EVALUATION OF COMMUNICATION ALTERNATIVES FOR INTELLIGENT TRANSPORTATION SYSTEMS

Final Report

South Carolina Department of Transportation

SCDOT

Principal Investigator

Ronnie Chowdhury Ph. D., P.E.,F. ASCE

E-mail: mac@clemson.edu

Intelligent Transportation Systems Group

Clemson University

CLEMSON UNIVERSITY

Technical Report Documentation Page

1. Report No. FHWA-SC-10-03	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Evaluation of Communication Alternatives for Intelligent Transportation Systems		5. Report Date August 31, 2010 6. Performing Organization Code
7. Author(s) Mashrur Chowdhury, K.C. Wang, Ryan Fries, Yan Zhou, Lee Tupper, Jennifer Ogle, Tahera Anjuman, Vikram Bhide, Parth Bhavsar		8. Performing Organization Report No.
9. Performing Organization Name and Address Department of Civil Engineering Clemson University Clemson, SC 29634		10. Work Unit No. (TRAIS) 11. Contract or Grant No.
12. Sponsoring Agency Name and Address South Carolina Department of Transportation 955 Park Street P.O. Box 191 Columbia SC 29202		13. Type of Report and Period Covered May 1, 2008 – August 31, 2010 14. Sponsoring Agency Code
15. Supplementary Notes		

16. Abstract

The primary focus of this study involved developing a process for the evaluation of wireless technologies for intelligent transportation systems, and for conducting experiments of potential wireless technologies and topologies. Two wireless technologies: Wireless Fidelity (Wi-Fi) and Worldwide Interoperability for Microwave Access (WiMAX) were chosen to demonstrate the proposed evaluation process. The authors performed numerous field tests on these technologies to evaluate various critical parameters of wireless communication. The authors also implemented a network design process using Wi-Fi and WiMAX technologies to support a traffic surveillance system in seven metropolitan areas of South Carolina. Additionally, a video surveillance test was conducted to study the transmission of real-time traffic video over a wireless network. Making use of the results from the field study, the authors applied a communication simulator, ns-2, to compare the communication performance of a traffic sensor network under simulated environmental conditions. They also built an integrated simulator using ns-2 and a vehicular traffic simulator, PARAMICS. This integrated simulator was then used to study the communication behavior of the system during traffic incidents. Additionally, the authors conducted a performance-cost analysis for selected wireless technologies. This study provided an important foundation for evaluating the performance and reliability of different wireless technologies. The research results presented in this study will benefit the SCDOT, other transportation agencies, and stakeholders in evaluating and selecting cost-effective wireless communication options for different traffic control and management applications.

17. Key Words Communication, Intelligent Transportation Systems, Wi-Fi, WiMAX	18. Distribution Statement No restrictions.		
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. Of Pages 244	22. Price

TABLE OF CONTENTS

LIST OF FIGURES

Figure **Page**

LIST OF TABLES

Table **Page**

ACKNOWLEDGEMENTS

Special thanks to the SPR 676 Steering Committee for their guidance to the research depicted in this report. We would also like to thank Dan Campbell, Director, SCDOT Intelligent Transportation Systems Division, for his support and guidance to the research team throughout the project; and the traffic management centers in Greenville, SC and Columbia, SC for their timely assistance. We would also thank Drs James Martin and James Westall, of the School of Computing, Clemson University, for their assistance with the WiMAX field study.

EVALUATION OF COMMUNICATION ALTERNATIVES

FOR

INTELLIGENT TRANSPORTATION SYSTEMS

Executive Summary

Communication systems enable effective and reliable traffic control and management applications. Although fiber optics and telephone lines have long been used for managing and controlling highway traffic systems, wireless communication technology shows great promise as an up-and-coming solution in traffic management applications due to the flexibility for deployment and cost-effectiveness for system expansion.

There have been few studies aimed at developing a process for systematically evaluating emerging wireless technologies for intelligent transportation systems. In addition, the reliability and performance of these wireless communication technologies have not been systematically examined. Therefore, the primary focus of this study involved developing a process for the evaluation of wireless technologies for intelligent transportation systems, and for conducting experiments of potential wireless technologies and topologies.

To achieve this objective, the authors first conducted an interview to identify the specifications of existing communication infrastructures deployed for various ITS related applications and the usage of wireless technologies in different states. Two wireless technologies: Wireless Fidelity (Wi-Fi) and Worldwide Interoperability for Microwave Access (WiMAX) were chosen to demonstrate the proposed evaluation process. The authors performed numerous field tests on these technologies to evaluate various critical parameters of wireless communication. The authors also implemented a network design process using Wi-Fi and WiMAX technologies to support a traffic surveillance system in seven metropolitan areas of South Carolina. A video surveillance test was conducted to study the transmission of real-time traffic video over a wireless network. Making use of the results from the field study, the authors applied a communication simulator, ns-2, to compare the communication performance of a traffic sensor network under simulated environmental conditions. They also built an integrated simulator using ns-2 and a vehicular traffic simulator, PARAMICS. This integrated simulator was then used to study the communication behavior of the system during traffic incidents. Additionally, the authors conducted a performance-cost analysis for selected wireless technologies and topologies.

The case study results identified the key limitations for both Wi-Fi and WiMAX technologies. The Wi-Fi field test indicated that wireless communication performance between two traffic sensors significantly degrades after 300 ft with an off-the-shelf radio employing transmission power up to 70 mW and omni-directional antennas. This distance was observed to vary with the modulation rates and transmission power used by the system. The WiMAX nomadic test suggested that line-of-sight (LOS) greatly affects the connectivity level. Moreover, the capabilities and the performance of the WiMAX network are affected by the specifications of the client radio. Through a video-transmission field test, the research team found that a jitter threshold of one second and a packet rate of 23 packets per second were sufficient for acceptable quality of traffic surveillance video.

The performance-cost analysis indicated a Wi-Fi mesh network solution has the highest throughput-cost ratio (109 bits/dollar) for supporting traffic surveillance systems. The research team found that the WiMAX infrastructure option provides the greatest amount of throughput (9.15Mbps per device) allowing for future system expansion.

A simulation analysis using ns-2 revealed the effects of environmental parameters on the multi-hop behavior of a WiFi traffic surveillance network. An analysis using the integrated ns-2 and PARAMICS simulations revealed that in order to facilitate a low false incident detection rate, the sensor spacing is critical. During this simulation, communication latency was found to have a low impact on the incident detection performance.

Although the researchers conducted multiple field tests and considered numerous simulation analyses, the SCDOT may need to carry out additional field studies before adopting a wireless communication option. For this reason, a detailed evaluation process is described in this report, providing a systematic method for evaluating new and/or existing deployments of ITS communication infrastructure. This report also presents an implementation strategy for applying the methodology during further studies.

To facilitate better management of the ITS infrastructure and to support its future expansion, a suitable asset management system is necessary. The researchers conducted a study wherein three asset management platforms were analyzed. They determined that as the SCDOT already implements enterprise based Geographic Information System (GIS) for other applications, the best option would be to extend its use for ITS applications rather than implement new software. However, because this transition may take time, off-the-shelf ITS asset management software may be a feasible option if SCDOT wishes to implement a system in the short term. If this latter option is used, databases developed for the off-the-shelf system are expected be transferable to the enterprise system with minimal effort.

This study provided an important foundation for evaluating the performance and reliability of different wireless technologies and topologies. The research results presented in this study will benefit the SCDOT, other transportation agencies, and stakeholders in evaluating and selecting cost-effective wireless communication options for different traffic control and management applications.

.

1 INTRODUCTION

Advanced transportation management relies on timely traffic information exchange between the various elements that make up a highway transportation system in order to make informed decisions and implement appropriate operational strategies. Intelligent Transportation Systems (ITS) involves the integration of information technology with the existing traffic infrastructure to resolve transportation problems and enhance mobility and safety. Passing processed information between roadside devices and traffic management centers can provide motorists with regular updates about traffic conditions, and incidents can be rapidly identified to reduce congestion and save lives. Failure or poorly performing communication systems, especially during emergency conditions or on key traffic infrastructures, will significantly affect the traffic management and operations. Poor operation can not only cause traffic delays and air pollution, but can also result in loss of property and increased risks of secondary crashes after traffic incidents. Therefore, a fast, reliable and cost-effective communication system to transmit real-time traffic information is of paramount importance.

1.1 Problem Statement

The National ITS Architecture presents possible communications between different subsystems via both wireline and wireless communications (USDOT 2007). The architecture defines three subsystems namely the center (e.g., traffic management centers, public transit management centers, and emergency management centers), the field (e.g., sensor, controller) and the vehicle (e.g., personal, commercial, and transit). The communication layer of the physical architecture identifies four major types of communications to support the communication requirements. For example, the centers-to-centers or the centers–to-roadside are connected mostly by wired communication systems. However, they can also be connected by wireless communication systems.

Presently, most of the transportation data and informations in the US is transferred from the field to the Traffic Management Center (TMC) via fiber optic cables, either owned by public agencies or leased through commercial carriers. However, wired systems that provide communication to individual system components, such as traffic detectors and field personnel, can be problematic due to lack of development in some areas where these components must operate. Because of the nature of system components, a wired system might be disabled completely in some cases under adverse conditions such as a hurricane. On the other hand, a wireless system may still be capable of supporting partial transmission. Furthermore, with the increased demand of on-line traffic management systems to cover the entire highway system, expansion of the wired system to such a wide scale can be costly. Moreover, the leased communication lines cost traffic agencies millions of dollars every year, and will increase during ITS expansion in the near future.

The demands of faster, more efficient and more reliable communication systems for ITS applications increase the requirements for high-speed broadband communication technologies. In recent years, wireless communication systems have received increasing attention for on-line traffic management due to their suitability for deployment in rural areas, the flexibility to support various applications and the cost-effectiveness for system expansion. For example, in rural areas where communication infrastructures are limited, or when one of the system components is mobile/remote, such as vehicles in the vehicle-infrastructure integration /IntelliDrive concept, wireless communications are preferred (Ma et al. 2008). The use of wireless transmission of traffic video and other information, which require high bandwidth, could reduce overall costs and allow for more rapid and flexible data transmission. Additionally, wireless communication is more tolerant in certain undesirable conditions when compared to the wired system, because it might maintain a partial connection in adverse conditions while wired systems might be down entirely.

Although traffic agencies and professionals are very interested in widely using broadband wireless technologies to support on-line traffic management in the near future, selecting and implementing a communication alternative to satisfy different ITS application needs can be challenging. Key technical factors involved are not clearly understood by traffic agencies, and they have concerns regarding the actual performance in the field when supporting various kinds of traffic control devices (Zhou[1] et al. 2009) because many potential factors could degrade the communication performance, even shut down the connection entirely. There are also concerns of the functional ability and reliability of using wireless technologies in adverse conditions such as bad weather (Zhou[2] et al. 2009), terrian and foliage covered areas. For instance, during Hurricane Katrina, both wired and wireless connections were destroyed by storm surges and flooding leaving the area vulnerable due to insufficient connection to inland emergency services.

Therefore, the research motivation is to identify the optimized location and operation strategies to deploy the sensors and wireless access points to implement the traffic sensor network that is technically feasibile, reliable and commerically cost-effective. As more and more regions throughout the United States moved towards deploying large scale wireless communication-based ITS networks to improve the traffic safety, efficiency and mobility for both daily and emergency situations, many communications options will sooner or later spring up. Information regarding their relative costs and benefits would become increasingly important for making implementation decisions. To assess the cost effectiveness, reliability, and adequacy of this communication infrastructure, there must be efforts undertaken to survey, evaluate, and model current and future communication alternatives and corresponding network infrastructures. However, there have not been any comprehensive studies conducted to cover this knowledge gap.

A careful and rigorous analysis of the existing infrastructures and future alternatives will assist the traffic agencies and professionals in selecting and implementing an appropriate ITS communication infrastructure, creating both short and long-term plans for technology integration, reliability enhancement, management, and efficient investment to improve nationwide mobility.

1.2 Study Objectives

This research has three study objectives to fulfill. The first objective is to identify existing wireless communication technologies that have been used in ITS and potential wireless communication alternatives that could be widely used in future ITS applications. The second objective is to develop a process for evaluating potential wireless technologies and topologies for ITS applications. The third objective is to evaluate the performance and cost of potential wireless communication technologies and topologies.

1.3 Report Outlines

The following categorized chapters present detailed study, analysis and discussion of the conducted research. Section 2 presents the literature review of characteristics of existing and potential wireless technologies, their applications, and previous research efforts that studied their performance and reliability when used under different traffic and environmental conditions. Section 3 presents the methodology which the authors utilized to interview selected public agencies, and to perform case study, field tests, simulation analysis and benefit-cost analysis. Section 4 presents a summary of interview responses. Section 5 reviews with the Field tests conducted in the course of the study. In Section 6 the authors present the network design case studies for seven metropolitan cities. The simulations conducted for this study are presented in Section 7. The results of performance-cost analysis are discussed in Section 8. Section 9 showcases the evaluation of selected asset management systems. Finally, section 10 summarizes the implementation strategy which provides a guide for SCDOT to use the research results. Lastly, Section11 lists the research findings, as well as presents the authors' recommendation regarding the implementation of the current work and future research based on the analysis presented in this study.

2 LITERATURE REVIEW

This section provides the readers the following information.

- Handbooks and other references related to communication systems used in traffic management and operation
- Technical characteristics of potential wireless communication technologies that can be used for ITS
- Existing applications and research effort in using wireless communications technologies for ITS

2.1 Handbook and Other Guidelines

In order to help public transportation agencies obtain better understanding of wired and wireless communication for ITS applications and assist further implementation, there are various documents developed under Federal Highway Administration (FHWA) sponsorship (Gordon et al. 1993; 2005; Neudorff 2003; Leader 2004; Klein et al. 2006). The *Communications Handbook for Traffic Control Systems* surveyed various available communication mediums, system architectures for traffic control applications (Gordon et al. 1993). Another handbook, *Traffic Control Systems Handbook*, reviewed the emerging technologies and control concepts, system architectures and their applications for planning, designing and implementing traffic control systems (Gordon et al. 2005). The *Telecommunications Handbook for Transportation Professionals* introduced the history and basic concepts of telecommunications systems used to transmit voice and data information (Leader 2004). The *Traffic Detector Handbook* comprehensively surveyed the operation, application, design, installation and maintenance of traffic sensor technologies. All of these handbooks provide decision-making process and trade-off analysis to serve as a guidebook for selecting and designing functional, effective, reliable and economical communication system for advanced traffic control.

2.2 Wireless Communication Technologies Suitable for ITS

Wireless communication technology has long been considered as an alternative to traditional fiber optics and telephone communications solutions for traffic management applications. Several studies have previously been conducted to recommend various wireless communications for ITS applications (Cai 2005; Smith 2004; Yang et al. 2000; Stephanedes et al. 1996). The Federal Highway Administration commissioned a survey with state agencies of available wired and wireless communication infrastructures for traffic control system and found a significant need to understand the performance and reliability of communication infrastructures for managing and implementing traffic signals and freeway management systems (Hwang 2006). Among wireless technologies, this survey listed Wi-Fi, cellular and satellite as potential wireless technologies for traffic management and control systems. Another study sponsored by FHWA evaluated the performance of various Digital Subscriber Line technologies (xDSL) with both laboratory experiments and field tests (Jones 2002). That study implemented high speed data services (e.g., 2 Mbps) with xDSL on the existing twisted pair wire for transferring traffic video images, and their field studies showed that the xDSL technologies were able to maximize the DSL throughput.

The review presented in this section focuses on three emerging wireless technologies; WiMAX, Wi-Fi, and DSRC. The contents in the following section will provide readers the general characteristics, strengths, and weaknesses of using each technology in ITS environments. It also aims to provide practitioners with a useful reference of wireless technology features.

2.2.1 WiMAX

WiMAX, Worldwide Interoperability for Microwave Access, has attracted global attention due to its high-speed broadband access, broad coverage and easy extension to suburban and rural areas. It is based on the IEEE 802.16 family of standards and designed to deliver high-speed wireless broadband access to fixed, nomadic and mobile users (Filis 2007). Fixed WiMAX provides communication between one base station and a number of fixed client devices. With mobile WiMAX, clients can maintain connection to the network through a base station at any time, handing off from one base station to another when moving through the stations' respective coverage areas. One such example is the connected subscriber located in vehicles moving at high rates of speed. Fixed WiMAX also supports nomadic applications, in which clients have devices that can change locations but do not expect continuous network connectivity when they move, hence requiring no hand-off support among base stations. Theoretically with the 802.16m released in April 2010, the WiMAX link rate can reach up to 300 Mbps and coverage can extend over 20 miles (White paper WiMAX and the IEEE 802.16m Air Interface Standard - April 2010). Though there is a tradeoff between coverage range and achievable link rate. A major benefit of WiMAX technology is the wide range of available profiles with different channel bandwidths from 1.75 MHz to 20 MHz, which can satisfy different ITS application requirements with an efficient bandwidth usage. WiMAX can operate in both licensed and un-licensed frequency bands.

