow meter and video detector).

- **Message routing** among sensors and controllers is done in the hierarchical address space with specific emphasis on *simplicity for sensors* and *intelligence at controllers*. Route discovery is based on local broadcasts, with which each sensor discovers, records, and registers with 1) its immediate upstream and downstream neighbors along its associated road segment, and 2) its presiding level-one controller at one of the two intersections linking the road segment. The process is iterative, i.e., each level-one controller continues to discover, record, and register with: 1) its immediate adjacent controllers at the other ends of all its connected road segments, and 2) its closest level-two controller. The process is completed when the top-level controllers are reached. Thus, the hierarchical routing procedure will always forward messages along the roads. Sensors route messages up or down the same road (if the destination is on the same road), or towards its presiding controller. Controllers then route messages in one of four ways: 1) up or down the same road, 2) to an adjacent controller, 3) to its presiding controller, or 4) to its subordinate controller or sensor.

3.2 Distributed Anomaly Detection and Resolution

Based on the hierarchical architecture, data processing and decision making procedures are defined for sensors, controllers, and clusters. To illustrate the system design method, a hypothetical distributed incident detection and resolution system is presented in Figure 2. In this example, sensors placed at regular distances along a highway measure vehicle speed and traffic volume. The distributed detection algorithm consists of three phases: detection, verification, and notification. In detection phase, each sensor independently carries out a simple detection algorithm based on a traffic shock wave concept. When a "possible" anomaly is detected, the sensor invokes the verification phase by sending a query to its adjacent sensor on each side. If any queried sensor has already observed a corresponding shockwave, or

will see one within a specified period, the anomaly is said to be verified. In the third phase, the verifying sensor proceeds to notify its cluster controller. Upon receiving the detection notification, the cluster controller will determine its response with an anomaly resolution algorithm. In this example, the cluster controller's response is to immediate notify its upstream controller to perform traffic diversion.

The shockwave detection algorithm is based on the fact that an incident causes two shockwaves in the traffic flow. The backward moving shockwave progresses upstream against the flow of traffic, as vehicle queues begin to form and both speeds and flow decrease. The forward moving shockwave is formed when the number of vehicles traveling past the incident location reduces the demand to the downstream freeway. The sensors detect a backward or forward moving shockwave by identifying abrupt changes in the instantaneous flow volume. The shockwave detection algorithm is only one of many incident detection algorithms suitable for use in such a distributed sensor system.

With the hierarchical architecture, it is also possible to partition the detection tasks into multiple levels according to the scope of concerned and the decision complexity. Sensors are the lowest level entities in the system. In addition to collecting traffic data, sensors can choose to process the data into different forms of information according to their ability, and choose to report (or not report) selected information to their supervising controller, one level up the hierarchy. A local controller can choose to process reports from its subordinate sensors to make a detection or response decision; it can also choose to report further summarized information to a controller yet one level up the hierarchy. The actual number of controller levels can be determined by traffic authorities, or be self-configured based on the topology and relevance in traffic characteristics.

