Distributed ITS Control and the Oklahoma Virtual TMC

Basel H. Kilani, Ekasit Vorakitolan, Joseph P. Havlicek, Monte P. Tull, and Alan R. Stevenson

Abstract— **Practically all major metropolitan and large scale modern intelligent transportation systems have a centralized traffic management center (TMC) at their logical and functional core. The TMC provides control, coordinates system wide communications, and typically serves as a common hub from which multiple agencies plan and execute coordinated incident responses. Early in the development of the Oklahoma statewide ITS, it became clear that the costs associated with building and operating a large, centralized TMC would be prohibitive. An alternative design strategy emerged built around a distributed peer-to-peer network of low-cost ITS consoles based on desktop PC's equipped with innovative software and special hardware to support efficiently handling multiple video streams simultaneously. This has led to a geographically distributed, fault-tolerant communications and control system where the desirable functionality of a large centralized TMC is realized by a virtual TMC that enables the stakeholder agencies to remain physical located in their current facilities around the State. In this paper, we provide an overview of the system architecture as it has evolved through the first quarter of 2009 and highlight some of the recently developed system enhancements.**

I. INTRODUCTION

A typical intelligent transportation system is comprised of a geographically distributed collection of ITS devices including sensors (*e.g.*, traffic and environmental sensors) and feedback devices (*e.g.*, traffic signals, dynamic message signs (DMS), advanced traveler information systems (ATIS), and ramp metering signals) which are connected together through a wide-area communication network. In broad terms, such systems are deployed to achieve the closely related goals of improving the efficiency of the transportation network and enhancing public safety. For example, video surveillance combined with powerful real-time interagency communication capabilities can improve the effectiveness of incident management while dramatically reducing incident response times, with the concomitant benefit of reducing secondary crashes. Overall efficiency of the transportation network is improved by providing travelers with timely traffic conditions and route selection information, as well as by improving the utilization of existing transportation infrastructure through means such as ramp metering and dynamic lane allocation. This saves both time and fuel expenditures by reducing congestion. In [1], the Texas Transportation Institute (TTI) concluded that the cost of congestion in the USA in 2005 was approximately USD 78B, including 4.2 billion hours of additional travel time and an expenditure of more than 2.9 billion additional gallons of gasoline. In the local Oklahoma City metro area, TTI estimated the 2005 cost of congestion at 21 hours of annual delay per traveler and 13 gallons of additional fuel expended per traveler for a total annual cost of USD 365 per traveler [1].

Both human and automatic control and coordination of intelligent transportation system resources are generally implemented via a monolithic, centralized traffic management center (TMC). The U.S. Federal Highway Administration defines the term *traffic management center* as follows [2]:

> "The TMC... is the hub of a transportation management system, where information about the transportation network is collected and combined with other operational and control data to manage the transportation network... It is ...a place where agencies can coordinate their responses to transportation situations and conditions."

Numerous U.S. states have deployed centralized TMCs for statewide, regional, and/or metropolitan area ITS control, including Florida, Texas, California, Georgia, New York, Washington, Utah, and others [3]–[9]. Many of these TMCs are based in major metropolitan areas such as Atlanta, Houston, Los Angeles, New York City, Salt Lake City, Seattle/Tacoma, and South Florida. The costs associated with deploying, operating, and maintaining these centralized TMCs can be *substantial*. For example, the cost of constructing the NaviGAtor TMC in Atlanta was approximately USD 13M in 1999, exclusive of software and systems integration costs [10]. Initial capital costs, software development costs, and systems integration costs for the Chicago, IL, TMC were approximately USD 14M in 2003 [11]. The Florida District IV SMART SunGuide TMC incurred initial capital costs estimated at USD 6.7M in 2006 [12]. In 2005, the estimated annual costs for operations and maintenance (O&M) at the Arizona TMC in Phoenix were USD 2M, nearly half of which were personnel payroll costs [13].