A typical WiMAX network, which consists of base stations and client radios called Customer Premise Equipment (CPE), is similar to cellular phone networks. A WiMAX base station provides point-to-multipoint service to client radios within its radio range (Vassilopoulos 2007). The throughput that can be expected from a WiMAX base station depends greatly on whether the client possesses a line-of-sight (LOS) connection to the base station. With a strong LOS signal from the base station to a client radio, a WiMAX network can support traffic cameras, mobile Internet applications, and other ITS components. If there is an obstruction between the base station and client, such as dense foliage or a building, the service range and achievable rate may be lower and not symmetric in all directions away from the base station (Broadcom 2006).

2.2.2 Wi-Fi

Wi-Fi, short for wireless fidelity, refers to the IEEE 802.11 family of standards and currently provides wireless access in hotspot-type short-range low-cost, high-bandwidth and low-latency coverage (JIWIRE 2008). While there has been discussion on replacing Wi-Fi with WiMAX, the two technologies differ greatly. Indeed, these tools are more effective when complementing one with another to provide different services under different circumstances (Dusit 2007). With a higher capacity and communication range, WiMAX is better suited for outdoor applications, while Wi-Fi is primarily used for short-range indoor or outdoor applications. One way to integrate of these two is to create a high-speed wireless access network with WiMAX providing backhaul support for mobile Wi-Fi hotspots (Dusit 2007). Theoretically, though the Wi-Fi link rate can reach up to 54 Mbps, the coverage range is less than 0.4 miles (Broadcom 2006). Early Wi-Fi contained a fixed channel bandwidth of 20 MHz, but recently released IEEE 802.11n can support 600 Mbps using a 40 MHz channel bandwidth (Broadcom 2006). Field performance of Wi-Fi using 802.11n still requires further study.

If designed correctly, an optimized Wi-Fi network can support multiple types of ITS components at relatively high throughputs. Wi-Fi networks have the benefit of being the lowest-cost solution for providing wireless access to remote sites, and well-known Wi-Fi technology can add redundant connectivity by enabling mesh mode operation of the access points. Wi-Fi networks can support any ITS components that send non-critical data, as they do not provide any delay or bandwidth guarantees. Further, because Wi-Fi operates in unlicensed frequencies that are open to public access, communication interference is more likely to occur than in licensed frequencies.

2.2.3 DSRC

The third emerging wireless technology discussed in this study is Dedicated Short Range Communications (DSRC). DSRC, based upon IEEE 802.11p standards, was initiated by the USDOT for supporting Vehicle Infrastructure Integration (VII) applications for ITS (UC Berkeley 2006). VII, also known as IntelliDrive, provides a communication platform for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications through various mobile wireless radio technologies. DSRC has been used to support electronic toll collection in Europe and Japan, and it also has the capability to support a large set of additional applications (ITSSA 2003). Some of these include intersection collision avoidance, transit vehicle signal priority, emergency vehicle preemption, commercial vehicle clearance and safety inspection, in-vehicle signing and probe data collection (Schnacke 2004). Similar to Wi-Fi, an ITS deployment containing DSRC base stations can provide relatively high throughput at high speeds over short range of 0.6 miles or less. Unlike Wi-Fi, DSRC uses one fixed, licensed, channel bandwidth of 10 MHz. While WiMAX and DSRC both operate in FCC-licensed frequency bands, a key advantage of DSRC technology is that it has very strict latency and error-rate control. Although, the DSRC link rate can reach up to 27 Mbps theoretically, the coverage range is still less than 0.6 miles.

2.3 Applications in ITS

While wireless technologies is gaining increasing popularity in traffic control and management, there is a need to re-evaluate communication strategies for use in online traffic management and traffic safety applications at a much larger scope and finer granularity. Traffic control communication technologies must cover wider areas and connect with substantially more field devices than ever before.

Previous field evaluations of performance and reliability on different wireless technologies have been carried out by many transportation agencies. Kentucky Transportation Center implemented and evaluated a base-station-based wireless communication technology as part of their TRIMARC traffic management system in 2002 (Hunsucker 2002). This study tested the applicability of a 220MHz wireless communication system to transmit traffic measurements from field sensors to a traffic management center. The 220 MHz wireless system was found to be equal to or better than the leased phone line in terms of functional reliability and cost effectiveness.

Virginia DOT studied several emerging wireless technologies, such as Mobile WiMAX, Software-Defined Radio, Cognitive Radio, and Femtocell short range cellular. These technologies have the potential to significantly affect traffic management and operations and vehicle-to-vehicle and vehicle-to-roadside communications in the future (Ammana, 2008). This study evaluated the field performance of wireless broadband technologies and topologies, spectrum usage and future investment opportunities. It also recommended departments of transportation to evaluate and implement emerging communication technologies to support operations and interoperability between agencies.

The domain of wireless communications has seen a lot of advancements over the past few years. The Texas Department of Transportation (TXDOT) studied the trends and impact of market available wireless communication in future Advanced Transportation Management Systems (ATMS) deployment, in an effort to move forward to provide robust, scalable and cost efficient ITS technologies (Brydia et al. 2008).

The three wireless communication technologies (WiMAX, Wi-Fi, and DSRC) have already been commonly used for different ITS applications in the US and all over the world. The following section discusses real word applications and research effort of wireless technologies in ITS.

2.3.1 WiMAX

Although WiMAX is a new technology, it has been used worldwide to provide broadband wireless service. After the December 2004 tsunami in Aceh, Indonesia, all communication infrastructures in the area, other than Ham radio, were destroyed. Survivors were unable to communicate with anyone from the outside and vice versa. WiMAX provided broadband access that helped regenerating communication to and from Aceh to assist in disaster recovery (BWEM 2006). Similarly, after Hurricane Katrina in 2005, WiMAX was used by Intel to assist the Federal Emergency Management Agency (FEMA) in their efforts to establish communication in the areas affected by flooding (NOAA 2006). In 2007, the Michigan DOT established a wide area VII testbed on interstates I-96 and I-696, in and around Oakland, Michigan. Their testbed integrated several communications technologies; namely DSRC, cellular and WiMAX (Horsley 2007).

WiMAX technology has been utilized by California DOT in the recent years for providing wireless communication service to travelers. In 2006, the Berkeley Highway Lab deployed a WiMAX testbed to support a 3-mile traffic monitoring system which includes 8 cameras and 168 loop detectors on a segment of interstate I-80 (BHL 2006).

To understand the characteristics and performance of WiMAX network, some studies have been previously conducted to assess the WiMAX communication performance under different applications (Gray 2007,Filis et al. 2007, Chen 2007, Martin et al. 2008). WiMAX Forum (Gray 2007) combined many efforts and evaluated the performance of a minimal configuration based WiMAX. They reported that WiMAX can meet stringent requirements to deliver broadband service in a mobile environment. They also demonstrated the advantages of mobile WiMAX compared with other mobile wireless alternatives in terms of superior throughput and spectral efficiency.

Chen (2007) analyzed the capacity and overhead of using WiMAX as backhaul and found that it can provide adequate backhaul transport at certain modulation compared with traditional licensed band microwave backhaul. Filis et al. (2007) presented an urban nomadic WiMAX network's stationary test result in which the maximum throughputs of both downlink and uplink can be observed at the distance of 500 m away from base station under non-line of sight (NLOS) environment. Martin et al. (2008) analyzed the performance of a 4.9GHz WiMAX network which consisted of 1 base station and 6 subscriber stations at Clemson University, South Carolina. This study observed the application level throughput ranges from 0.64Mbps to 5.1 Mpbs, which was 13% lower than expected.

With the trend of deploying WiMAX network for ITS, some researchers have identified the operational feasibility in different applications (Niyato and Hossain 2008, Chen 2007,Bultitude et al. 2007, Wang 2007, Zhou[3] et al. 2009). Niyato and Hossain (2008) introduced an integrated WiMAX and Wi-Fi network architecture for ITS by providing optimal priced mobile hotspot services. Chen (2007) described a WiMAX and Wi-Fi integrated emergency management system that can spread the wireless communication coverage area and guarantee the efficient emergency operation.

Bultitude et al. (2007) studied a mobile WiMAX server housed in an emergency vehicle for public safety applications. Wang et al. (2007) evaluated the performance of two non-stationary vehicle-to-vehicle channels and found that the WiMAX system performance in the non-stationary channel is more volatile than that in stationary channels. Zhou[3] et al. (2009) evaluated the performance and feasibility of using a regional WiMAX network to support fixed and nomadic applications in the highway environment. This study found that besides the LOS, the communication performance at client side also depends on the types of client radio used.

Overall, studies on WiMAX indicate significant promise for application supporting transportation operations. Not only has it been proven in a variety of frequencies, but also for a variety of uses by different independent studies.

2.3.2 Wi-Fi Mesh Networks

Several other transportation agencies have studied the usage of Wi-Fi in an ITS environment (Ammana 2008; Brydia et al. 2008; Hwang et al. 2006). The USDOT, comparing Wi-Fi and WiMAX for advanced public transportation systems, found Wi-Fi to be cost effective for corridor and small deployment, and WiMAX more suitable for large scale, long distance applications (Hwang et al. 2006). The Virginia DOT also evaluated the performance and capability of Wi-Fi and WiMAX for statewide transportation operations (Ammana 2008). Their study found that compared to Wi-Fi and the other wireless technologies studied; WiMAX can potentially provide more robust wireless communication links. The study also found Wi-Fi and WiMAX networks to be very dependent on the terrain characteristics and available infrastructure for mounting antennas.

The City of Phoenix has deployed a Wi-Fi mesh network for traffic surveillance cameras and traffic signals. The network operates in both the unlicensed 2.4 GHz and the 4.9 GHz public safety spectrum. The mesh network connects to the city’s fiber network for backhaul to a monitoring room in police headquarters that is staffed by two officers

(Crunch 2006). A recent implementation of a Wi-Fi-enabled ITS network was created by the California DOT (Caltrans) to add traffic surveillance to bridges and tunnels in the San Francisco Bay area. Caltrans deployed sixteen miles of point-to-point Wi-Fi links operating in the 5GHz spectrum. These links can handle a typical throughput of 90 Mbps, and support video-over-IP transmission of the surveillance data (Brydia et al. 2008).

2.3.3 DSRC

DSRC (Dedicated Short Range Communication) has been receiving increasing attention in owing to its usage in VII and related ITS applications. With VII test beds being implemented in California, Michigan, and Minnesota, more and more research, mostly in the three states, have focused on using DSRC to meet the needs of mobile or nomadic applications. For instance, VII-enabled vehicles periodically report to the infrastructure about their on-board measurements, such as travel time, location, and maneuver parameters; roadside units can report useful information to vehicles, such as traffic flow, density, incidents and control information. A California VII research group designed a VII pedestrian safety system that enables V2V and V2I communication for transmitting pedestrian detection signals (Chan 2006). They also designed a cooperative active safety warning system to alert slippery road conditions (UC Berkeley 2005). Such studies have found that communications between roadside infrastructure and vehicles can improve safety and mobility.

2.4 Wireless Performance Evaluation

Any effective transportation management applications require reliable communication systems. Previous catastrophic events and natural disasters, such as September 11 and Hurricane Katrina, indicate that wireless networks seem to be more affected by transmission errors due to external environmental interferences, lack of transmission power and terrain characteristics (Heidemann et al. 2004, Gordon et al. 2005).

Many studies have been performed to gain a better understanding of the performance and behaviors of the wireless sensor networks. Among the existing evaluation efforts, some measures of effectiveness (MOEs) were recognized as the most important indicators of the performance of the communication system. Gordon et al. (2005) summarized possible attributes such as bandwidth, signal attenuation, latency, power consumption, signal-to-noise ratio, bit error rate, and error control technique as the fundamental MOEs for evaluating performance of communication networks. Some researchers chose throughput and packet delivery ratio or packet reception rate as MOEs to illustrate the performance of wireless communication under various environments (Zhao and Govindan 2003). While measuring the packet delivery ratio of a dense wireless sensor network in an indoor office building, an environment with moderate foliage, and an open parking lot, Zhao and

Govindan (2003) found the delivery ratio to be affected by the communication range in this environment.

In addition, the quality of service assurance, the delay and jitter control of the video motion image were also widely used MOEs to assess the performance of the communication network (Ramachandra et al. 2004). Ramachandra et al. (2004) evaluated the performance of wireless ad hoc networks in terms of throughput, average routing overhead, packet delivery ratio, and end-to-end delay across diverse architectures. They discovered that the multi-hop architecture had a much greater packet delivery ratio and throughput than ad-hoc architectures. Multi-hop networks, while similar to ad-hoc networks, differ in that their nodes are relatively fixed to each other, which may result in hierarchical network architecture. A similar study of packet loss pattern and the potential reasons for packet drops was conducted on a 38-node network composed of 802.11b radio devices in a Boston (MA) urban environment (Aguayo 2004).

Although these studies highlighted many important MOEs, such as throughput and packet loss ratio, used to capture the wireless communication performance, the wireless ad hoc network used in traffic management applications have different requirements, such as bandwidth, architecture design and deployment. Jones (2002) considered throughput and video image/motion quality as the MOEs for evaluating communication systems that support traffic surveillance systems using CCTV. Osafune (2004) used maximum throughput to analyze the performance of a wireless ad hoc network for vehicle-to-infrastructure communication. Gallanger et al. (2006) tested the sensor communication range and packet error rate for both the vehicle-to-vehicle and road-to-vehicle communication under highway situations. Xu et al. (2004) assessed the reception reliability and channel usage of DSRC architectures under various traffic and vehicular traffic flows, such as different data rate, packet size and vehicle density.

The Texas DOT identified the number of devices, communication link bandwidth and latency as the important criteria for evaluating communication alternatives (Brydia et al. 2008). Besides analyzing the link-level behavior of wireless network by measuring the packet drop rate, Bai et al. (2006) developed an analytical model to relate application level reliability with communication reliability and vehicle safety communication parameters. The study found that DSRC can provide adequate communication reliability since, even under the harshest freeway traffic environment, the packet drops do not occur in bursts, meaning consecutive packet losses. Kim et al. (2007) developed a framework to simulate and study vehicle ad hoc network. Because the nodes in most wireless ad hoc networks compete to access the shared wireless medium, the communication performance may be affected by this competition, also known as collisions. These studies have characterized the performance of individual sensor links and point-to-point communication applications.

Many recent research efforts also have been undertaken to study the impacts of key factors on video quality, and corresponding minimum performance requirements. Typically, data transmission of real-time video has specific requirements of bandwidth, delay and loss (Wu et al. 2001). Those factors also serve as the key indicator of video quality, and provide a client the ability to specify the quality requirements (Joe 1996, Endoh et al. 2008, Baskaran et al. 2005, Ferries 1990, Lu et al. 2009, Koul 2009). Ferrari (1990) proposed a set of performance specification such as delay bounds, throughput bounds and reliability bounds from a client’s viewpoint to achieve certain video quality requirements. More importantly, Ferrari concluded that compared to throughput, delay bounds are more significant in digital video and audio communication, especially in the form of jitter bounds. Joe (1996) stated that real-time video communication over a packet switching network is subject to packet loss and random delay variation which causes significant performance degradation, video discontinuity, and even additional packet loss. Joe’s study also found out that real-time video protocol which control the delay jitter and packet loss result in good reception video quality. Lu et al. (2009) used packet losses and delay jitter as importation parameters to evaluate the video quality based on network statistics. Similarly, Koul et al. (2009) examined several objective video quality assessment methodologies and concluded information regarding to packet loss and frame jitter are the only required features at the receiver side to evaluate the quality. Moreover, Endoh et al. (2008) stated that interactive video steaming applications, such as remote control or tele-surgery, demands extremely low delay and low jitter. Again, Ngatman et al. (2009) compared several existing multimedia transmission techniques and found out that both the jitter delay and packet loss must be both solved to fulfill the standard quality performance. Baskaran (2005) evaluated the performance of live compressed motion image transmission via utilization of the 5.8 GHz Outdoor Wireless LAN network. Overall, these studies indicate that jitter control and packet loss are the two standard metrics for video transmission quality.

The transmission power used by wireless devices achieves and ensures the wireless network connectivity (Wang 2005, Park and Sivakumar 2002, Krunz 2004). Park and Sivakumar (2002) specifically mentioned that because the transmission power of the wireless devices in a network determines the network topology, this power may considerably impact the throughput of the network and the energy consumption of the devices. Krunz (2004) introduced several transmission power control approaches to increase throughput, and discussed the transmission power selection. Wang et al. (2005) also found that the packet reception ratio can be increased by dynamically adjusting the power setting of radio transceivers.

Wireless sensor network applications have been studied for use in traffic management (Heidemann et al. 2004, Wang et al. 2005, Kiyotaka et al. 2006, Chowdhury et al. 2007, Cheung 2007, Hyoungsoo et al. 2007). Heidemann et al. (2005) studied the feasibility of using wireless sensor network in short term traffic monitoring and data collection. Wang et al. (2005) proposed to wirelessly connect traffic sensors and controllers to enable them to collaborate within the network to monitor traffic and report detected events in real time. Kiyotaka et al. (2006) studied the radio propagation for a wireless ad hoc networks constructed at both railway stations and waysides. Chowdhury et al. (2007) also proposed and evaluated a distributed sensor network to detect and respond to incidents along freeway through simulation study. Cheung et al. (2007) developed and tested a novel wireless sensor network for traffic surveillance in California. His test results showed this type of network functions better than the typical inductive loop detectors in terms of reliability, flexibility and accuracy.