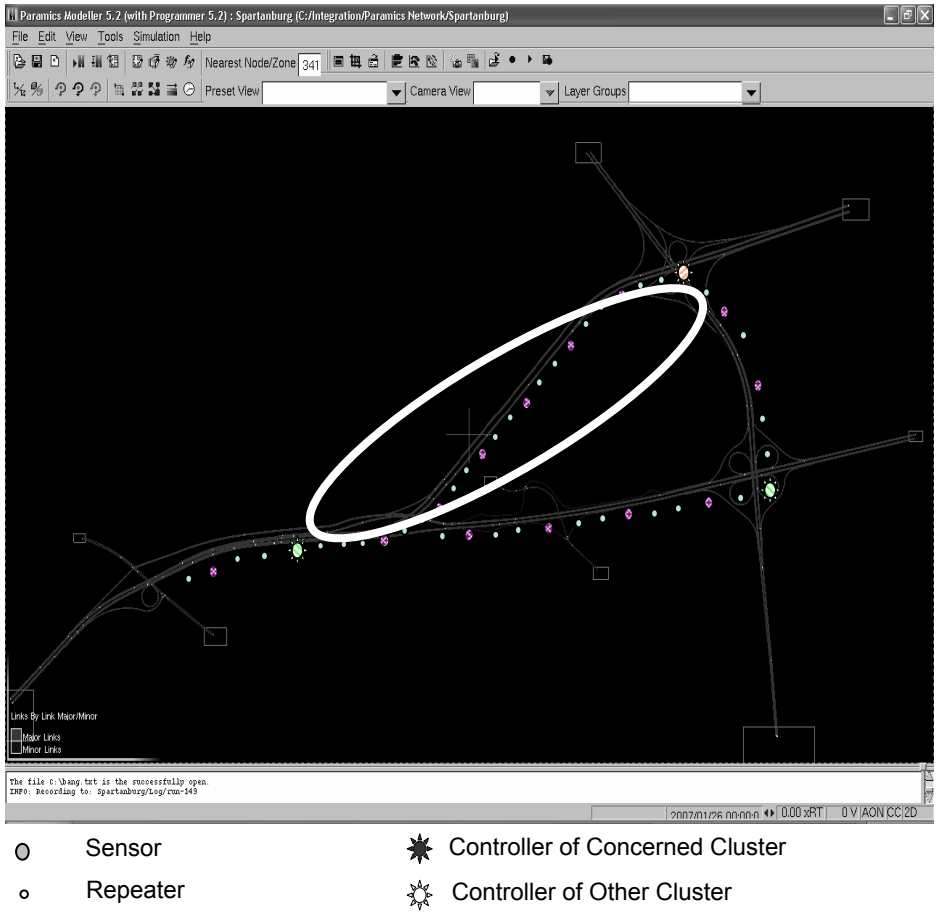

Figure 2: Simulated Freeway and Placement of Sensors and Controllers

3.3 Study Site

The freeway network shown in Figure 2 is in Spartanburg, South Carolina, containing three freeway corridors I-85, I-26, and I-85 Business, which meet and form a triangle. This figure shows this network as it appears in the PARAMICS microscopic traffic simulator. The I-85 segment is between exit 68 and exit 70, has high traffic volumes and a high occurrence rate of incidents that block all lanes, hence it was identified as the main link where anomalies would be generated in our simulation. The other two corridors served as the alternative routes for the main link.

After site selection, the research team used the PARAMICS simulation software to build, calibrate, and validate the roadway network. Network building began by collecting various data on site, including geometric, traffic control, and traffic volume data. The calibration process includes comparing the simulation volume output to the obtained on-site traffic count data, as well as comparing the simulator animation to the authors' field observation of traffic flow at the site. The validation process compared queue lengths and travel times collected during the site visits to those produced by the simulation model. After many iterations and adjustments to the road network and driver behavior, the simulation model accurately reflected the observed travel times within 1 percent and matched observed queue length.

4.0 ANALYSIS

This section presents selected results derived from an integrated simulator for traffic modeling and wireless sensor network communications. The simulator was created with PARAMICS and the network simulator ns-2. **Figure 3** presents the incident to upstream controller notification time, defined as the time-period between an anomaly occurs and when the upstream cluster controller is notified. Incidents were generated at different locations on the segment, at different distances to an upstream sensor. The top and bottom of each line marks the extreme values observed, while the solid bar represents the 95 percent confidence interval. The notification time is the sum of the time for sensors to detect and verify anomalies, which is a function of the traffic shockwave, and the latency for communication between the sensors and the controller, which depends on the designed sensor network topology. The notification time generally increased as the upstream sensor distance increased.