Although the full functionality of an integrated multiagency centralized TMC was considered highly desirable in Oklahoma, the costs associated with constructing, operating, and maintaining such a facility were deemed prohibitive [14]. As a result, a novel design concept for a low-cost, distributed, virtual TMC constructed using "commercial off-the-shelf" (COTS) desktop computers and, where possible, open source software emerged through a public-public partnership between the Oklahoma Department of Transportation (ODOT) and the University of Oklahoma Intelligent Transportation

This work was supported in part by grants from the Oklahoma Department of Transportation and the Oklahoma Highway Safety Office.

B. Kilani, E. Vorakitolan, M. Tull, and J. Havlicek are with the University of Oklahoma ITS Laboratory, School of Electrical and Computer Engineering, Norman, OK 73019, USA. {basel,ekasitv,tull,joebob}@ou.edu

A. Stevenson is with the the Oklahoma Department of Transportation, Technology Services Division, Oklahoma City, OK 73105, USA. astevenson@odot.org

978-1-4244-5521-8/09/$26.00 ©2009 IEEE

Systems Laboratory.

The virtual TMC is comprised of a geographically distributed fault-tolerant network of low-cost *ITS consoles*, each of which is capable of controlling ITS resources that are currently visible to it on the statewide private ITS network. Stakeholder agencies are not required to relocate to a central facility; rather, ITS consoles are deployed to their existing sites along with multiple channel voice over Internet Protocol (VoIP) capability to provide interagency voice communications that emulate the multi-agency incident management environment characteristic of a large, centralized TMC. In rural areas where fiber optic capability is not available, ITS consoles with limited multi-channel video capability can still be deployed provided that an Internet connection capable of supporting secure virtual private networks (VPNs) exists. The first ITS console was deployed in 2003 and, as of first quarter 2009, 45 consoles have been deployed statewide. It was remarked in [15] that the architecture of the Oklahoma statewide ITS "...enables the elimination of an expensive centralized TMC. Operators are connected by a peer to peer network into a virtual, geographically distributed, and fault-tolerant TMC" [15]. In this paper, we give a high level overview of the system as it has evolved through the first quarter of 2009 and highlight in more detail several of the important architectural and design changes that have occurred since 2005 [14].

II. Architectural Overview

The main feature that enables implementation of a full-featured statewide ITS in Oklahoma without a centralized TMC is the concept of a low-cost statewide ITS console. The console is a desktop personal computer (PC) with an Intel Pentium 4 CPU under the Windows XP operating system. In most instances, a pair of graphics cards capable of supporting four monitors and cable TV reception is added. The hardware cost is about USD 1,000 per unit. The basic elements of the ITS console software load were discussed in [14] and include an Apache web server, MySQL database, an open source GIS package called MapServer, php, and the Microsoft .NET framework. In the current software version, the Microsoft Message Queue (MSMQ) is required.

Under normal conditions where the network is fully connected, all consoles maintain a common database that fully describes the state of all devices connected to the network, including lists of all mutually visible ITS consoles. Changes in the network state are generally initiated by an ITS console and propagated throughout the network by message passing via MSMQ. For example, an operator at one console might take control of a pan-tilt-zoom (PTZ) camera; this state change would quickly be known to all consoles. Control is fully distributed and the system is fault-tolerant in the sense that in case of partial or catastrophic network failures, any group of connected consoles can continue to function and continue to control and manage all ITS resources visible within their group. Throughout the outage, database update messages destined for consoles that are not currently visible are queued until network connectivity is re-established.