2.5 Wireless Network Topology

Communication network can be deployed under various topologies, also called configurations, which define the interconnection pattern and routing paths between nodes (Peterson and Davis 2003). Typically used network topologies includes centralized and distributed. Distributed topology can be deployed in several different patterns, such as ad-hoc topology or mesh topology.

2.5.1 Centralized Network

State-of-the-art traffic surveillance systems around the world have been built with an emphasis on centralized observation and control (USDOT 2006; Tokuyama 1996; City of Cape Town 2005; New South Wales Road and Traffic Authority 2006). Transportation agencies deploy as many sensors as affordable along the highway and establish Traffic Management Centers (TMCs) at central locations to collect data from sensors for making centralized control decisions. Substantial investments have been made to connect all sensors to central or regional controllers with dedicated communication links. Following predetermined schedules, roadside sensors transmit data to TMCs, where human operators identify possible incidents from the continuous data streams and initialize a response if an incident is detected.

Several problems arise from the existing centralized traffic surveillance networks. First and foremost, the required dedicated communication infrastructure is prohibitively expensive as a system grows in coverage and number of sensors, thus making wide deployment difficult as a system expands to broader suburban and rural areas. Dedicated communication infrastructure and centralized control centers are also vulnerable to terrorist attacks and natural disasters.

2.5.2 Distributed Network

Distributed control concepts are not new to traffic control systems. To optimize traffic delays locally, traffic signal controllers have been long organized into local clusters. State-of-the-art traffic signal control systems include: Split, Cycle, Offset Optimization

Technique (SCDOT) (Siemens 2006), Sydney Coordinated Adaptive Traffic System (SCATS) (Tyco Integrated Systems 2006), and RHODES (Real-time Hierarchical Distributed Effective System) (Mirchandani and Head 1998). While these methods may be effective for today's traffic control, they have been limited to the scope of fixed signal control clusters, and have required expensive communication infrastructure. In Coifman and Ramachandran (2004), The authors outlined a vision of deploying intelligent sensors along highways that could engage in distributed sensing and local data processing to report only concise information to TMCs or other responsible controllers if an anomaly is detected. The strength of this approach lies in the ability of sensors and controllers to make collaborative decisions without human intervention.

The tradeoff between constant centralized control capability and communication cost needs to be carefully balanced. In existing on-line centralized traffic management systems, communication links continuously send data from traffic sensors to staffed centralized TMCs for assessment. As these data frequently require no traffic management action, unnecessary communication costs are incurred. In addition, these systems are vulnerable to single point of failure and suffer from scalability issues. With distributed-only systems, there is no single point of control; however, it is more difficult to implement system-wide optimization.

2.5.3 Wireless Ad-hoc Networks

Among various wireless communication topologies, wireless ad hoc networks are one of the emerging technologies in which different nodes communicate with each other directly without the need of any access points or base stations. This type of operation allows wireless devices that are within range of each other to find and communicate in a peer-to-peer fashion without the need of a fixed infrastructure to provide central access points (NIST, 2008). Compared to traditional wired communication systems, wireless ad hoc network provides a possibility to construct large-scale networks for various ITS applications. Because wired system, such as fiber optic, can be very costly at large scales, wireless ad-hoc network provides a cost-effective alternative or supplement to a wired system.

In a wireless ad hoc network, nodes determine the paths to forward data based on network connectivity. Each sensor can only communicate with the other sensor within their communication range and the maximum communication range depends on the transmission power. Aside from network connectivity, transmission power also affects the link performance between two adjacent sensors.

Previous studies have investigated the use of wireless ad hoc network technology to support advanced traffic management strategies (Heidemann et al. 2004, Wang et al. 2005, Kiyotaka et al. 2006, Chowdhury et al. 2007, Cheung 2007, Hyoungsoo et al.

2007). Traffic sensors, also considered as roadside devices, can be deployed along highways to detect and record traffic information in real time. Since each node is directly connected to other nodes by an ad hoc wireless network interface, the detected traffic information is transmitted from one successive node to the next, finally arriving at a traffic management center (TMC) for further processing. This processed information exchanged between roadside devices and traffic management centers can provide TMC with the most updated traffic conditions for use in rapidly identifying incidents to reduce congestion, fuel use, emissions, and save lives. Thus, wireless communication can support more effective and efficient traffic management applications.

2.6 Summary of Literature Review

The selected three wireless communication technologies, Wi-Fi, WiMAX and DSRC, have been used for various ITS applications worldwide and have shown great promise for providing broadband access, cost-effective operations, and easy system expansion in the future. However, traffic agencies have concerns about the real performance of these potential technologies in the field under various physical and environmental conditions while supporting different types of bandwidth demanding devices. The effect of different factors, such as distance, transmission power, foliage coverage, weather and terrain, to the wireless link performance are needed to be identified and further quantified. Moreover, the maximum distance between the traffic sensors (devices or repeaters) that support reliable system performance required intensive field studies. Additionally, some of the previous research studied the data gathered from sensors encompassed traffic flow information, such as speed and flow. This information, which is of a light load and insensitive to delays, does not have the same substantial communication bandwidth requirements as does a camera-based traffic surveillance system that sends streaming video to traffic management centers. Research is needed to comprehensively study the field performance, coverage range and deployment feasibility of wireless communication technologies used for traffic sensor network, including video based systems.

Selecting and applying appropriate wireless technologies in specific ITS applications requires several steps including selection of technology and network topology, sensor deployment, power supply and benefit-cost analysis. Few studies have proposed a systematic method that can guide traffic agencies to select the suitable technologies from the array of options currently available and build their own wireless systems for specific ITS applications. For example, limited studies actually discussed the deployment feasibility of a regional WiMAX network for ITS applications in terms of performance and coverage. The relationship between sensor distance from WiMAX base stations and signal loss pattern, as presented in this study, provides tools to investigate the potential of WiMAX highway traffic sensor network. Therefore, a general design method has not been previously presented to help transportation agencies and other stakeholders in selecting wireless communication options and building networks for different traffic control and management applications.

Two commonly used tools for evaluating the wireless communication used in ITS are field study and simulation analysis. Simulation tools attempt to mimic the traffic management and operation under different alternative communication technologies and network topologies. There has been limited research undertaken to utilize simulation tools to evaluate both wireless communication and traffic operation performance of using wireless communication technologies to support online traffic management, such as incident management performance under different network topologies.

This study aims to contribute to the knowledge of performance and reliability analysis of different wireless technologies and topologies for ITS applications. As limited literatures exist in the area, this study will provide good guidance essential for future ITS applications and research.

3 METHODOLOGY

Advanced transportation management relies on timely traffic information for making informed decisions and implementing appropriate operational strategies. One of the most important strategies used in Intelligent Transportation Systems (ITS) for managing and controlling highway traffic is real-time communication and data exchange between the various elements that make up a highway transportation system. These elements consist of different subsystems: center, roadway, vehicle and driver (Figure 1). The center subsystem includes various stakeholders in highway traffic operations, such as traffic management centers, public transit management, motor vehicle departments, and law enforcement agencies. The roadway subsystem includes roadside devices such as traffic signal controllers, traffic cameras and traffic detectors. This study focuses on the communication between centers and field devices, and between field devices.

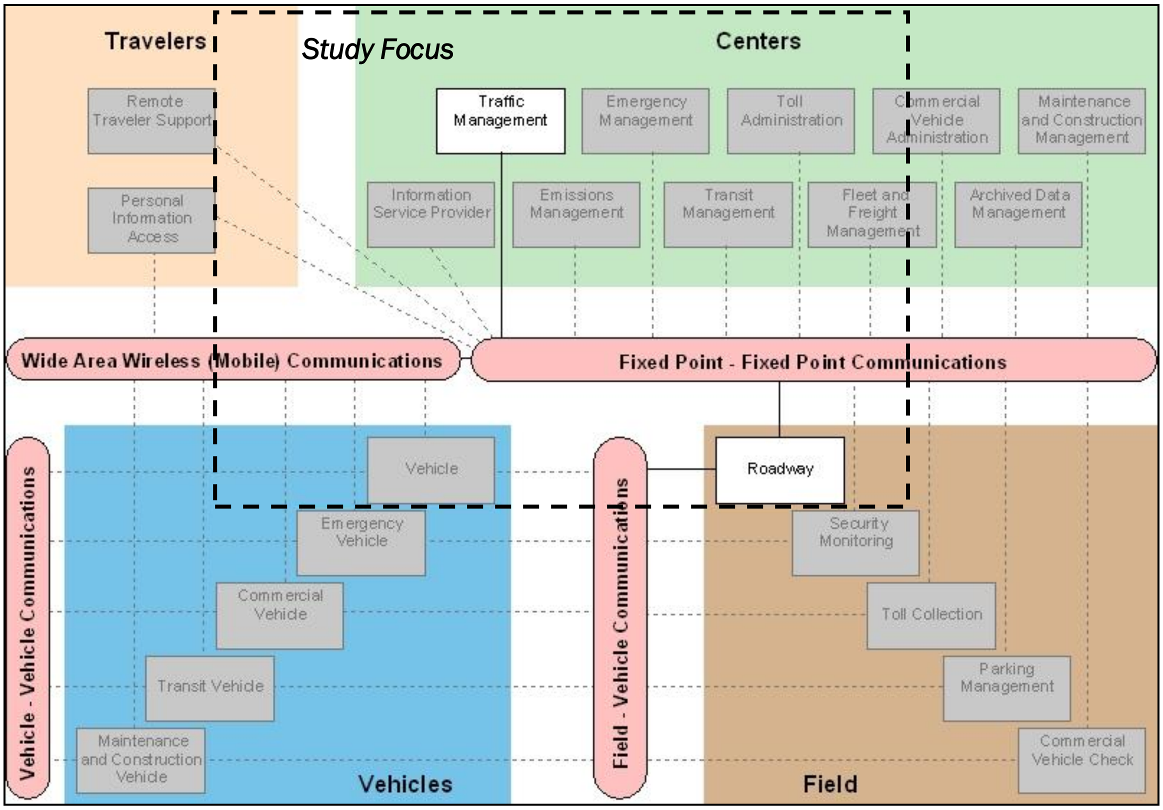


Figure 1: Study Focus (U.S. DOT 2007)

This study methodology can be presented in a manner shown in Figure 2. First, through a literature review, the study identified wireless communication technologies and network deployment strategies that could potentially be used in ITS. Then, an interview was conducted to identify traffic agencies' experiences and expectations related to those potential wireless technologies used in existing applications. A copy of the interview questionnaire is included in Appendix A.

With their increasing popularity newer and newer wireless technologies are coming to forefront. From the time the authors started working on this project there have been quite a few upgradations to the technologies that transportation agencies considered for evaluation. Hence this report lays a framework for the transportation personnel to conduct a similar work. The mesh and infrastructure topologies for two potential wireless technologies; Wi-Fi and WiMAX were considered in the case study.

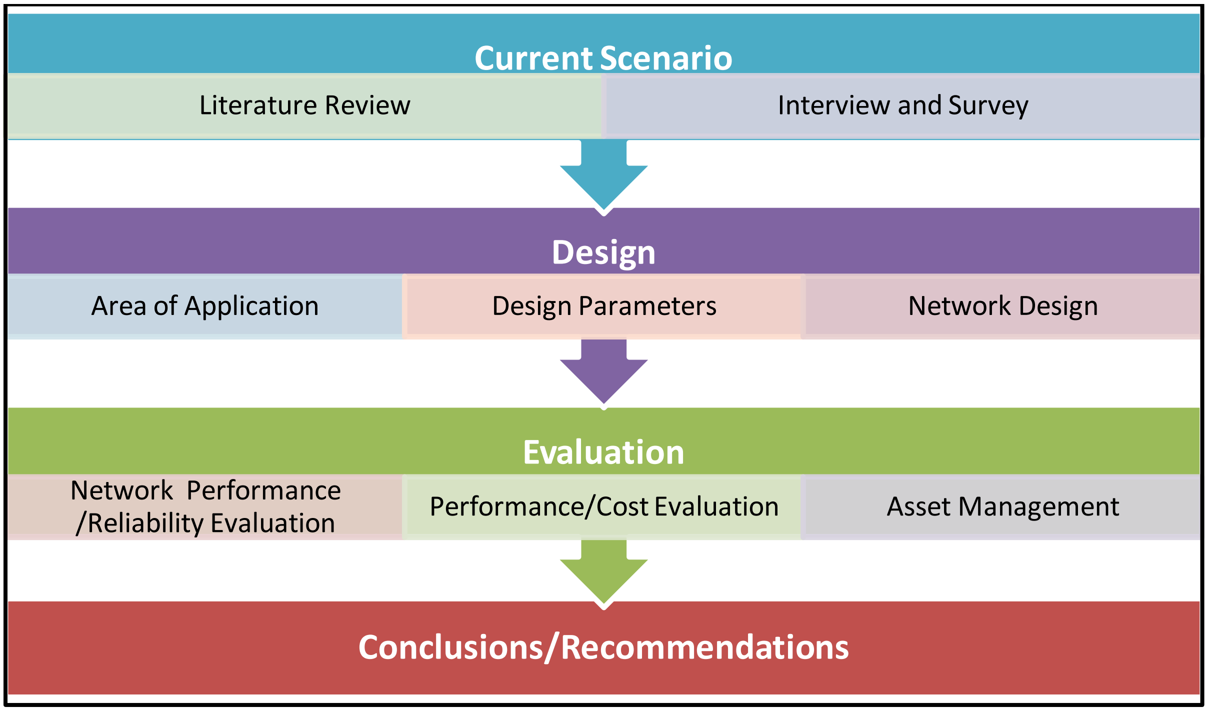


Figure 2 Research Methodology

To evaluate different network options such as topology, communication mediums, and technologies; the authors proposed network design methods that can be used by traffic agencies to design and implement wireless sensor network for traffic management and operations within a metropolitan area. The methodology was based on lessons learned from previous studies, refined by expert opinion, and described in detail for future practitioner use. The assessment was performed at two levels; subsystem level and system level. At the subsystem level, factors that can affect the wireless communication performance and reliability in a real highway environment were considered by conducting field tests. These factors included transmission power, modulation rate, and highway terrain and foliage obstructions. One of the primary functions in ITS is on-line traffic video surveillance, which is commonly supported by communications between roadside cameras and a TMC. The authors conducted a quality requirements study of traffic video transmission from field to a center.

The system level analysis was carried out by conducting a simulation study. This study assessed the throughput per device under different network topologies presented. Performance-cost analysis was conducted using the results generated utilizing this simulation output. The total device costs associated with two topologies were also presented. The output of the case study was used in the simulation study. Field experiments were conducted to evaluate the communication performance, between field devices or between centers to devices, for two potential wireless technologies; Wi-Fi and WiMAX.

In the end, based on the study results, the authors developed recommendations for practical applications of the study findings. Table 1 demonstrates the research methods used in this study and their functions. Figure 2 shows how these tools were incorporated in carrying out major research tasks for this study. This study also evaluated several ITS asset management systems as required by SCDOT.

Table 1 Research Tools

Tools	Functions
Literature Review/ Interviews	• Identified current communication options and strategies and evaluated reports throughout the duration of the study; • Conducted telephone/email interviews with selected public agencies with successful ITS programs regarding their experiences while using various communication options for ITS and related qualitative and quantitative impacts.
Case Studies	• Proposed an network design process to implement traffic sensor network using different wireless technologies • Conducted case studies for traffic surveillance systems in seven metropolitan areas in SC using the proposed design process
Field Tests	• Evaluated the performance and reliability of wireless alternatives under different highway terrain and foliage coverage conditions in real highway environment • Evaluated the video quality requirements of on-line traffic surveillance and proposed suitable threshold value for quality control
Simulation Analysis	• Compared the communication performance of a traffic sensor network under simulated environmental conditions • Studied the communication behavior of the system in case of a road incident using an integrated simulator
Performance-Cost Analysis	• Utilized benefit cost analysis to recommend best communication alternatives for ITS

4 INTERVIEW AND SURVEY

At the inception of the study, an interview was conducted to examine the specifications of existing communication infrastructures being deployed for various ITS applications and the usage of wireless technologies in different states. This interview was also designed to collect information regarding state transportation agencies' experiences in reliability and performance regarding different ITS-related communications and future plans. Based on their response to the first round of interviews, a follow-up questionnaire was sent to gather further information in more details. Interview questions and follow-up questionnaire are shown in Appendix A and B, respectively.

The following agencies were interviewed: South Carolina Department of Transportation (DOT), Virginia DOT, Georgia DOT, Washington State DOT, North Carolina DOT, Illinois DOT, Missouri DOT, Minnesota DOT and the city of Phoenix, AZ. The interview and follow-up questionnaire primarily focused on the following areas.