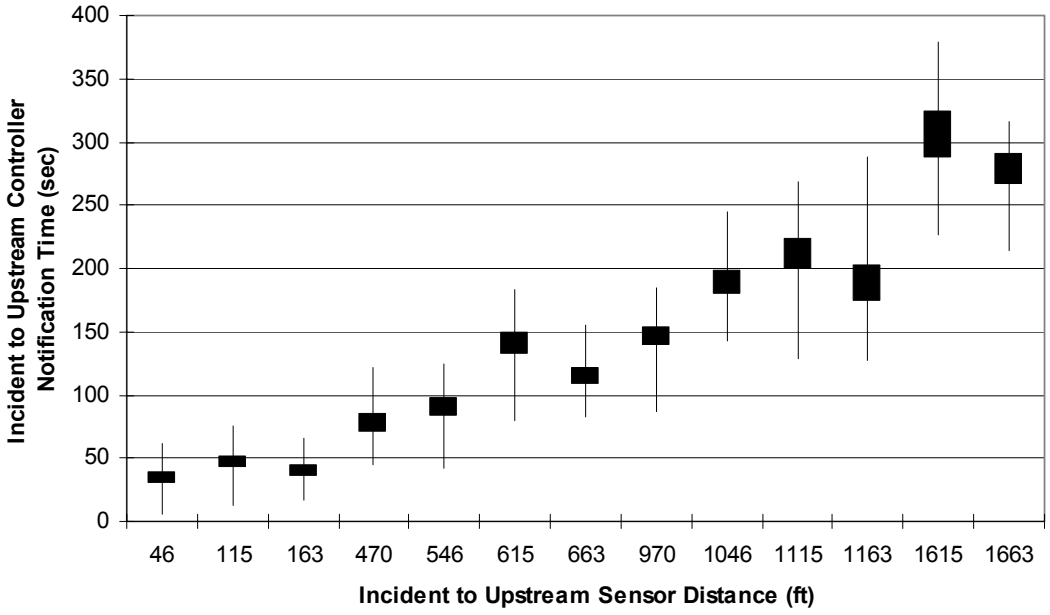

Figure 3: Incident to Upstream Controller Notification Time Versus Incident to Upstream Sensor Distance

An arbitrary number of experiments, 394, were conducted to study the detection rate and false alarm rate. For each experiment, a warm up period of ten minutes was configured to allow the simulated vehicle flow to approach a steady condition prior to any anomalies. Anomalies were randomly generated along the freeway link after this warm up time. The study found a 100 percent detection rate using its eight sensors. The false alarm rate was calculated both with respect to the number of detection attempts (Equation 2) and to the observation time (Equation 3).

False alarm rate = 8 / (394*10*60/30) false alarms per 30 sec (decision interval) = 0.001 / 8 (number of sensors) = 0.0125% (Equation 2)

Or

= 8 false alarms / (394 * 10 min) = 0.12 false alarms per hour (Equation 3)

A linear regression analysis of the incident to upstream controller notification time was conducted to illustrate how the simulation results can guide the adjustment of design parameters. As Figure 4 shows, the total time that an upstream cluster controller needs to be notified, increases linearly as the incident location to upstream sensor distance increases. The results suggested that the propagation speed of shockwaves dominates the anomaly notification time. As the distance between sensors increases, both the notification time and its variance increase. The simulation results indicated that higher sensor density will effectively enhance the detection latency and stable performance.