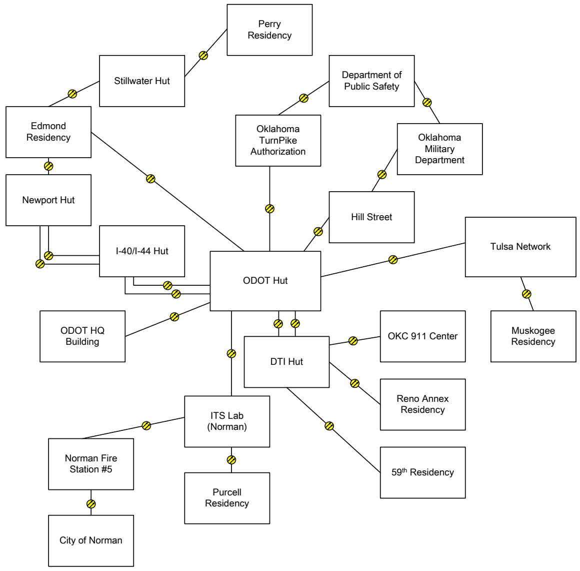

Fig. 1. Inherently distributed topology of the OK ITS network. The box marked *Tulsa Network* represents a packet switched multiagency network providing comprehensive connectivity throughout the Tulsa metropolitan area.

Certain features such as real-time weather data, speed data acquired from a network of Remote Traffic Microwave Sensors (RTMS), and certain work zone data are coordinated through a central Linux server and are not available at an ITS console during periods when the server is not visible. The main design philosophy is that any sufficiently privileged operator can be logged into any console at any time and can control/utilize all ITS resources currently visible to that console. In some cases, some or all of these functions are also available to sufficiently privileged operators through a computer located at their home and/or through a handheld device. Moreover, operators are able to make on-site decisions and post messages to a permanent or portable dynamic message sign (DMS) via web server interfaces from any location that provides hardwired or wireless Internet connectivity.

The network backbone consists of a Virtual Local Area Network (VLAN) implemented over a dedicated Gigabit Ethernet (GigE) network which enables connectivity between the ODOT Headquarters in Oklahoma City and ODOT Division offices around the State, as depicted in Fig. 1. The statewide private ITS fiber optic network was also recently extended to support connectivity for several large military installations throughout the State. With the cooperation of partners like the Oklahoma Transportation Authority (OTA) and the OneNet network for education and government, the dedicated ITS network now covers most of the State.

III. Details and Recent Developments

There have been several important changes made to the statewide ITS hardware and software designs since they were last reported in 2005 [14]. Many of these changes were made to accommodate the growing number of ITS consoles that have been deployed and the increasing amount of information that the ITS now accommodates. Throughout the improvements, cost and efficiency have remained high priorities and have not been compromised.

A. Fiber Backbone

To reinforce the network fault-tolerance, underutilized existing assets were used to implement a ring topology. Three additional communication paths were established using existing fiber cores. These can be seen in Fig. 1 as the connection between the Edmond ODOT office, labeled “Edmond Residency”, and the ODOT communications hut and the connection between the Oklahoma Turnpike Authority and the communications hut. These form cycles in the network graph and allow communications on multiple paths. The additional redundancy protects against network equipment outages and power loss of network devices such as routers and switches at any point along the ring. Unfortunately this cannot provide complete immunity against damage to buried cables from mishaps such as improperly planned excavations, which remain a threat to the system at this time.

B. Wireless Backbone

The demand for network resources used by ITS consoles and devices has increased considerably every year since the initial development of the statewide ITS. ITS resources are deployed to geographically dispersed locations where distance from maintenance facilities, geographic barriers, and especially cost make it prohibitive to deploy in-ground fiber networks [14]. Despite this limitation ITS resources are deployed further afield everyday. One technique that has been used in Oklahoma to overcome these obstacles is the deployment of Motorola Canopy PTP-400 point-to-point microwave links. These devices have been used for the transmission of streamed video data as well as for device control and they have introduced a wireless backbone into the ITS network where it is not feasible to deploy fiber optic cables. The PTP-400 can provide up to 60 Mbps of bandwidth and boost microwave signal transmission to a range of over 50 miles depending on the type of antenna installed. Operation can be at the public frequency of 5.8 GHz or at the licensed frequency of 4.9 GHz, which is allocated by the FCC for public safety. The PTP-400 can easily be installed as a network bridge at either urban or rural sites [16].