- Types of communication infrastructure currently deployed
- Previous communication evaluation experience
- Awareness of available reports on communication systems for traffic management
- Future plans to use any new, currently non-existing, wireless alternative to support traffic management applications
- Future plans to expand any currently existing traffic management infrastructure
- Experiences with communication infrastructures for traffic management
- Typical data rate expected for traffic surveillance systems and other similar devices
- Average traffic camera density in metro area and average distance between devices on the monitored highway sections
- Coverage and service cost (if leasing) of existing communication infrastructure(s)
- Existing and planned network topologies used to connect video surveillance and other ITS devices

According to the first round response, the follow-up questionnaire was aimed to gather further information on the following areas.

- The typical data rate(s) of the existing video surveillance system
- The minimum and maximum required data rate expected for current and future video surveillance system or other similar devices
- Average camera density on monitored roadways in metropolitan areas
- The percentage of current communication infrastructure owned by public agencies
- The amount of money spent on leasing the current communication infrastructure
- The current and planned network topologies used to connect the video surveillance and other traffic devices

- Usage status of licensed wireless communication technology
- Preference and future plan for implementing licensed wireless technology

Summary of Responses

This section presents a synthesis of interview responses received as of October 1, 2009. As summarized in Table 2, current widely used communication technologies for traffic management are fiber optic or T1 lines. Wireless has been used by all nine survey participants, however on a limited scale. Respondents used cellular services provided by commercial providers; state owned and operated microwave systems, unlicensed wireless systems, and WiMAX networks. One responding agency even used a state owned and operated microwave system to connect their radio-based land mobile system. Respondents also reported using cellular communication for low bandwidth applications, such as dynamic massage signs (DMS) and traffic signals. Two states reported using WiMAX technology to provide communication for traffic surveillance cameras. The city of Phoenix used 2.4 GHz WI-Fi to connect 96 traffic signals within 25 square miles. In other states, Wi-Fi connections are more widely used in rest areas and office buildings to provide hot-spot service. It was found that due to cost issues, states typically own the fiber system but depend on leased wireless service in certain segments.

Most responding agencies expressed interest in using wireless technologies to replace the leased lines to reduce cost. They also emphasized the need for the wireless system to be reliable, especially for critical ITS infrastructures, such as surveillance systems in tunnels, on bridges and at important interchanges. One state reported that their wireless performance was affected by foliage coverage, especially during the summer months. Another state reported that rain and fog affected wireless communication performance.

Wireless is not expected to replace fiber systems, rather its integration into existing systems will enhance their performance. For example, some agencies prefer to use wired communication to build redundant backbone systems to improve the reliability of their wireless communication infrastructures.

Table 2 Summary of Interview Responses

Categories	Responses
Types of communication infrastructure	Wired: T1, Fiber (9) Wireless: unlicensed wireless (9), Cellular (9), Wi-Fi (4), WiMAX(2)
Previous communication evaluation experience	Yes (4) No and no short term plan (5)
Experiences with wireless communication for traffic management	Affected by foliage coverage, rain and fog Potential interference if using unlicensed
Licensed or Non-licensed wireless	Licensed: WiMAX (2), Wireless 4.9 GHz (2) and 5.9 GHz (1) Unlicensed: 200 MHz (1), 700MHz (1) and 900MHz (6), Wi-Fi (4), Wireless 5.1-5.8 GHz (2)
Future plans to use any new, currently non-existing, wireless alternative	Yes (9) such as Wi-Fi
Future plans to expand any currently existing traffic management infrastructure	Yes (9) by either fiber or wireless
Typical data rate expected for traffic surveillance systems and other similar devices	256 Kbps ~ 1.2 Mbps
Average traffic camera (or other devices) density	Major metropolitan areas: one camera/ mile Key Intersections: two cameras/mile
Service cost (if leasing)	NA
Existing and planned network topologies used to connect video surveillance and other ITS devices	Existing: Point-to-multipoint (8), Mesh (1) Planned: Mesh (wireless)

Note: The number inside ( ) indicates the number of responses

Although all nine states surveyed plan to extend both their wire and wireless infrastructures for traffic management systems, only three have evaluated the performance and reliability of their communication infrastructure. The other six have short-term evaluation plans. Among the types of ITS devices used for traffic surveillance and management, traffic cameras require the largest bandwidth. Currently deployed traffic camera surveillance devices require data rates between 256 Kbps and 1.2 Mbps. On average, camera density is roughly one per mile in major metropolitan traffic corridors, and increases to one per half a mile near key interchanges. Some states plan to expand their camera density to every mile at key intersections and interchanges in rural areas of the state. However, the bandwidth limitations of many existing wired communication infrastructures and their associated leasing cost issues severely limit the effectiveness of these initiatives. Consequently, most of respondents (7 of 9) expressed a strong interest in wireless technologies such as Wi-Fi and WiMAX, because of their broadband capability and cost-effective deployment. Respondents also expressed interest in exploring the feasibility and initial costs to build state owned wireless infrastructures for traffic surveillance and monitoring such as South Carolina. Moreover, one state agency expressed a desire for a network that would allow multiple state agencies (e.g. police, traffic, and emergency services) to share a WiMAX network in certain strategic areas.

The authors found that unlicensed wireless frequencies are more widely used than licensed, except the 4.9 GHz band which is reserved for public safety. Reported unlicensed frequencies include 200 MHz, 700 MHz, 900 MHz, 2.4 GHz and 5.8 GHz, due to low cost of the unlicensed frequencies and ease of use. The Case Study section in Section 6 contains a detailed discussion on the differences between licensed and unlicensed frequencies. No interference with other wireless systems has been reported, largely due to the lack of wireless systems operating near highways. However, all respondents also expressed a desire to determine the feasibility of such systems in the near future. Only three states responded with plans for using licensed wireless band such as 4.9 GHz radios. One state agency currently uses it for temporary and permanent links to a fiber optic backbone; the other uses it to support signal controller, DMS and traffic cameras.

Table 3, developed based on both the interview results and literature review, describes potential and existing ITS applications, as well as the reliability guarantees that the various wireless technologies support. Table 3 does not reflect a complete list of possible ITS applications, rather it is a sample of the more common uses.

Table 3 Summary of Wireless ITS Applications

State	Project	Technology	Description
Arizona	Phoenix ITS Wireless Network	IEEE 802.11 a/b/g ad hoc 2.4/4.9 Ghz	Wireless mesh network for public safety video surveillance and traffic lights
California	Bay Area Surveillance Enhancement	Proxim Wireless 5 Ghz spread spectrum	16 miles point-to-point wireless network operating at 90 Mbps for video-over-IP transmission for surveillance of bridges and tunnels in the San Francisco Bay area
	VII- Dynamic Route Advisory System	IEEE 802.11b, DSRC	Use in-vehicle GPS to generate traffic data and transmits it to the roadside Wi-Fi access point which then calculates optimum route for the vehicle
	VII- Intersection Collision Avoidance	IEEE 802.11b, DSRC	Use in-vehicle unit and roadside unit at intersection to warn the driver the traffic timing and the vehicle coming from the side road
	Remote monitoring of Bridge sensors	802.11	Caltrans connects sensors on Kings Stormwater channel Bridge
Colorado	Denver Test Bed	DSRC	Plan to implement5.9 GHz DSRC technology for high performance tolling and enforcement
Florida		IEEE 802.11	Provides police officers in-vehicle access to applications from the central office in North Miami Beach
		IEEE 802.11	Used for monitoring parking meters in Cocoa Beach, Fl.
Georgia	AirSage System	IEEE 802.11	Real-time video streaming for public safety
Illinois		IEEE 802.11	A mesh network for maintenance management of train yards in Chicago
Illinois		2.4, 4.9, 5.1-5.9 GHz radios	Used for temporary and/or permanent links to fiber backbone.

State	Project	Technology	Description
Indiana	Advanced Traffic Monitoring System	900 MHz spread spectrum	Wireless traffic sensor network for monitoring weather and traffic congestion
Iowa	Wireless rest areas		
Maryland		Wireless LAN, GPS	Wireless ad-hoc networks for traffic surveillance and management
Missouri		4.96 GHz	Support traffic signal controller, traffic cameras and some of the dynamic message signs
Michigan		900 MHz serial radio	Use wireless for signal, traffic and pedestrian management, transit, demand management in Detroit
	VII Michigan Test Bed Program	DSRC, GPS, Cellular, Wi-Fi, WiMAX	Support VII deployment and transmit VII data for associated applications
Minnesota	In-vehicle Signing Project	DSRC radio with a localized secure data network	
		Fixed WiMAX	Used for highway video monitoring
	VII test-bed (plan)	WiMAX, Wi-Fi, DSRC	Plan to support the VII deployment and related applications
New Mexico	Highway 550 Wireless	Wi-Fi Mesh Network	Connect the traffic signals on New Mexico Highway 550 to coordinate traffic, provide real traffic counts, network access for NWDOT Used for video monitoring of the corridor
New York	ITS Test Bed Laboratory Transportation Network	3G Cellular	Support data sharing between vehicles and infrastructure to collect the path choice information
New York	State-wide network	Land Mobile Radio	Integrated wireless public safety/service radio network for interagency and intergovernmental communications
	Commercial Vehicle Infrastructure	DSRC, IEEE 802.11p	Development, testing, and demonstration of commercial vehicle-based data communication

	Integration Program		with VII roadside equipment
	2009 ITS World Congress VII Test Bed	DSRC, Cellular	Test bed for demonstrate VII applications including in-vehicle signing, transit priority, commercial vehicle operations, school zone warnings, etc
Texas	Houston Metro	IEEE 802.11a/b/g	Used for real-time video monitoring at Houston METRO Park and Ride lots and major stops
	Intersection Control for Autonomous Vehicles	DSRC	Vehicle requests time slots for traversal through the intersection using vehicle to roadside communications
South Carolina		Wi-Fi, Cellular	To support traffic surveillance on I-385 near Greenville, SC To support data transmission to mobile dynamic traffic signs
	State-Wide WiMAX	WiMAX	Plan to share the state-wide WiMAX network between different agencies
Virginia	Tyson’s Corner Wireless Video	Proxim Tsunami Spread Spectrum	Used for video surveillance of construction sites
	I-81 Wireless Cameras	Pelco Cameras Wireless Spread Spectrum	To support traffic sensors and cameras on I-81
	Route 460 Wireless Cameras	Motorola Canopy Spread Spectrum	To support video surveillance system on Route 460
Washington		700 MHz	To support communication between all DOT vehicles, workers in the field and some ITS devices
West Virginia		WiMAX operates at 4.9 GHz	Used for public safety and monitoring

5 FIELD TESTS

The following field test description is to assist SCDOT in conducting performance and reliability evaluation of potential wireless options. Several field tests were performed to demonstrate the test process and generate results that can be used during an actual deployment. Wi-Fi and WiMAX field tests evaluated the subsystem communication performance.

The field tests indicated that wireless communication is largely dependent on the line of sight between the transmitter and receiver. Modulation rate was observed to influence the saturation throughput and the received signal strength. For a video surveillance application using wireless communication, it was observed that the quality of the real-time traffic surveillance is acceptable when the packet rate is more than 23 packets per second.

5.1 Wi-Fi and WiMAX Field Tests

The following sections present the process and measures of effectiveness related to Wi-Fi and WiMAX field tests. Experimental results recorded from the field tests following the process are also presented.

5.1.1 Description

Field study aims at evaluating communication performance between field devices as well as between field devices and the traffic management centers. The use of wireless communications for these scenarios has been limited due to a number of reasons. First, each node (this report will use the term node interchangeably for a field device) can only communicate with the node within its radio range. Furthermore, the effective wireless communication range and performance are different when the system is operating at different modulation rates, and also can be affected by different transmission powers.

Traffic sensors, such as surveillance devices, are normally deployed in a longer distance interval than the wireless communication range. A communication relay, or access point, are needed to relay the information over longer distance between two traffic sensors. The research motivation is to first identify the optimized distance to deploy the traffic sensors and relays to enhance the performance and reliability in a most cost-effective way. Moreover, it will try to quantify the effects of the different factors in a highway environment, such as modulation rate, distance and transmission power, which traffic agencies can use as a reference for future ITS applications. Besides data transmission between the field devices, this study also assessed the quality requirements of the real time video transmission between field cameras and a monitoring station.

Among the three selected wireless technologies, the authors conducted two types of field test to evaluate the performance, reliability and feasibility of using Wi-Fi and WiMAX for ITS applications in the field environment under prevailing roadway conditions. Because DSRC is used more for vehicle to vehicle and vehicle to infrastructure communication, it was not studied.

The following sections explain how the experimental tests were designed and conducted. Measures of effectiveness (MOEs) were carefully selected for each test to quantify important factors that affect the performance and reliability of wireless communications.

5.1.2 Wi-Fi Communication between Two Adjacent Nodes

Aim: To evaluate the effects of transmission power and modulation rates on the wireless communication performance between two sensors at different distances on a two-lane two-way (TLTW) state highway.

This test was aimed at studying the deployment parameters for the Wi-Fi technology. Field tests were systematically conducted with the following objectives:

- Identify major measures of effectiveness (MOEs) to accurately present the performance of wireless communication.
- Evaluate the performance of wireless communication between two adjacent nodes which support networking between neighboring sensors operating at different modulation rates.
- Evaluate the effect of transmission power strength on network performance under prevailing roadway conditions.

5.1.2.1 *MOE Selection*

Effective traffic management applications rely on the real time traffic information collected by roadside devices to improve the traffic safety and mobility, such as incident response and clearance, traveler information assistance and commercial vehicle management (Gordon 2005, Chowdhury and Sadek 2004). Therefore, a reliable communication network is the foundation for effective and timely traffic monitoring and operations. The foliage coverage has an effect on how much data the receiver can receive during certain time period, which ultimately affects the functionality and reliability of a traffic management system.

Wi-Fi field test selected four relevant MOEs: the saturated throughput, packet delivery ratio, Receive Signal Strength Indicator (RSSI) and Signal-To-Noise Ratio (SNR). Saturated throughput is the maximum throughput achieved by the system as the transmitted data load increases (Pourahmadit et al. 2003). Packet delivery ratio is the percentage of packets sent by the sensors that can be successfully received by their designated receiver. RSSI is a value representing the received signal strength in dBm (Peterson et al. 2003), while SNR is a measurement of signal strength relative to background noise, usually measured in decibels (dB). Based on these four metrics, this field study was able to systematically analyze and quantify the communication performance under different conditions.

5.1.2.2 *Experimental Setup*

- Dates when conducted: August 2008 to December 2009
- Locations: South Carolina State Highway 93 (SC 93) and Williamson Rd, Clemson University campus, Clemson, South Carolina.

First, the field test was conducted on a segment of Williamson Rd, which is a two lane two way (TLTW) road, shown as location 1 in Figure 3. The presence of large amounts of foliage near the roadside didn't prevent direct line of sight between the two nodes.