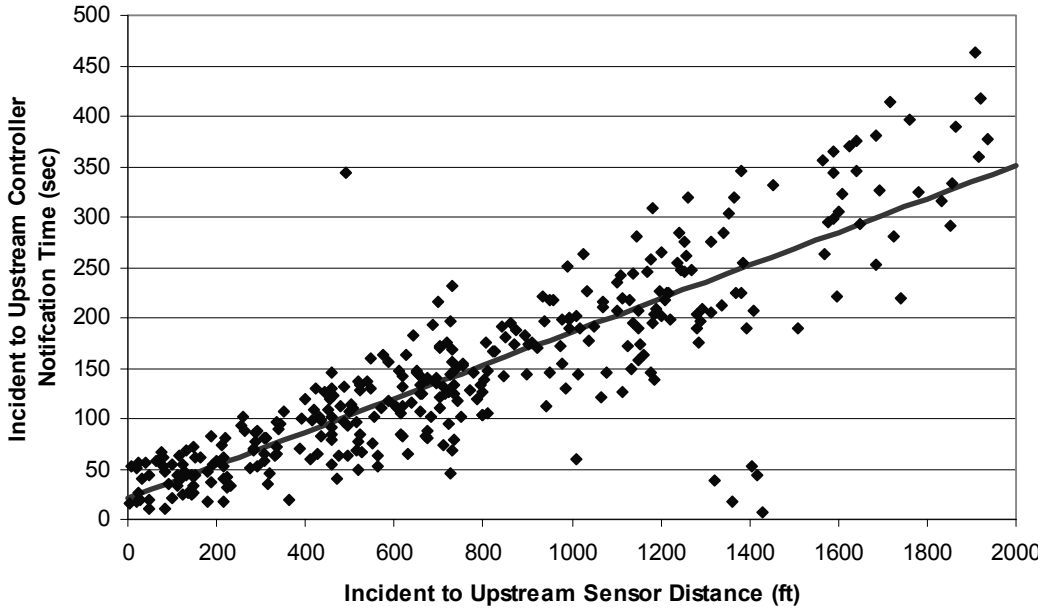

Figure 4: Linear Regression Model of Incident to Upstream Controller Notification Time versus Incident to Upstream Sensor Distance

In the simulated scenario, communication time was not significant compared to the overall anomaly detection time, which depended more on properties of the traffic flow itself (shockwave propagation speeds). The variation in communication time was, however, useful in understanding the potential disturbances to the correct execution of the distributed algorithms, enabling critical assessment of the system's correctness and reliability. Figure 5 shows the total communication latency, defined as the sum of the latency for communication between detecting sensor and verifying sensor, verifying sensor and downstream local controller, and local controller and upstream controller, versus the distance between the incident location and the downstream local controller. The farther the anomaly location was from the local controller, the more time was needed for the notification to reach the upstream controller because messages needed to be forwarded in multiple hops. The variance of the total communication time increased as the incident location became father away from the downstream local controller. Variations in communication latency are expected results of the concurrent communications by nearby sensors, who compete for wireless transmission opportunities in the

same channel following the adopted IEEE 802.11 random medium access control protocol. While relatively small compared to the traffic propagation latencies, it is essential that distributed traffic control procedures recognize the consequences of such random delays on the order of received messages for distributed decisions such as anomaly verification, notification, and so on. Such random delays must also be considered when handling real-time operations.