For example, Midwest City, Oklahoma is currently the largest subnetwork linked to the ITS network via a wireless bridge utilizing PTP-400s. This PTP-400 link provides bandwidth for 4 PTZ cameras, 16 web cameras, 2 DMSs, and 2 ITS consoles. This is a reliable and inexpensive alternative to the deployment of a buried cable network from Oklahoma City to Midwest City. Most data collection devices such as Remote Traffic Microwave Sensors (RTMS) and DMSs require relatively little bandwidth for operation; a dedicated PTP-400 is not needed to support such devices alone.

As an alternative for applications which require a smaller total bandwidth, 900 MHz radio has effectively filled this role. The use of 900 MHz radio is an appealing alternative because it operates at the public frequency and is near line of sight. The Orion 900 was the first radio used for DMS wireless communications in the Oklahoma ITS. The Orion 900 provides scalable data bandwidth of up to 5.5 Mbps using 5 MHz per channel, up to 11 Mbps using 10 MHz per channel, and up to 22 Mbps using 20 MHz per channel. With one watt output power and various external antenna types, the Orion 900 can support most of the metro, urban, and rural area needs for small bandwidth applications, especially in locations without existing data infrastructure [17]. The main down side of the Orion 900 is that it can only support an Ethernet interface. Many commonly used ITS devices require RS-232 or RS-422 interfaces, so adaptation is required with the Orion 900; this can lead to a high adapter cost, additional complexity, and a potential for hardware failure.

Networking options that use the public service network (cell-phone network) like Code Division Multiple Access (CDMA) modems have been considered for data retrieval and control systems for ITS devices in urban areas where investment in the dedicated ITS network infrastructure is not possible. However, using the public service network as a part of the ITS network is usually avoided due to security considerations and the reliability of the network during certain catastrophic circumstances. CDMA systems tend to be insecure and there is a history of exploitation of these systems by hackers to display inappropriate messages [18]. Also, the system is susceptible to weather phenomena such as tornados or other natural disasters leaving vital systems non-functional in times of emergency. On the other hand, CDMA modems have worked perfectly to support temporary deployments of mobile cameras in applications that do not require high levels of security and reliability.

As a replacement for the Orion 900, the COMMPAK IP made by ENCOM radio was utilized to mitigate the needs for adapters/converters. However, this comes at the expense of a lower data throughput. The COMMPAK IP operates at the 900-928 MHz ISM band having a throughput of 1.1 Mbps compared to the 11 Mbps of the Orion. Since the COMMPAK IP uses frequency hopping when it detects a high signal-to-noise ratio, the COMMPAK IP provides a reliable wireless network and is resistant to noise [19].

C. Devices

A variety of ITS resources are currently deployed and networked around the State as shown in Table I. These include but are not limited to the following.

1) 45 ITS consoles in various government agencies around the State, including 911 centers, Department of Public Safety, the Oklahoma Highway Patrol, municipal government agencies, and regional associations of municipal governments.
2) 210 analog pan-tilt-zoom (PTZ) and IP web cameras.
3) 18 permanent Dynamic Message Signs (DMS).
4) 57 microwave traffic sensors.
5) 6 Road Weather Information Systems (RWIS).

One of the main advantages of the statewide application is the ability to control different vendors' devices using a common software user interface. For each type of device

TABLE I
DEVICES SUPPORTED BY THE OK ITS CONSOLE

Device Type	Make	Model
Web Camera	AXIS	2140
	AXIS	221
	AXIS	2420
CCTV camera	Bosch	LTC-8560
	Bosch	LTC-8561
	COHU	3850
	COHU	3920
	COHU	3950
	COHU	3965
	VICON	SVFT-PR22
	VICON	SVFT-PR23
Video Encoder	TLC Watch	TLC-1000 software
	TLC Watch	TLC-1000 hardware
	iMpatch	i4000
	ATEME	VSS-111-F
	ATEME	VSS-110-F
	Indigo Vision	8000
	COHU	9900 i-link II
Traffic Sensor	EIS	RTMS
	Wavetronix	Smart Sensor
Permanent DMS	Skyline	Walk-in 3X25
Portable DMS	ADDCO	Brick