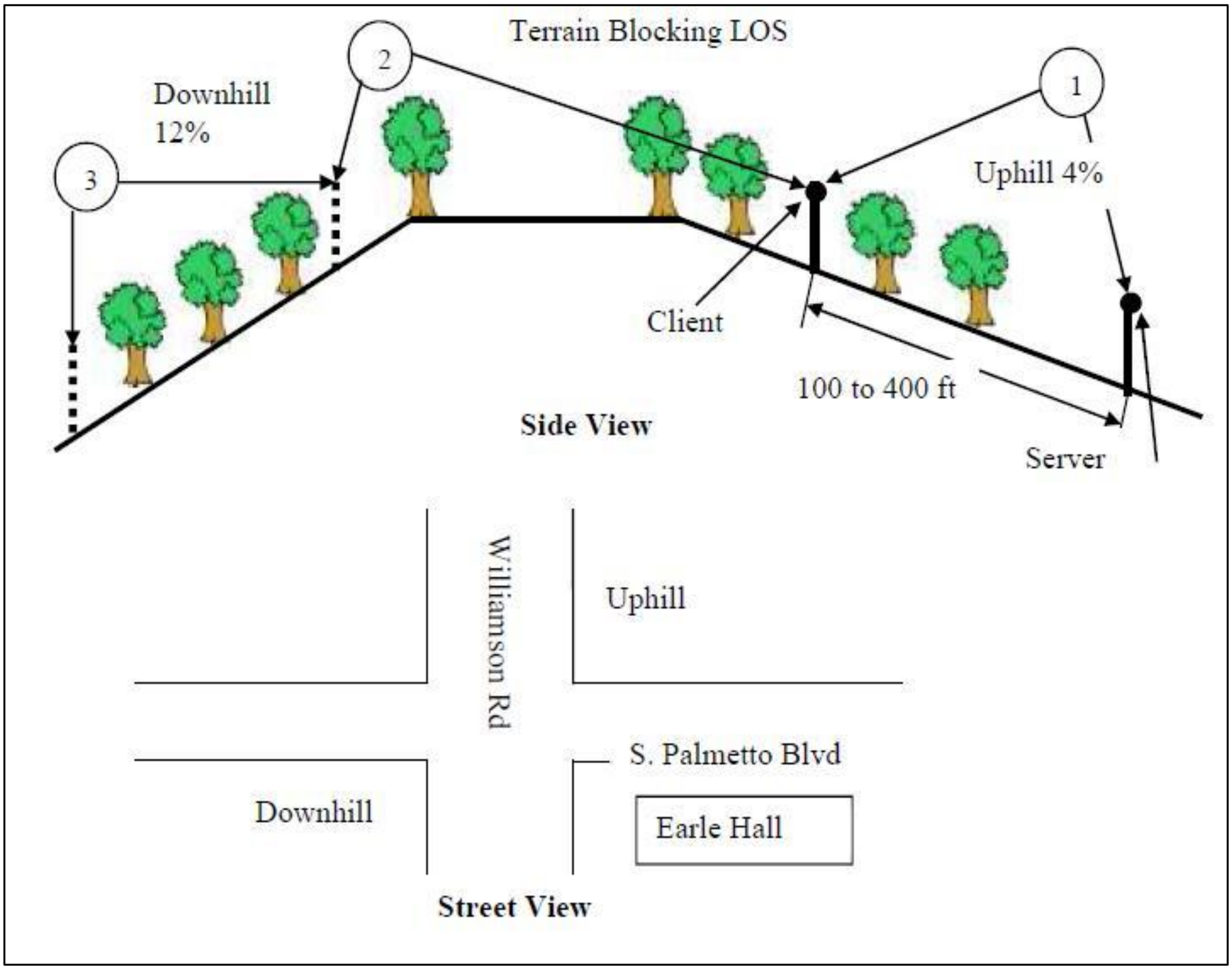


Figure 3 Field test loactions on Williamson's Road

The network setup consisted of two wireless access points (Linksys WRT54GL flashed with the Openwrt version Kamikaze firmware with luci lua interface) (dd-wrt 2009) and two laptops. One router was configured in the access point (AP) mode and the other was configured as a repeater bridge, thereby bridging any clients connected to them on two ends of the link. The two routers were placed on the side of the road with obstructed LOS in between. The two routers were connected to a laptop (running Linux) through Ethernet cables. The laptops' built-in wireless interface was shut down to avoid interference. One laptop and one router were placed on top of a plastic box on each side at the same height, approximately 4-5 ft from the ground. There was a third laptop at the receiving side running Wireshark to capture every data packet to record the average received signal strength. Figure 4 demonstrates the experimental setup. Other possible factors that can affect the wireless communication performance, such as weather, traffic condition and other environmental conditions, were similar in different test days.

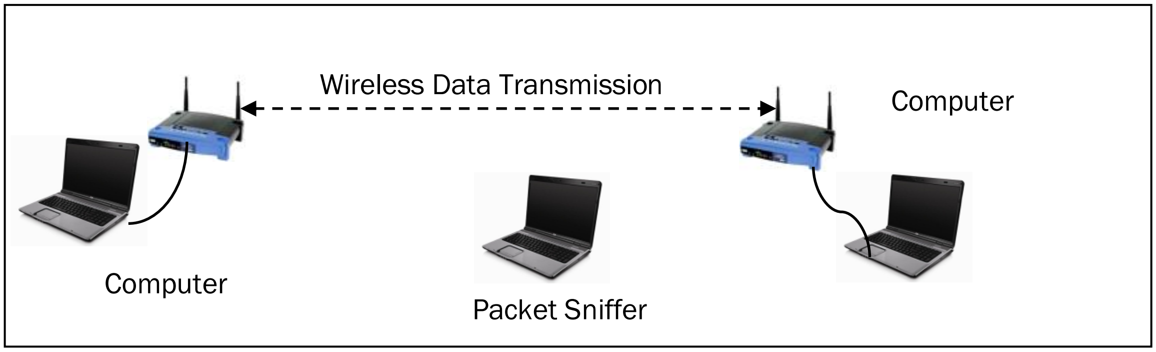


Figure 4 Field Test Experimental Setup

The two laptops were used to run the iperf client on one side, and server on the other side, and to measure the link performance in this experiment. Originally developed in University of Illinois (Iperf, University of Central Florida), iperf is a commonly used network testing tool written in C++ that can create TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) data streams and measure the maximum throughput of a network that is carrying them. Both TCP and UDP are commonly used protocols on the Internet. TCP offers error correction and flow control to guarantee delivery but UDP does not. Errors occur and packets get lost when collisions occur during transit over the Internet in UDP mode. Therefore, TCP is more suitable for transmitting important data such as webpage, database information, etc., while UDP is commonly used for streaming audio and video due to its lower network overheads and latency (Peterson and Davis 2003). For time-critical applications such as traffic video surveillance, UDP can be a potential option for data transmission, however it has performance and quality concerns because it has no form of flow control or error correction. This field test only studied TCP protocol.

Then, the similar test was conducted in another location on South Carolina state highway SC 93, as shown in Figure 5. The two nodes were directly adjacent to this TLTW state highway. The presence of large amounts of foliage near the roadside prevented direct line of sight between the two communicating nodes.

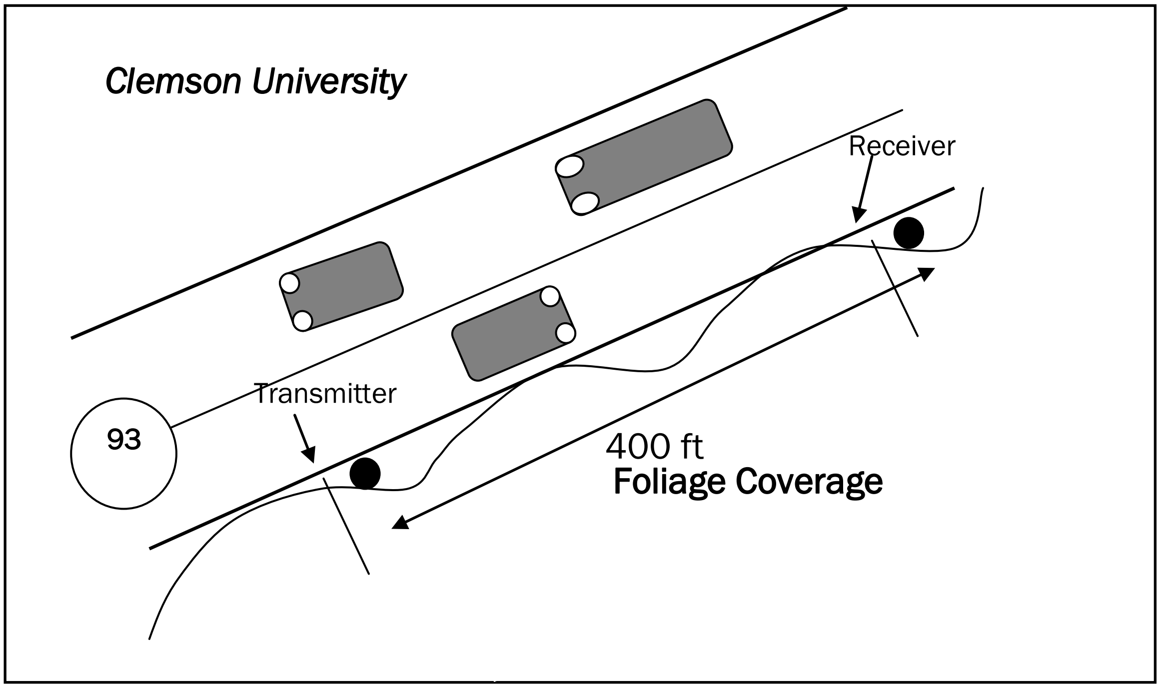


Figure 5 Test Location and experimental Setup on SC93

Lastly, the field test assessed the effect of the highway terrain characteristics on wireless communication between the two nodes. As shown in Figure 3, three test scenarios were chosen including ‘uphill’ (location 1), ‘terrain blocking LOS’ (location 2) and ‘downhill’ (location 3). The distance between the two nodes, 250 ft, was kept same for all these three scenarios. At location 2, there was no direct line of sight between the two nodes. The slope of the roadway section, where the test was conducted, was about 2% upgrade and 3% downgrade.

5.1.2.3 *Measurements*

First, five distances were selected, starting at 100 ft and increasing to 500 ft using 100ft intervals. At each distance, the authors first measured the saturated throughput under seven modulation rates and four transmission powers using iperf. At the same time, received signal strength and SNR of each packet were recorded and measured on the client side through Wireshark. All tests were 120 sec in length with throughput and signal strength measurements taken each second. Average was taken at the end of each test.

This field test aimed to assess the communication performance, the throughput and reliable communication range, of both 802.11g and 802.11b Wi-Fi technologies. 802.11g and 802.11b support different modulation rates. Table 4 summarized the main parameters used in the field test.

Table 4 System parameters used in field test

Parameter	Values
Modulation Rates	802.11b: 2Mbps, 5.5Mbps 802.11g: 6Mbps, 11Mbps, 24 Mbps, 48Mbps Auto
Transmission Power (mW)	15, 30, 50, 70
Distance (ft)	100, 200, 300, 400, 500
Test Duration	120 seconds

Transmission power of 84 mW is the commonly-used maximum value (DD-WRT 2009). Transmissions power higher than 84 mw is reported as unreliable and might damage the router. Therefore, The authors only tested the transmit power range up to 70 mW. The transmission power was set as 50 mW when testing the effects of highway terrain characteristics. Although 802.11g has a maximum throughput of 54 Mbit/s, a significant percentage of this bandwidth is used for communications overhead. In reality, the effective maximum throughput is about 25 Mbit/s measured in the lab environment at a close distance. Many factors, such as metal, water, and thick walls, reduce the transmission range significantly by absorbing signals (Peterson et al. 2003).

Iperf was used to measure the throughput of both the server side (receiving end) and client side (sending end). The sending side exhibits throughput similar to the system bandwidth values, however, this is not the real throughput achieved on the wireless link. Because when the transmitting end is sending many packets to the router, packets might get dropped by the router without really being sent over the wireless link especially when the data rate is very high. Therefore, in order to investigate the real communication link performance between two nodes, the network throughput was recorded at the receiving end. In the TCP mode, the throughput value measured by iperf is the saturated throughput at different transmission powers and modulation rates.

5.1.2.4 *Analysis of Wi-Fi Field Tests*

Figures 6 through Figure 13 present the performance evaluation results of the two-node wireless network under different scenarios in TCP modes. All the results represent the throughput taken in the server side and will be discussed in the following paragraphs.

- Verification of Average behaviour of the system

To determine if the average throughput taken during 120 sec represents the average communication performance, the authors first investigated the throughput variation with time in TCP modes while taking the measurements in different scenarios. For example, using the throughput variation at a transmission power of 70mW, the average link throughput was recorded every 10 sec at the server side within a total of 300 sec test time. As shown in Figure 6, the throughput varied between 10 Mbps to 12Mbps with the deviation within 5% of the mean value. Therefore, the average throughput taken in 120 sec test is adequate for capturing the network performance.

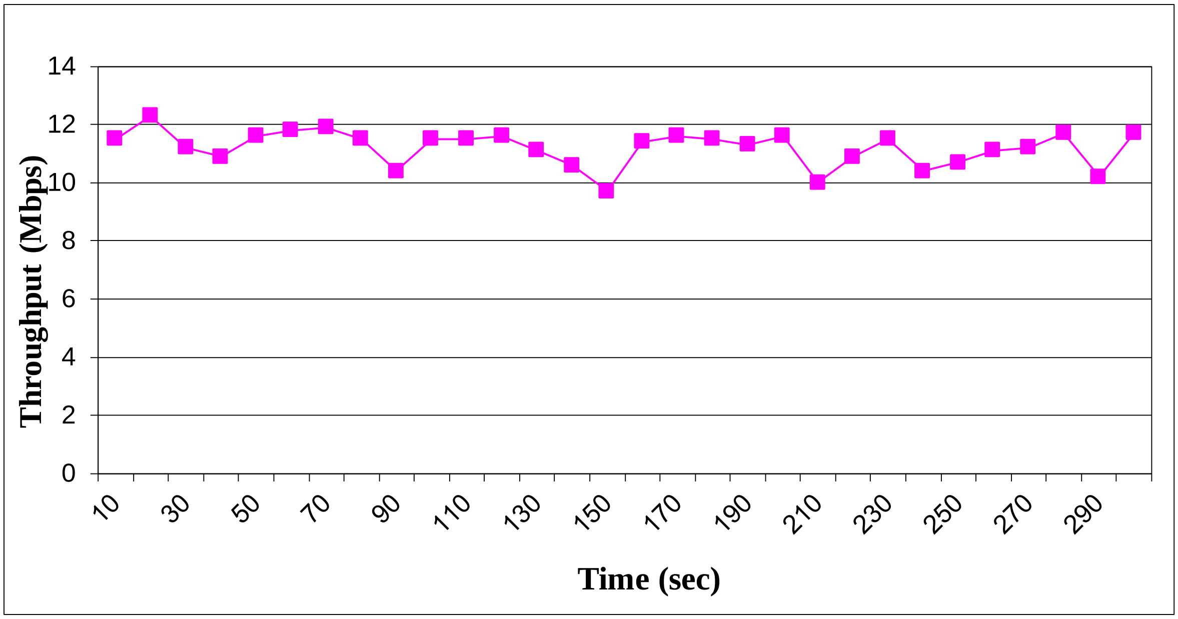


Figure 6 Throughput Variation with time (TCP)

- **Effect of Modulation Rate and Transmission Powers on saturation Throughput and Delivery Ratio**:

Modulation Rates considered: 2Mbps, 5.5 Mbps, 6 Mbps, 11Mbps, 24 Mbps, 48 Mbps

Figures 7 a) to 7 f) present the saturated throughput at different distances between transmitters and receivers under four different transmission powers.
Figures 8 a) to 8f) present the Delivery Ratio at different distances between transmitters and receivers under four different transmission powers.

As seen from Figure 7, at each modulation rate except 11 Mbps and 48 Mbps, throughput first stays constant until a certain distance, and then starts to drop. For example, at modulation rate 2 Mbps (Figure 7 a)), the saturated throughput achieved was around 1.34 Mbps within the 300 ft range, however, it dropped to 1.02 Mbps at 400 ft. Therefore, after a certain distance, the communication link becomes very unstable and performance degrades.

Rather unexpectedly, at 100ft range, throughput corresponding to modulation rates 11 Mbps and 48 Mbps are much less than the throughput at 200 ft. These two special cases might be caused by multipath propagation at the 100 ft location, which degrades the wireless communication performance. Multipath, which is a propagation phenomenon, results in radio signals reaching the antenna in the receiving end by more than one path, which could potentially be constructive or destructive for signals. Causes of multipath in this case could be the reflection from terrestrial objects such as parked cars, buildings or trees (Tse and Viswanath 2005).

For most of the modulation rates, the drop occurs between 300 ft to 400 ft. Within 300 ft, at one specific distance, the throughputs at different transmission power are very similar to each other. One reason is that the successful delivery ratio at this point is already very high, which is about 67% at modulation rate 2 Mbps, as shown in Figure 40. Within 300 ft, field test results indicated that performance is more dependent on the modulation limit than the environment limits, especially at lower modulation rates. For higher modulation rates, the communication performance could be affected by both modulation rate and distance limits. The successful delivery ratio decreased to around 36% at a modulation rate of 48 Mbps.

One thing to note is that the difference in performance between different powers is not significant because the power used in this experiment is very low, compared to the real transmission power used.