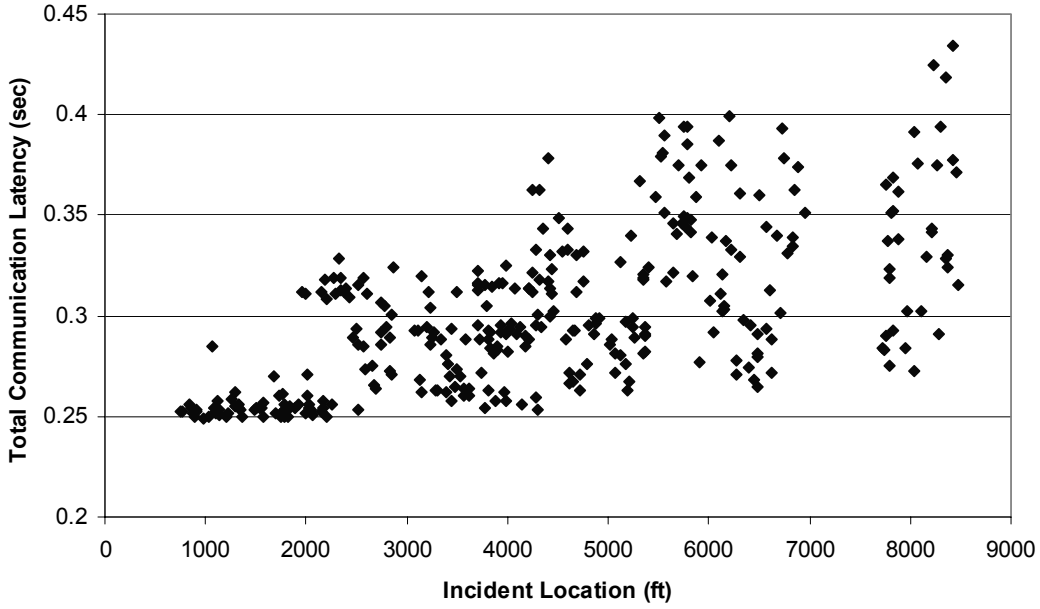

Figure 5: Total Incident Latency versus Incident Location as Measured from Downstream Local Controller

5.0 CONCLUSIONS

This research presented a hierarchical wireless sensor network architecture and distributed decision data processing and control decision paradigm that can potentially contribute to the incremental development of a large-scale traffic sensor system with specific emphasis on operation efficiency, traffic safety, and transportation security. The authors illustrated its application through the development of a simulated anomaly detection and response system using an integrated traffic and wireless sensor network simulator. Recommended future work includes developing distributed Artificial Intelligence (AI) based incident detection and verification system, which will adapt to the changing traffic environments. While simultaneous detections caused unforeseen communication latency, the communication times were not significant compared to the time required to detect the incidents. The simulation results revealed the dependency of detection performance on sensor density, showing opportunities and direction for improvement.

Like the Internet, the hierarchical and distributed nature of the proposed sensor network provides strength and resiliency towards security concerns in the national infrastructure. The hierarchical distributed wireless sensor network shifts responsibilities of highway surveillance, incident response and traffic control towards individual sensors and controllers, which will collaborate on site to implement designated traffic management functionality to enhance safety through more effective and efficient management. Furthermore, the distributed and hierarchical control methods reduce the possibility of entire system blackouts under any conditions by allowing the data processing and decision making to take place at different levels over the network. In the current safety- and security-conscious atmosphere, this characteristic will be a source of comfort for the government and the general public.

6.0 REFERENCES

1 K-C. Wang, M. Chowdhury, R. Fries, M. Atluri, Neeraj, Kanhere (2005), "Real-time Traffic Monitoring and Automated Response with Wireless Sensor Networks", *Proc. ITS World Congress*. San Francisco, November.

2 U.S. Department of Transportation, "Intelligent Transport Systems: Technology overview," http://itsdeployment.ornl.gov/technology_overview/, accessed 2006.

3 Hideo Tokuyama, "Intelligent Transportation Systems in Japan," http://www.tfhrc.gov/pubrds/fall96/p96au41.htm, 1996.

4 Cape Town, South Africa, "Traffic Signal Services," http://www.capetown.gov.za/atrams/, accessed 2006.

5 New South Wales, Australia, "Sydney Coordinated Adaptive Traffic System (SCATS)," http://www.rta.nsw.gov.au/trafficinformation/trafficfacilities/scats/, accessed 2006.

6 M. Chowdhury and A. Sadek, Fundamentals of Intelligent Transportation Systems Planning, Artech House, Inc. Maine, 2003.

7 M. Papageorgiou, C. Diakaki, V. Dinopoulou, A. Kotsialos, and Y. Wang, "Review of Road Traffic Control Strategies," in Proceedings of the IEEE, pp. 2043--2067, 2003.

8 Principles of SCOOT, Siemens, available online at <http://www.itssiemens.com/en/t_nav224.html>

9 SCATS, Traffic-Tech, available online at <www.traffic-tech.com/pdf/scatsbrochure.pdf>

10 RHODES, University of Arizona, available online at<www.sie.arizona.edu/ATLAS/docs/TRISTANIII.pdf>

11 D. Estrin, L. Girod, G. Pottie, and M. Srivastava. Instrumenting the world with wireless sensor networks. In International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2001), Salt Lake City, Utah, May 2001.

12 Sinem Coleri and Pravin Varaiya, "PEDAMACS: Power efficient and delay aware medium access protocol for sensor networks," California PATH Working Paper UCB-ITS-PWP-2004-6, 2004.