(*e.g.*, camera, DMS), the ITS console application software provides a single graphical user interface by which system operators can acquire and control devices of that type. Thus, the operator need never be concerned with the specific vendor for any particular device since the control surface will look and feel the same regardless. The vendor specific protocols are implemented in the database as stored procedures, which are invoked selectively based on the vendor identification field stored in the database for each deployed piece of equipment. In most cases, vendor specific functionality has been implemented such that the common control surface will show, *e.g.*, a control for a vendor specific functionality provided by vendor *A* when a camera manufactured by *A* is being controlled, but that functionality will be "grayed out" when controlling a camera manufactured by vendor *B* which does not provide the functionality.

D. Video Distribution

As described in [14], a novel closed circuit television (CCTV) system was designed to capture video data from full motion and web cameras not connected to the GigE backbone and also from select commercial television programs (*e.g.*, local news), as well as to provide video distribution to ITS consoles not connected to the fiber backbone. The CCTV system is like a private cable TV service, and most ITS consoles are equipped with a video tuner card that can switch channels under computer control to display one of the video streams multiplexed on the CCTV system. Over time, it became clear that interoperability between the CCTV system and the digital video streams present on the GigE backbone would be highly desirable. This capability was provided by introducing a bank of dedicated encoders and decoders that bridge between the GigE backbone and CCTV system, as shown in Fig. 2.

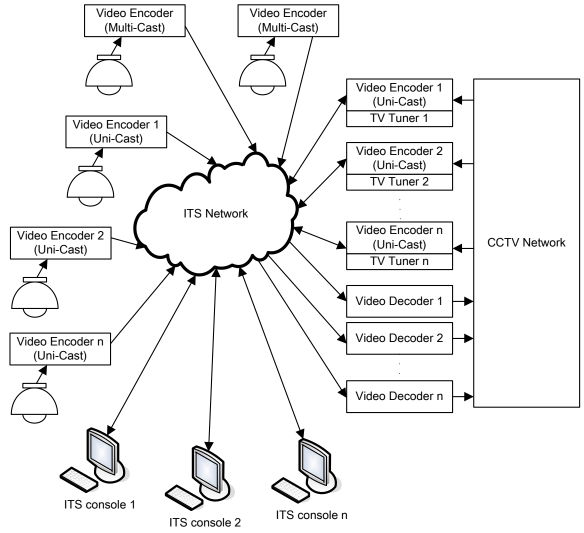
Video Encoder (Multi-Cast)
Video Encoder (Multi-Cast)
Video Encoder 1 (Uni-Cast)
Video Encoder 2 (Uni-Cast)
Video Encoder n (Uni-Cast)
ITS Network
Video Encoder 1 (Uni-Cast)
TV Tuner 1
Video Encoder 2 (Uni-Cast)
TV Tuner 2
Video Encoder n (Uni-Cast)
TV Tuner n
Video Decoder 1
Video Decoder 2
Video Decoder n
CCTV Network
ITS console 1
ITS console 2
ITS console n

Fig. 2. A bank of digital video encoders provide on-demand interoperability between the high bandwidth analog video distribution system, the packet switched digital video distribution system, and the lower bandwidth CCTV video distribution system.

The available broadcast options are 1) IP multicasting, 2) IP unicast or 3) IP multi-unicasting. Briefly, multicasting is broadcasting to all users regardless of their desire to receive the broadcast, Unicasting is broadcasting to a single user on request, and multi-unicasting broadcasts to several users, but only upon request. IP Multicasting consumes the most bandwidth but is also the most convenient because viewing simply requires connecting to the the video stream. There is a greater delay in the other two paradigms, since a request for the video must be issued by the user and the streaming must be negotiated. However, techniques (2) and (3) reduce the total amount of data broadcast to the network.

Video sources with high bandwidth network connections multicast directly to the GigE backbone, as indicated by the upper two cameras in Fig. 2. Consoles with fiber connections need only connect to the stream to view this video. Alternatively, sources with a smaller bandwidth connection instead use a unicast encoder to transmit the video to one of several decoders capable of rebroadcasting on the CCTV network. These decoders can also be used to switch one of the multicast video streams onto the CCTV system on an as needed basis for distribution to consoles that lack a fiber connection.