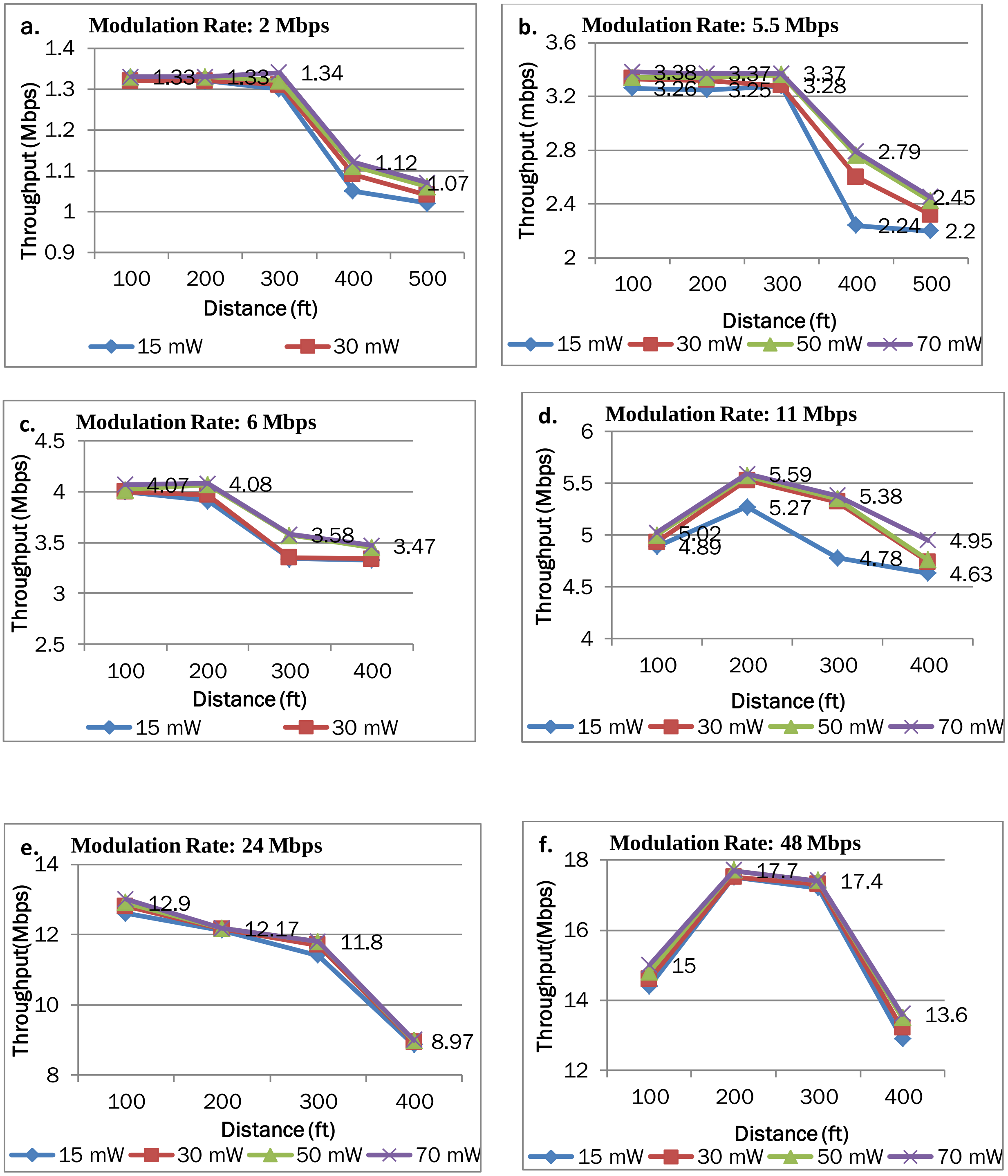


Figure 7 Saturation Throughput (TCP)

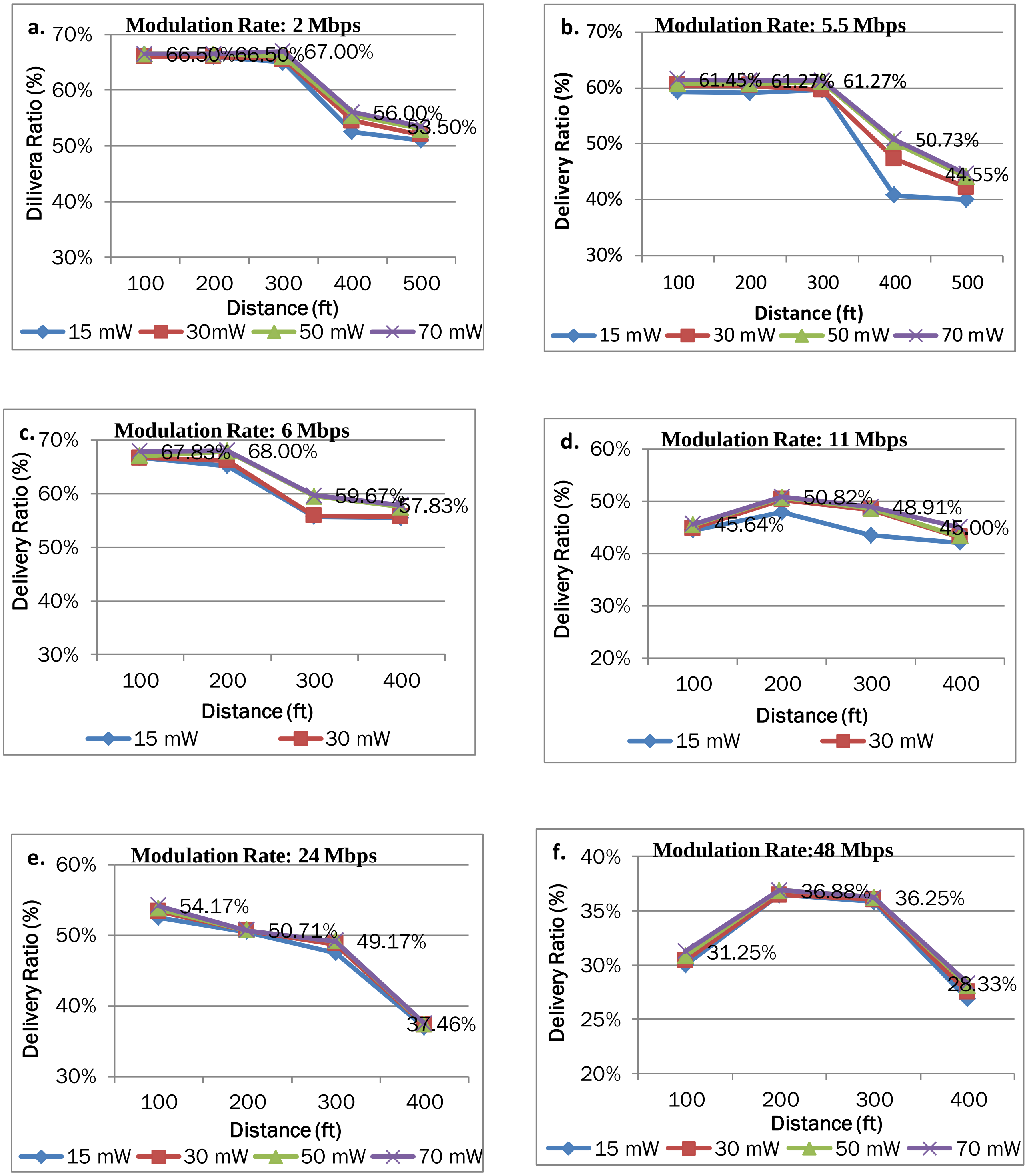


Figure 8 Delivery Ratio (TCP)

Higher modulation rates provide better throughput, so more data from the field can be transferred in real time. However, higher modulation rates are normally less robust to the background noise and interference, so more data packets got dropped. As seen in Figure 8, higher modulation rates provide lower successful delivery ratio due to the communication error. Moreover, delivery ratio decreases with the distance increases, except the 100 ft at modulation rate 11 Mbps and 48 Mbps. The effective throughput is the modulation rate times the successful delivery ratio. For traffic agencies, it is of paramount importance to operate the system in the modulation rates that provide certain balance between throughput and delivery ratio for particular applications.

During the field test, the authors also observed that the both received signal strength and throughput decreases for a few seconds when vehicles are passing the test location. Future study needs to be conducted to quantify the effects of vehicular traffic on the wireless communication between roadside traffic devices, especially for the congested areas, where traffic control devices are most likely to be deployed

- **Effect of setting modulation rate as a function of received signal strength:**

The field test focused on studying the 802.11 b and g technologies. Hence modulation rate options available are 11 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps. Figure 9 shows the saturated throughput at auto modulation rate under 4 transmission powers at different distances between a transmitter and a receiver.

In order to find out the most frequently used modulation rate in each scenario, the authors calculated the percentage occurrence of each modulation rate, studied during the 120 seconds test period and the average rate for each scenario, as presented in Figure 10. For example, at 200 ft with 70 mW transmission power, when the modulation rate set as auto, 54 Mbps was used 54% time during the test period, while 48 Mbps, 36 Mbps, and 24 Mbps were used 25%, 16% and 2% time during the test period, respectively.

As seen from test results, when modulation rate is set as auto, high modulation rates, such as 54 Mbps, 48 Mbps and 36 Mbps, are most likely to be utilized to achieve higher throughput. It is interesting to note that the three most used rates are all supported by 802.11g technology. Moreover, within 300 ft distance, modulation rate 54Mbps and 48 Mbps are more likely to be used than other rates. However, at 400 ft, 48 Mbps and 36 Mbps were chosen more frequently than 54 Mbps. The reason is clear from the previous test which stated that the successful delivery ratio reduced with increase in the modulation rate. Thus, the system needed more robust modulation at higher rates thereby automatically dropped to the lower rates in the auto mode.

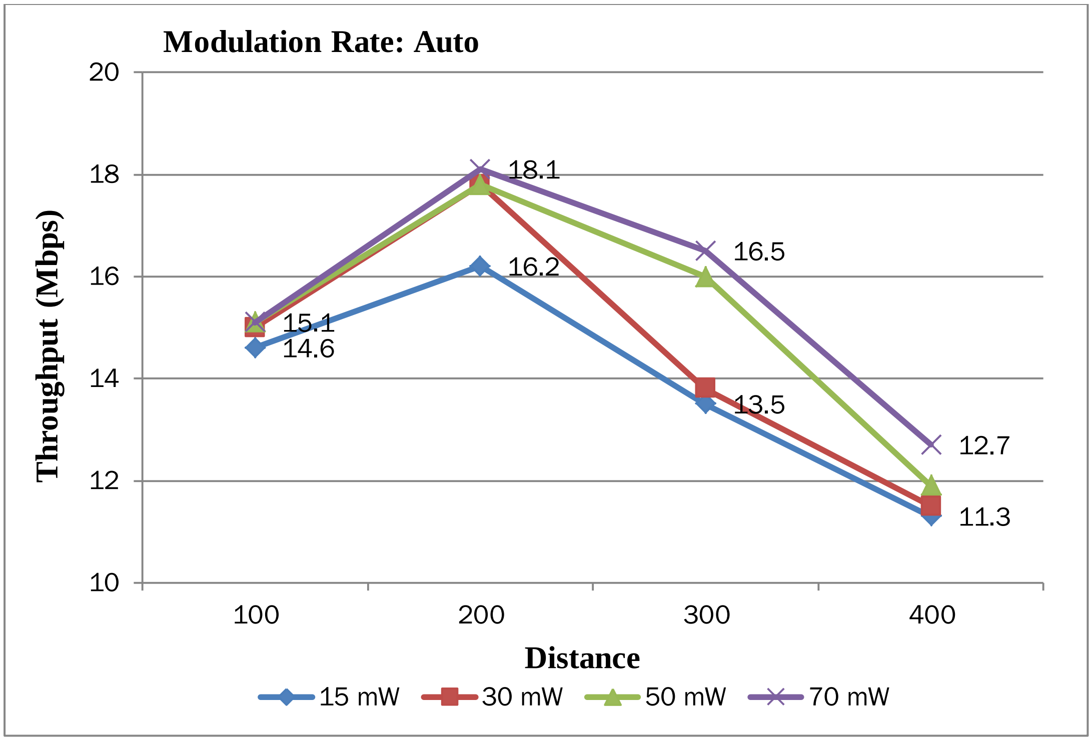


Figure 9 Saturation Throuhput with Modulation Rate Auto

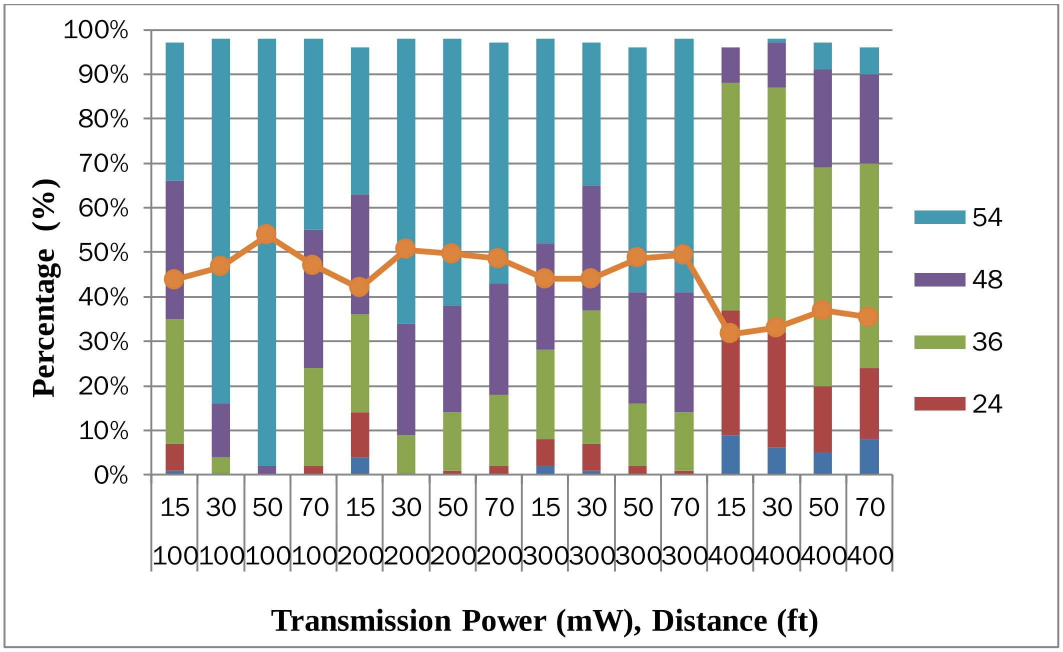


Figure 10 Percentage Occurrence of Modulation Rates

- **Path loss as a function of distance and modulation rate:**

Received transmission power is another important performance metric studied in the field test. The height of the antenna and the antenna gain both play a role in the network performance achievable at any location. Yet, the antenna height and gain can be captured as a constant ratio as depicted by the following equation found in most mobile communication textbooks (Schwartz 2005):

$$P_R = P_T G_T G_R \frac{(h_t h_r)^2}{d^\alpha} \qquad \text{Eq. (1)}$$

where P_T and P_R stand for the received and transmitted radio power, G_T and G_R stand for the transmitting and receiving antenna gains, h_t and h_r stand for the transmitting and receiving antenna heights, and d stands for the two antennas' distance. The authors characterized the performance dependency with respect to the distance, while the gain and height impacts can be proportionally and independently applied to our results.

At each distance, $G_T G_R \frac{(h_t h_r)^2}{d^4}$ can be considered as a constant, K. Take the 10log10 of both side of $P_R = P_T G_T G_R \frac{(h_t h_r)^2}{d^4}$ in mW gives the (P_T- P_R) (dbm) = 10log10 (K) (dbm). (P_T- P_R) in dbm is also known as path loss of the wireless communication, which is the loss of signal strength incurred between the transmitter and receiver. Higher (P_T- P_R) indicates higher lost in signal strength. Theoretically, the K should be constant at one specific location under different modulation rates and transmission power.

Figure 11 a) to 11 d) presents the measured P_T- P_R and calculated K at 100 ft, 200 ft, 300 ft and 400 ft, respectively. G_T and G_R are equal to 1, while h_t and h_r equal to 5 ft and 3 ft, respectively. The calculated K is shown in red color. For each modulation rate, for values of transmission power were considered .As seen in the Figure 11, the measured path loss (P_T- P_R) changes with the modulation rate. Moreover, it appears that lower modulation rate sees larger path loss at 100 ft and 300 ft. At 200 ft, the path loss stays almost constant at each scenario. At the same modulation rate, the path loss generally decreases as the transmission power increases, when the theoretical model suggests that it should be constant. At 100 ft and 400 ft, the measured path loss is much higher than the calculated K, especially at 400 ft. Similar to previously discussed, the abnormal situation at 100 ft might due to the multi-path effect. At 300 ft, the calculated K, 73.04, seems to match with the path loss at modulation rate of 5.5 Mbps and 6 Mbps.

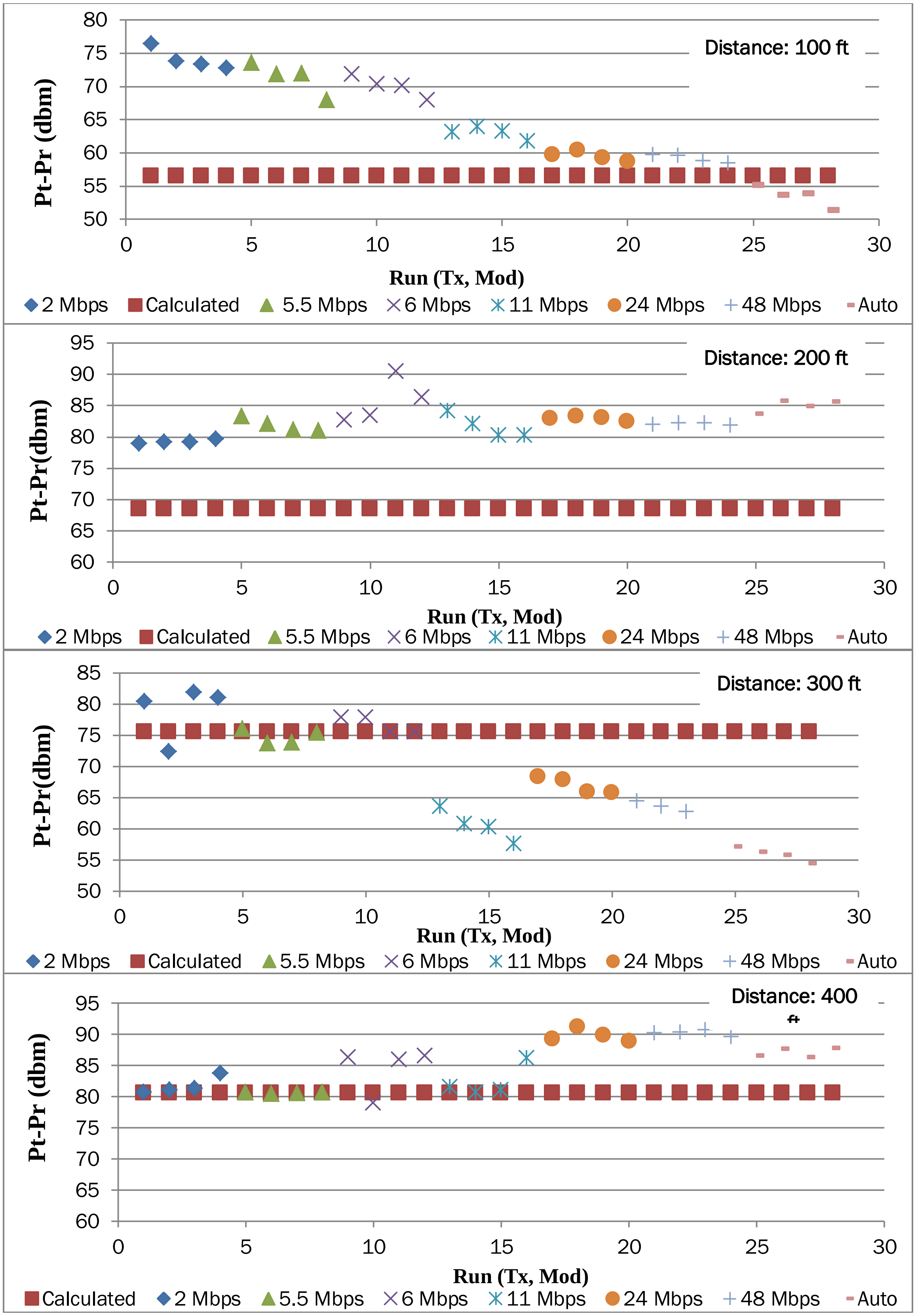


Figure 11Path Losses at different distance

- **Effect of Line of Sight on the performance metrics:**

  Field measurements were conducted in three scenarios, uphill, terrain blocking LOS, and downhill for location shown in Figure 3. In the uphill and downhill scenario, the saturated throughput can be about 12 Mbps, because of the clear line of sight between two nodes. Figure 12 presents the improvement in saturated throughput and error rate of uphill and downhill scenario, compared with the over the hill scenario. As seen in Figure 12, the saturated throughput measured over the hill decreased 28% when compared to the uphill scenario. Similarly, the saturated throughput decreased 29.6% when compared to the downhill scenario. Compared to the downhill scenario, the error rate increased 243%, which indicated significant performance degradation although the throughput is still as high as 8.8 Mbps.

  For wireless communication received signal strength plays a significant role on the intelligibility of the signal. Therefore, the impacts of different terrain on ITS communication performance was studied.

Table 5 Field measurements for testing terrain effects

Scenario	Datagram Error Rate	Saturated Throughput	UDP Bandwidth	TxPower	SNR
1 – Uphill	4.50%	12.3 Mbits/sec	13Mbits/sec	50mw	-67 dbm
2 – Terrain blocking LOS	12%	8.8 Mbits/sec	13Mbits/sec	50mw	-78 dbm
3- downhill	3.50%	12.5 Mbits/sec	13Mbits/sec	50mw	-69 dbm

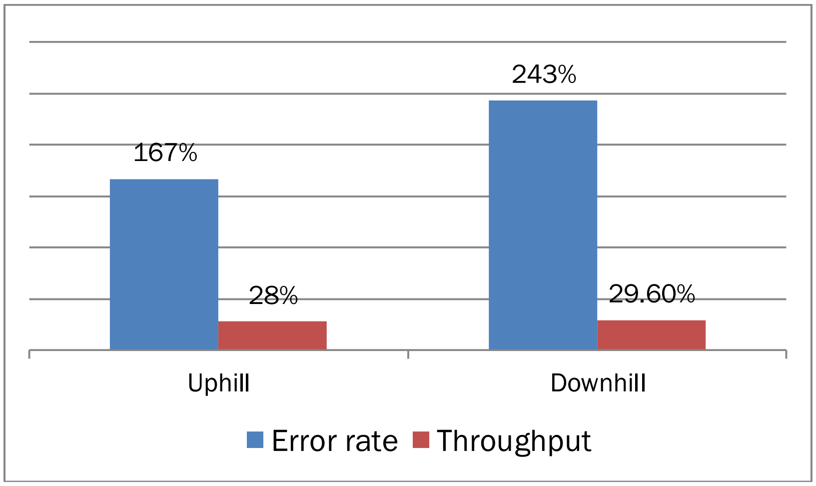


Figure 12 Improvements in error rate and throughput compared to "Over the Hill"

- Study the effect of transmitted power on Throughput for a different location:

  Location: SC State 93 (May to August, 2008)

In this case saturated throughput was measured at one distance using iperf. Figure 13 presents maximum achievable throughput at different transmission power levels in TCP mode. The distance between the transmitter and receiver is about 400 ft. Modulation rate was set as auto. As shown in the Figure 13, the throughput increases sharply, from 4.25 Mbps to 7.81 Mbps, when the transmission power increases from 5 mW to 50 mW. The throughput increase begins to slow when the transmission power increased beyond 50 mW.

Apparently, the throughput measurement at this location is very different from the measurement from Williamson Rd (Figure 9). Therefore, besides modulation limits, each location is associated with its own environment factors that limit the system performance. Possible factors include traffic condition, foliage blockage, even interference from nearby wireless communications.

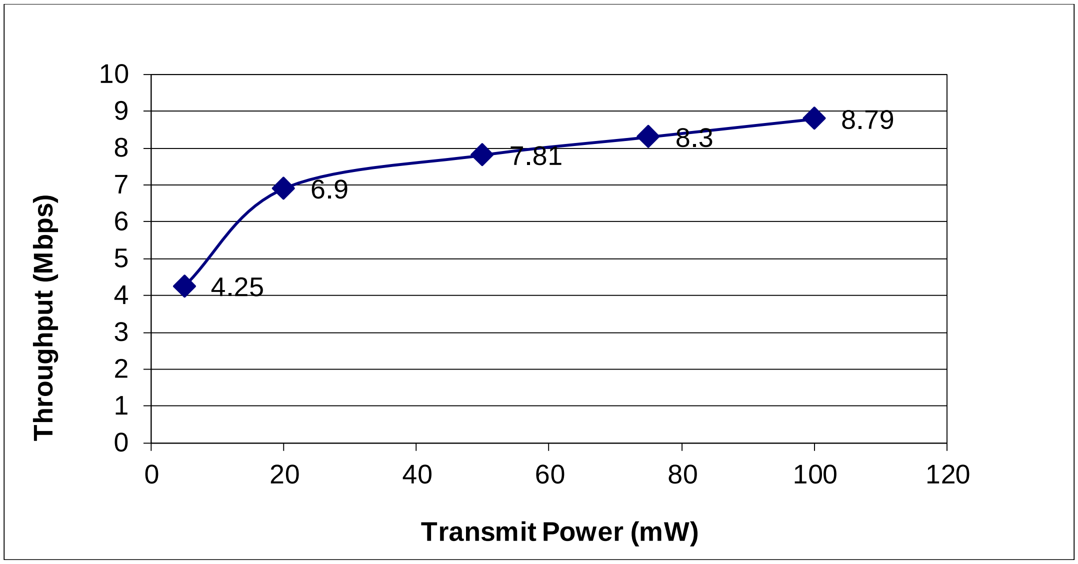


Figure 13 Saturation throughputs at different transmission power (TCP)

5.1.2.5 *Summary of the field study*

1. Modulation Rate has a significant impact on the maximum throughput and delivery ratio. For ITS applications requiring higher throughput should have higher modulation rate. However if successful delivery ratio is considered as the most important factor, there are limitations on the maximum throughput that the system can achieve as well as the sensor spacing that is allowed. For the test conditions considered 300 feet is the threshold distance between transmitter and receiver beyond which the system performance degrades.
2. The received signal strength indeed varies with different modulation rates and transmission power levels. When traffic agencies implement wireless traffic sensor network in the field, Equation (1) must be refined with on-site measurements. Future research should be undertaken to quantify the impacts of the transmission power and modulation rates, and derive a constant K to be a reference for traffic agencies applying 802.11 b and 802.11 g technologies for ITS applications.
3. Line of Sight is a very decisive factor for choosing Wi-Fi communication between two nodes.
4. In order to identify the achievable performance, such as saturated throughput, delivery ratio and received signal strength of the communication link at one particular location, similar field test needs to be conducted following the procedure proposed in this section.

5.1.3 WiMAX Field Test

Aim: To evaluate the feasibility of deploying a regional WiMAX network for traffic surveillance in terms of performance, coverage and variation of client radio capabilities and power supply requirements

According to the literature review, the authors found out that there have not been many studies that have reported the performance of WiMAX networks with respect to requirements for advanced traffic management, or the feasibility of using a regional WiMAX network to support ITS applications. Thus, the first step was to identify the most appropriate transmission spectrum for ITS from the wide WiMAX spectrum range, the spectrum which is appropriate for ITS must be chosen, and more specifically, the WiMAX system profiles must be selected for traffic management applications. Moreover, the performance of a typical WiMAX CPE on real roadway environments needs to be evaluated to find out whether it can support the required data bandwidth for effective and reliable traffic data transmission.

WiMAX supports connectivity between base stations and client devices either for line-of-site (LOS) or near-line-of-site (NLOS), making it an attractive option for urban application where LOS is unlikely due to buildings and trees. However NLOS WiMAX application may require increased power to support the same throughput as LOS application, which can make mobile WiMAX more costly. Furthermore, WiMAX also supports dynamic modulations where optimal modulation is selected based on environmental signal propagation conditions (Nuaymi 2007). Based on the knowledge of bandwidth requirements and range coverage, different modulations will be selected by the WiMAX base station. Modulation robustness ranges from 64 Quadrature Amplitude Modulation (64QAM) to Quaternary Binary Phase Shift Keying (QPSK) even Binary Phase Shift Keying (BPSK), etc. QAM, which is a modulation scheme, alters the amplitude of two carrier waves to convey data (Nuaymi 2007). QPSK is a two-bit digital modulation that conveys data by changing the phase of the carrier wave. BPSK is a one bit modulation. Lower rate modulation schemes are more robust to receiving low signal to noise ratio (SNR) signals. The further the client subscriber is from the base station, the greater possibility that of a modulation rate, as shown in Figure 14 (H'mimy 2005).

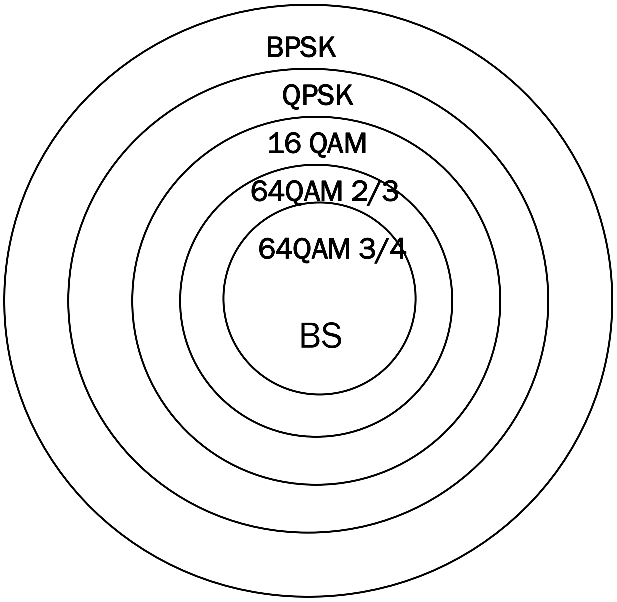


Figure 14 WiMAX modulations with respect to distance

5.1.3.1 *WiMAX Testbed and Experimental Setup*

- Dates when conducted: June through July, 2008.
- Location: Fairmount, West Virginia

The WiMAX network at Fairmount, West Virginia, consists of three base stations and each station has two or three 120 degree antennas. One station is located on the rooftop of the Research Center, West Virginia High Technology Consortium Foundation (WVHTC) building with altitude 1341.7 ft (refers to the BS1 in the Figure 15). The other two, called Verizon tower (BS2) and Fairmount tower (BS3) are located on the top of the hills within the city limits. The altitude information of Fairmount tower was not available. The research center had 2 sectors, the Verizon tower had 2 sectors, and the Fairmont antenna had 3 sectors.

Antenna height for all these three towers are approximately 160 ft. Figure 15 illustrates the sectors supported by the directional antennas and the approximate coverage (in miles) associated with each base station. All these three base stations are high powered and produce a maximum effective isotropically radiated power (EIRP) of 40 dBm. EIRP is a measure of the effective power emitted by a transmitter, or received by a receiver (Tse and Pramod 2005). The technical characteristics of the experimental testbed are shown in Table 6.
There were two types of tests conducted, fixed and nomadic. In Fixed operation, a client radio, Airspan EasyST, was located in a stationary car. In nomadic operation, the performance was measured when the car was moving. The client radio is a higher power M-A/COM subscriber (with an external 6 gain dB) antenna attached to the roof of the test car while the measurement tool was operated in the car. The equipment operated in the

4.9 GHz band reserved for public safety operations. All measurements were taken on or near the highway. Due to the geographic and environment characteristics of the city of Fairmount, West Virginia, some test locations or segments of the road did not have clear line of sight with the base station due to large amount of vegetation and presence of hills in the area.

During the nomadic test, the client antenna did not always have line of the sight to the associated base station. Client radios were fixed to one channel during all testing to avoid handoffs. Future work will focus specifically on the impacts of handoffs. Figure 15 illustrates the experimental set up.

The network testing tool *iperf* was used to obtain application throughput measurements. A laptop was used for collecting the data through *iperf* and was positioned in the test car for each test, and then the *iperf* program transferred as much TCP data as possible for 10 seconds; first in the upstream direction and then in the downstream direction. The *iperf* is configured to display the observed TCP throughput every second, and the modulation was assumed constant during the transfer process.

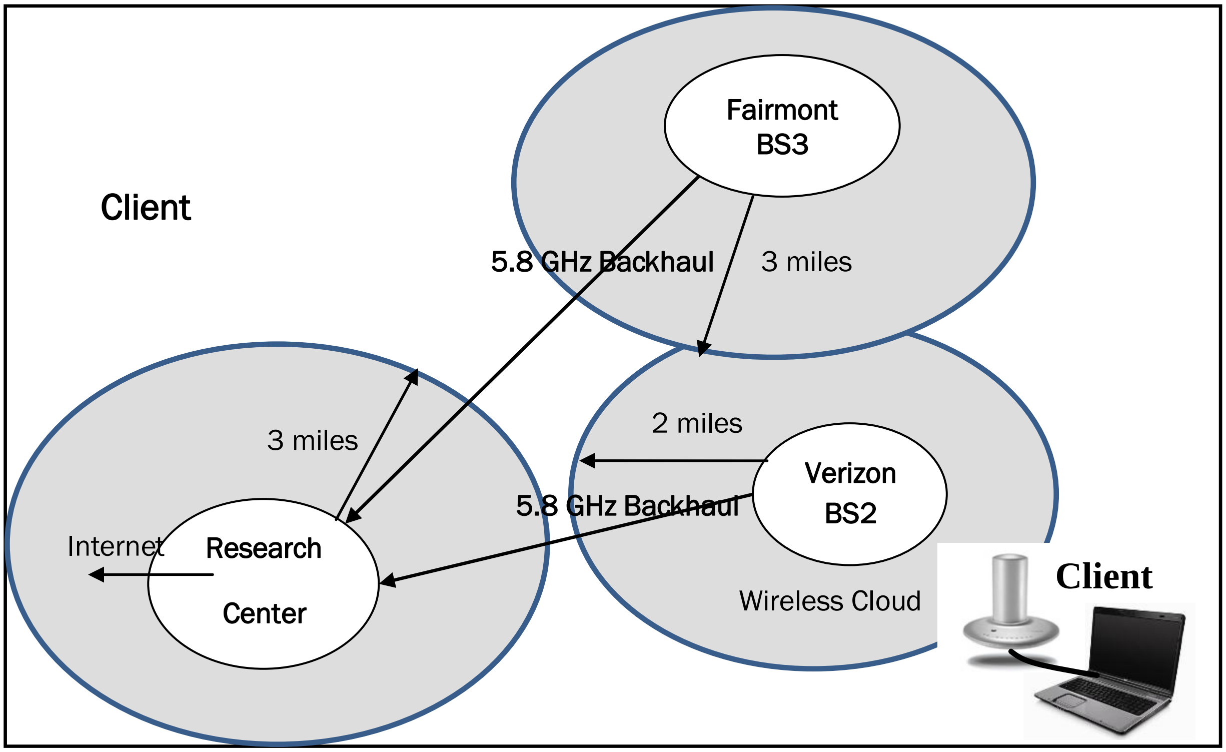


Figure 15 Network diagram and coverage of WiMAX experiments

Table 6 Technical characteristics of WiMAX experimental test bed

Base Stations/ CPE	
Standard Compliance	IEEE 802.16d
Bandwidth	5 MHz
Duplex Method	Time Division Duplex (TDD)
Modulation Supported	BPSK, QPSK, 16QAM, 64QAM
Maximum Transmitted Power	Up to +40dBm per antenna element
Maximum Radiated Power	EIRP 40
Rx sensitivity	-115dBm(1/16), -103dBm(1/1)
Frequency	4.9 GHz
Antenna System	
Degree	120
Gain	12 DBI

Figure 16 Network diagram and coverage of WiMAX experiments

5.1.3.2 *Analyzing the results of the tests*

The following section presents the results for the various WiMAX field tests. We initially summarize the results for Fixed WiMAX operation and then nomadic operation.