Since 2005, it has also been realized that the audio signals embedded in the RF modulators of the CCTV signals were not being used. This excess audio bandwidth was exploited to broadcast National Oceanic and Atmospheric Administration (NOAA) Weather Radio (NWR) and all hazard information. In addition, this audio channel can also be used to broadcast voice audio from ODOT managers for the purposes of coordination and control.

A mobile camera system was designed and implemented

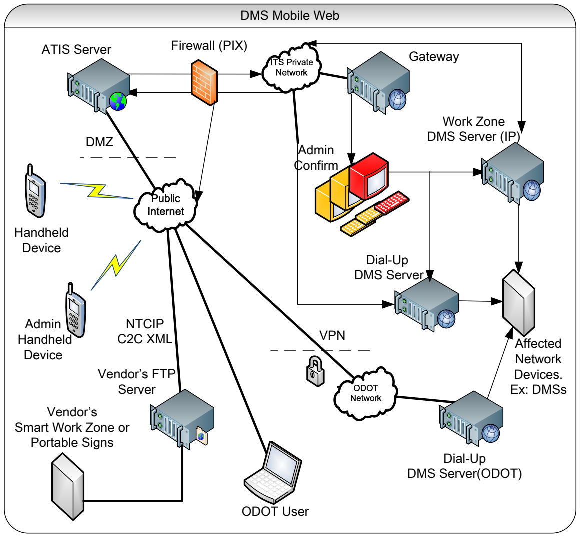

Fig. 3. Block diagram of DMS communications network.

where solar power is used as a power source for a single camera and a CDMA modem. The mobile camera is useful when a temporary system is needed to monitor traffic during special events. This system was deployed so that ITS console operators can view the traffic across the Oklahoma and Texas border during special events such as university football games that have historically generated significant congestion in the border area.

E. DMS Control/ Communication

A block diagram of the DMS control and communications subsystem is shown in Fig. 3. An important recent software development is the ability to use handheld mobile devices to post messages onto the DMSs. An authorized user submits a request to post a message to the DMS after logging into the DMS mobile website using any Internet browser on a mobile handheld. The request is sent to the list of available administrators, who can receive the requests via email on their handheld devices. The administrator that logs in first will view the request details and decide whether to accept or reject the request. In addition, other administrators may view the status of the requests that have been accepted or rejected. A service, running out of a dedicated work zone server, monitors the database of pending requests and sends the requested messages that have been approved. All the posted messages will have a specific priority that will be overwritten with higher priority messages such as AMBER alerts.

In addition, the DMS interface application has the ability to identify the appropriate communication port to be used based on the location of a specific DMS. In case of a failing communication port, for example, it will automatically alternate between attempts to send via IP using a terminal server connected to the DMS RS-232 port and sending directly to the DMS dialup port.

Recently, a commercial product called WebRelay from ControlByWeb was integrated into the ITS network. WebRelay is wired to the power inputs of devices that need to reboot frequently, such as DMS controllers. The administrator is able to cycle power on the DMS controller without sending anyone to the field sites.

F. Network Monitoring

Because the ITS network is dispersed around the state, the problems facing network maintenance are time, cost and man power. The Orion product from SolarWinds is currently being used as the main data network monitoring device using simple network management protocol (SNMP) and in-house network monitoring services to watch the network at all times. The network monitoring system notifies the network administrators by e-mail immediately when the network fails to respond. The network administrators are able to access a custom alarm web server to check where the problem is occurring. This monitoring system makes rapid network maintenance possible.

G. CDMA/Pix

As the Oklahoma statewide ITS has evolved, a need has emerged to provide ITS console functionality to users who do not have access to the secure private network. However, security is a great concern when considering this option. To handle security issues, a solid firewall system was built using Private Internet eXchange (PIX) and data encryption. This has allowed the ITS console to be provided to government agencies where the ITS private network is unreachable. Since every state agency already has Internet access, it is possible to simply set up the security encryption on the ITS consoles that are deployed. Operators can get video images through a bank of video encoders that are installed in communication huts. With two-way communications, the operators are able to control the camera pan, tilt, and zoom by using the ITS consoles in the same manner as they would on the ITS secure backbone network. ITS consoles have also been recently deployed to the homes of some critical managers. These managers can access and control ITS devices from their home by connecting to an ITS console through an ISP provided device if the appropriate security hardware is installed on their home machine.

H. VoIP

Public communication methods such as cellular telephony may not provide reliable communications to ITS devices such as DMSs during natural disasters and other catastrophic events. Ironically, these are often the times when it is most important for ITS system resources to be fully functional. Since the ITS backbone is able to support video and voice data, the ITS console has integrated Ventrino (a free VoIP application) into the system. Using this application, ITS operators can talk to each other via the ITS private network, which is based on reliable underground fiber optic networks. Teleconferences between agencies and groups of individuals can be quickly and easily organized, instantiated, modified, and dropped, effectively simulating the highly desirable interagency communications capabilities provided by a large, centralized TMC. An exciting new design effort currently under way will also use VoIP channels to implement virtual bridges to provide interoperability between multiple police and other first responder agency radio systems.

IV. Future Plans

ODOT is currently investing in a Network Trunking System (NTS) which allows for low data bandwidth communication around the state. Because the communication to a DMS is low bandwidth (2400 to 9600 bps), the current plan is to integrate existing ODOT radio system infrastructure into the ITS network to control DMS devices. Another approach under consideration is to manage incoming RS-232 control messages being received via various modalities such as WiFi, air-card, and dedicated radio links by deploying a small computer at each DMS site specifically for this purpose. This has the advantage of providing inherently redundant connectivity to the DMS in case one or more communication modalities fail.

OneNet received authorization to implement the WiMAX around OKC for government agencies. A partnership is planned to use the existing ITS camera poles for installation of the WiMax equipment.

An alarm system is being developed based on the open source TCP/IP stack (AN883) from Microchip Technology Inc. [20], hence giving the alarm module low-cost functionality. The alarm module will be installed at the communication huts and the cabinets. It will monitor the door, temperature, UPS battery level, main power condition, and air-conditioning operation among other variables. When any alarm event occurs, the alarm module will send the input value to the server via User Datagram Protocol (UDP). The server will notify the administrator of both minor and major alarms via e-mail. With the UDP protocol and the push (from alarm to server) topology, a limit is placed on the alarm data being sent around the network.

Road surface conditions from RWIS stations are being combined with Global Positioning System (GPS) data acquired from maintenance vehicles to realize a comprehensive Automatic Vehicle Location (AVL) capability in the near future. It is unclear at this time if the mapping software will be open source or a commercial product such as Microsoft Virtual Earth. A travel time algorithm is also being developed to send automatically updated travel times to both permanent and temporary DMSs.

References

[1] D. Schrank and T. Lomax, “The 2007 urban mobility report,” Texas Transportation Institute, The Texas A&M University System, Tech. Rep., Sep 2007.

[2] U.S. Department of Transportation, Federal Highway Administration. Using highways during evacuation operations for events with advance notice – glossary. Visited May, 2009. [Online]. Available: http://ops.fhwa.dot.gov/publications/evac_primer/26_glossary.htm

[3] ITS Florida TMC Co-location Task Force. regional transportation management center co-location white paper. Visited May, 2009. [Online]. Available: www.i95coalition.net/i95/Portals/0/Public_Files/uploaded/Incident-toolk%it/documents/Policy/Policy%20_Co-Loc_FL.pdf

[4] Houston TranStar. 2008 annual report. Visited May, 2009. [Online]. Available: http://www.houstontranstar.org/about_transtar/docs/Annual_2008_TranStar%.pdf

[5] Calif. Dept. Transp. Los Angeles Regional Transportation Management Center. Visited May, 2009. [Online]. Available: www.cio.ca.gov/Government/ITawards/pdf/2008CrossBoundaryCollaborationan%dPartnershipsCaliforniaDepartmentofTransportationLARTMC.pdf

[6] Georgia Dept. Transportation. About navigator. Visited May, 2009. [Online]. Available: http://www.georgia-navigator.com/about

[7] New York City DOT. Motorists: Real-time traffic cameras. Visited May, 2009. [Online]. Available: http://www.nyc.gov/html/dot/html/motorist/atis.shtml

[8] Washington State Dept. Transportation. Traffic operations: Traffic management centers (tmcs). Visited May, 2009. [Online]. Available: http://www.wsdot.wa.gov/Operations/Traffic/tmc.htm

[9] UDOT CommuterLink. Visited May, 2009. [Online]. Available: http://www.commuterlink.utah.gov

[10] “Metropolitan transportation management center, a case study: Georgia navigator,” U.S. Dept. Transportation, Washington, DC, Tech. Rep. EDL 11494, Oct 1999. [Online]. Available: http://ntl.bts.gov/lib/jpodocs/repts_te/11124.pdf

[11] Research and Innovative Technology Administration (RITA). The initial capital costs for software development and systems integration at the Chicago TMC were estimated at $4 million. Visited May, 2009. [Online]. Available: /www.itscosts.its.dot.gov/its/benecost.nsf/ID/D0014FAE3228F763852573E90%064A8DA?OpenDocument&Query=CApp

[12] ——. Florida DOT District IV 2006 budget supports a variety of SMART SunGuide transportation management center programs. Visited May, 2009. [Online]. Available: www.itscosts.its.dot.gov/its/benecost.nsf/ID/FD2D9EE0DA5E6DE18525727400%659AF0?OpenDocument&Query=CApp

[13] M. Wolf, D. Folds, J. Ray, and C. Blunt, “Transportation management center staffing and scheduling for day-to-day operations,” Human Systems Engineering Branch, Georgia Tech Research Institute, Tech. Rep. FHWA-OP-06-XXX, Jan 2006. [Online]. Available: http://tmcpfs.ops.fhwa.dot.gov/cfprojects/uploaded_files/Final_Technica%l_Document1.pdf

[14] R. Huck, J. Havlicek, J. Sluss, Jr., and A. Stevenson, “A low-cost distributed control architecture for intelligent transportation systems deployment in the state of oklahoma,” in *Proc. IEEE Int’l. Conf. Intel. Transportation Syst.*, Vienna, Austria, Sep. 2005, pp. 919–924.

[15] M. Darter, K. Yen, B. Ravani, and T. Lasky, “Literature review of national developments in ATMS and open-source software,” California AHMCT Program, University of California at Davis and California Department of Transportation, Tech. Rep. F/CA/RI-2006/10, Dec 2006.

[16] Motorola Canopy PTP 400 series user guide. Visited May, 2009. [Online]. Available: http://canopy-wireless-solutions.com/Products/PTP/Manuals/PTP400UM.pdf

[17] Wireless Interactive Communications Inc. Orion 900 MHz wireless. Visited May, 2009. [Online]. Available: http://www.wirelessinteractive.com/pdf/radios/Orion900_manual.pdf

[18] The Associated Press. Hackers’ road sign pranks worry highway officials. Visited August, 2009. [Online]. Available: http://www2.tbo.com/content/2009/feb/04/hackers-road-sign-pranks-worry-%highway-officials/

[19] ENCOM Wireless Data Solutions. Commpak ip - wireless ethernet/serial transceiver. Visited May, 2009. [Online]. Available: http://www.encomwireless.com/index.php?option=com_docman&task=doc_downl%oad&gid=80\&Itemid=53

[20] Microchip Technology Inc. Microchip tcp/ip stack application note. Visited May, 2009. [Online]. Available: www.microchip.com/stellent/idclg?IdcService=SS_GET_PAGE&nodeId=1824&app%note=ern011993