1. WiMAX Fixed Operation Test

   Seven locations were selected to measure both the upstream (US) and downstream (DS) throughput. Upstream is the data transmission from the client side to the base station and downstream is from the base station to the client. Table 7 summarizes the throughput measurement and modulation of each test location. The throughput results represent the average of ten 1-second samples as observed by *iperf*.

Table 7 Performance measurement results of WiMAX fixed operation test

Location No.	Average US TCP Throughput (Mbps)	Average DS TCP Throughput (Mbps)	US Modulation	DS Modulation
1	714 Kbps	900 Kbps	BPSK1/2	64QAM3/4
2	1.5	1.8	QPSK1/2	64QAM2/3
3	2.2	2.7	QPSK3/4	64QAM2/3
4	2.9	3.6	16QAM1/2	64QAM3/4
5	4.4	5.4	16QAM3/4	64QAM3/4
6	5.8	6.2	64QAM1/2	64QAM3/4
7	NA	6.3	64QAM3/4	64QAM3/4

**Note: NA means the data was not available*

As shown in Table 7, the observed average upstream throughputs of all seven test locations range from 714 Kbps to 6.3 Mbps depending on the distance and environment. In this experiment, the authors observed substantial losses at multiple occasions. The link errors will likely lead to end-to-end retransmissions, which consumes usable bandwidth and leads to throughput degradation. The disparities in throughput while using a common modulation scheme (e.g., the downstream TCP throughput for locations 4, 5, and 6 were quite different even though the same modulation was used) reflect relative packet loss.

Today’s standard definition video surveillance format can consume large amounts of bandwidth (up to 2 Mbps for high quality H.264 content). The purpose of the fixed operational test was to provide rough data points demonstrating that WiMAX can support current standard definition video traffic devices. With a typical data rate requirements ranging from 64 Kbps to 384 Kbps for each traffic camera (Gordon et al. 1993), the test network is clearly capable of supporting useful camera-based surveillance systems.

2. WiMAX Nomadic Operation Test

In these tests the authors basically studied how the location of base-station and the choice of consumer equipment might affect the received signal strength. Nomadic operation test uses a coverage measurement tool that was developed by the School of Computing at Clemson University to assess the coverage of the WiMAX network (Martin 2008). This tool is a program that collects information such as time/date, GPS location, vehicle speed and various measures that represent the link connectivity quality, including the received power signal strength and the signal-to-noise (SNR) level. During a data collection 'run', data samples were obtained frequently (every 1 second), and recorded by the laptop. The program runs on a Linux host which is connected to the WiMAX network through a client radio.

A web site, using Google map service, was used to visualize the datasets. The data at each point is represented by a color-coded ice cream cone symbol. The top part of the symbol represents the most recent downstream received signal strength indicator (RSSI) statistic observed by the radio and the bottom cone represents the most recent downstream SNR. RSSI is a value representing the received signal strength in dBm (ANACOM). Green, yellow, orange and red stand for level of excellent, good, fair and poor, respectively. Black means no signal detected, thus there is no connection at all. Figure 16 shows the legend used in the visualization results.

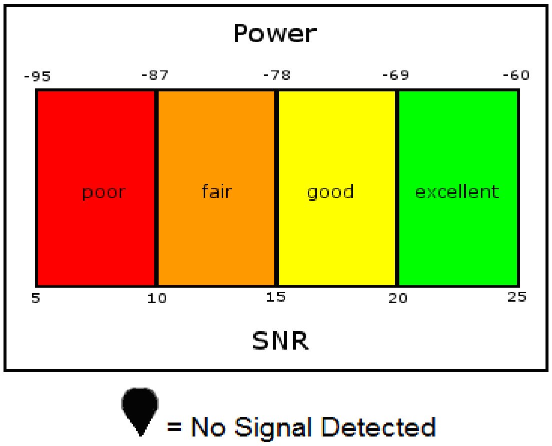


Figure 17 Legend of connectivity level

i. **Effect of location of Base-station:**

In this we studied how line-of sight plays an important role in WiMAX network by choosing one of the previously mentioned base stations at the test location. The Figures 17 to 19 illustrate the connection status while the test vehicle was driving along several paths on the highway. The vehicle speed (obtained from the client GPS device) was generally slower than 25 mph.

a. In the first path, the driving started from the research tower and then went onto a highway, next to the I-79, for about two miles. The client radio was fixed to BS1 during the test. As shown in Figure 17, signal level was very good at the beginning points, however it started to drop sharply as the distance between the BS1 and the client radio increased. The black segment was caused by NLOS because the road is located next to a hill.

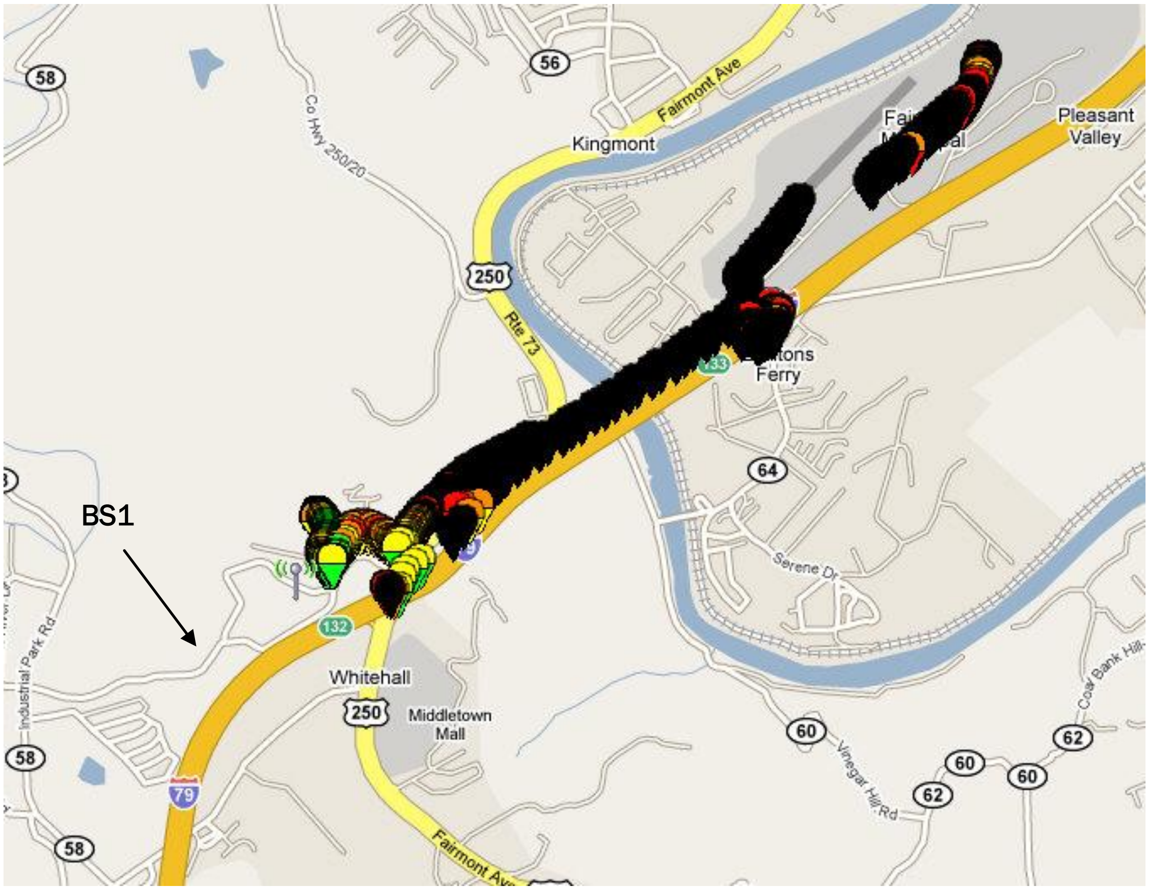


Figure 18 Connectivity level when associated with BS1

b. Figure 18 demonstrates the connectivity level while the vehicle was driving on highway US 19, which is across the downtown area, and the client was associated with BS 2. The black section was caused by the obstructed buildings in downtown area.

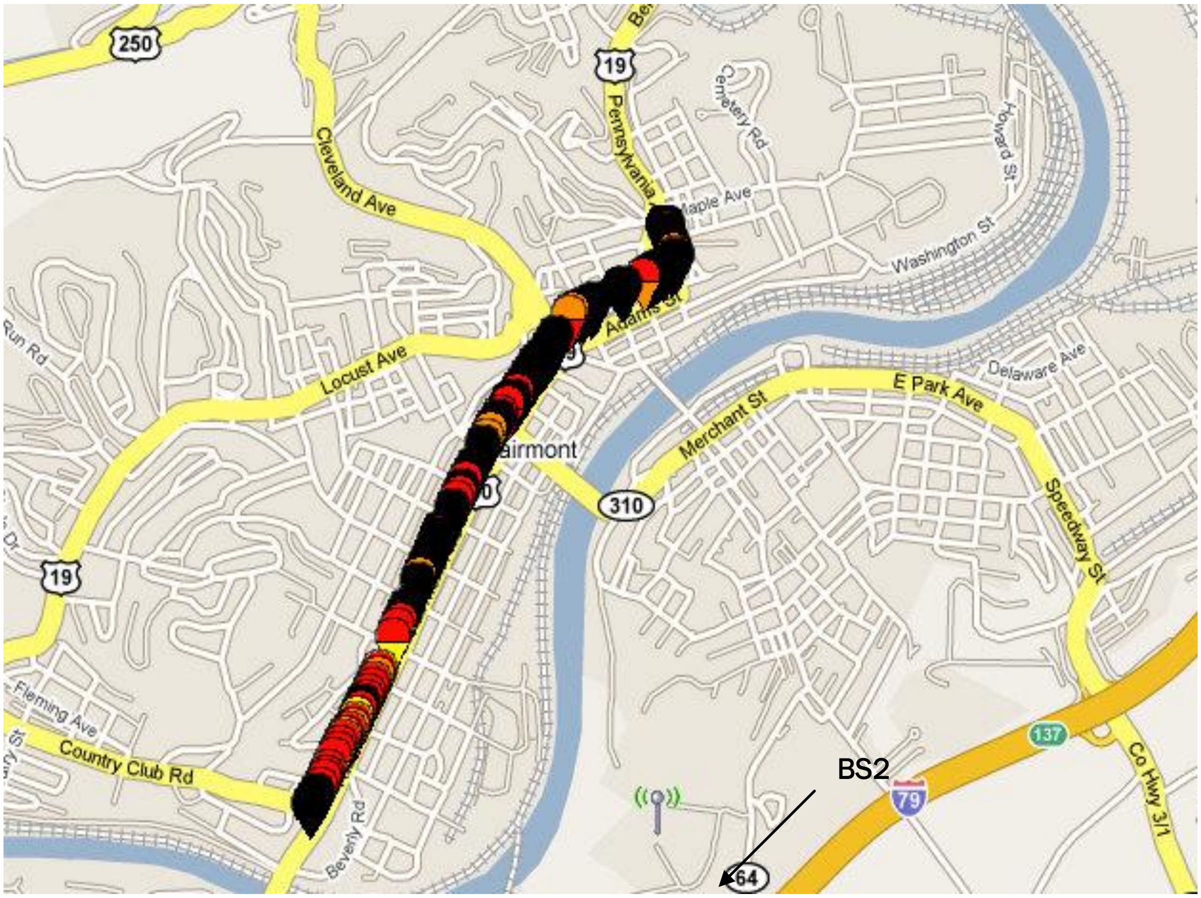


Figure 19 Connectivity level when associated with BS2

c. Figure 19 shows very good connectivity all along the way because the BS 3 located at very high altitude on the top of a hill; however detailed altitude information was not available. In this case, the client always had very good LOS, ensuring an operational link.

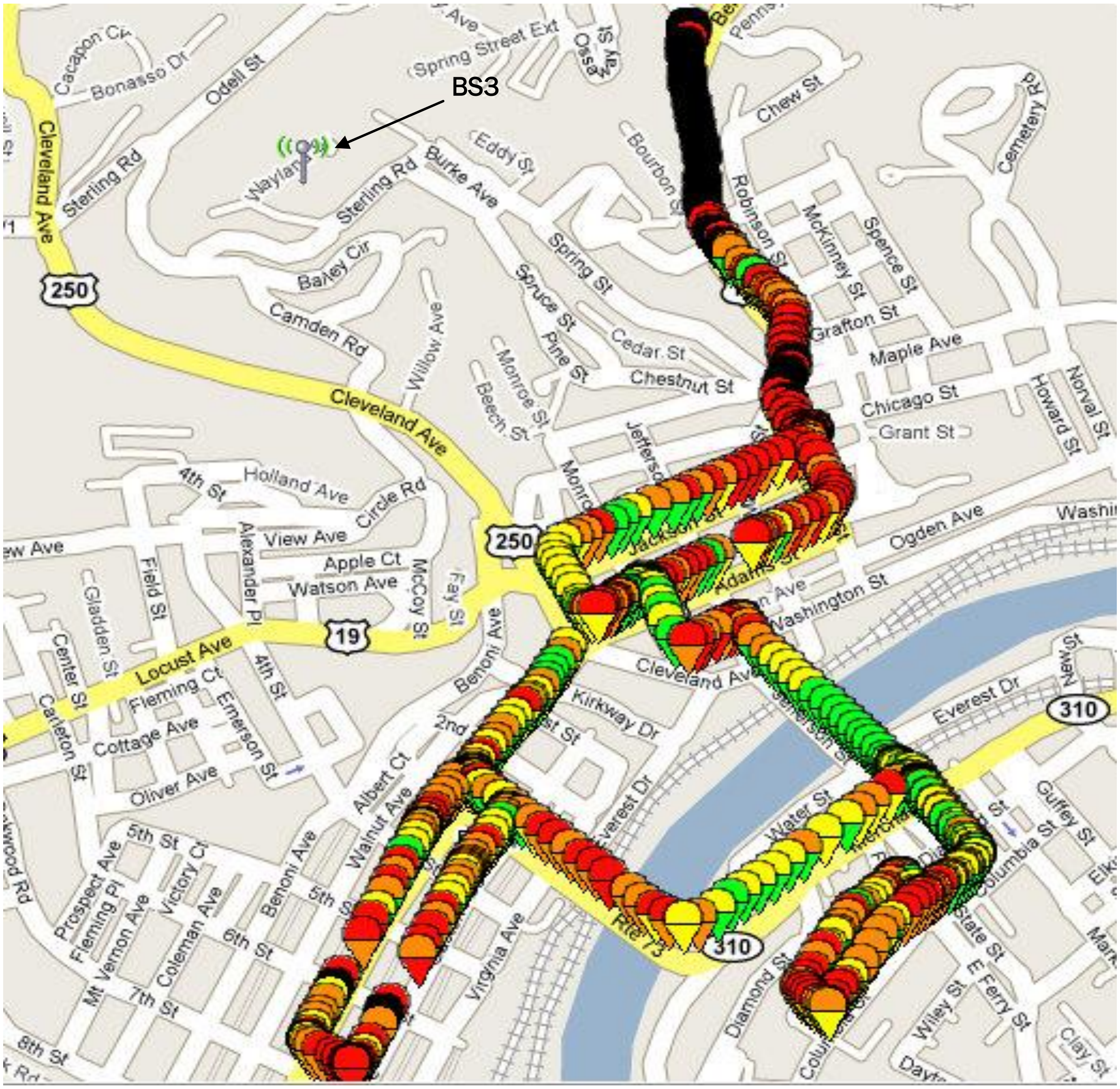


Figure 20 Connectivity level when associated with BS3

The performance of the network primarily depended on whether the client was in line of sight of the BS. When in line of sight, the coverage extended for 1 to 2 miles. .

ii.Choice of CPE

For the WiMAX field test, client devices, and in particular the quality of the antenna system also plays an important role. Figure 20 compares the connectivity performance of the same driving path but with different client devices. The left one used an M-A/COM radio and the right one used an Airspan EasyST radio. The test location was in parking lot in front of a mall.

While driving slowly around the parking lot, the client maintained LOS with the base station for most if the time. The Airspan EasyST clearly achieved better connectivity in this scenario. With one data point located at the furthest most distance from the base station (roughly 2595 feet away), the Airspan radio receives a signal strength of 30 db higher than observed by the M/ACOM radio.

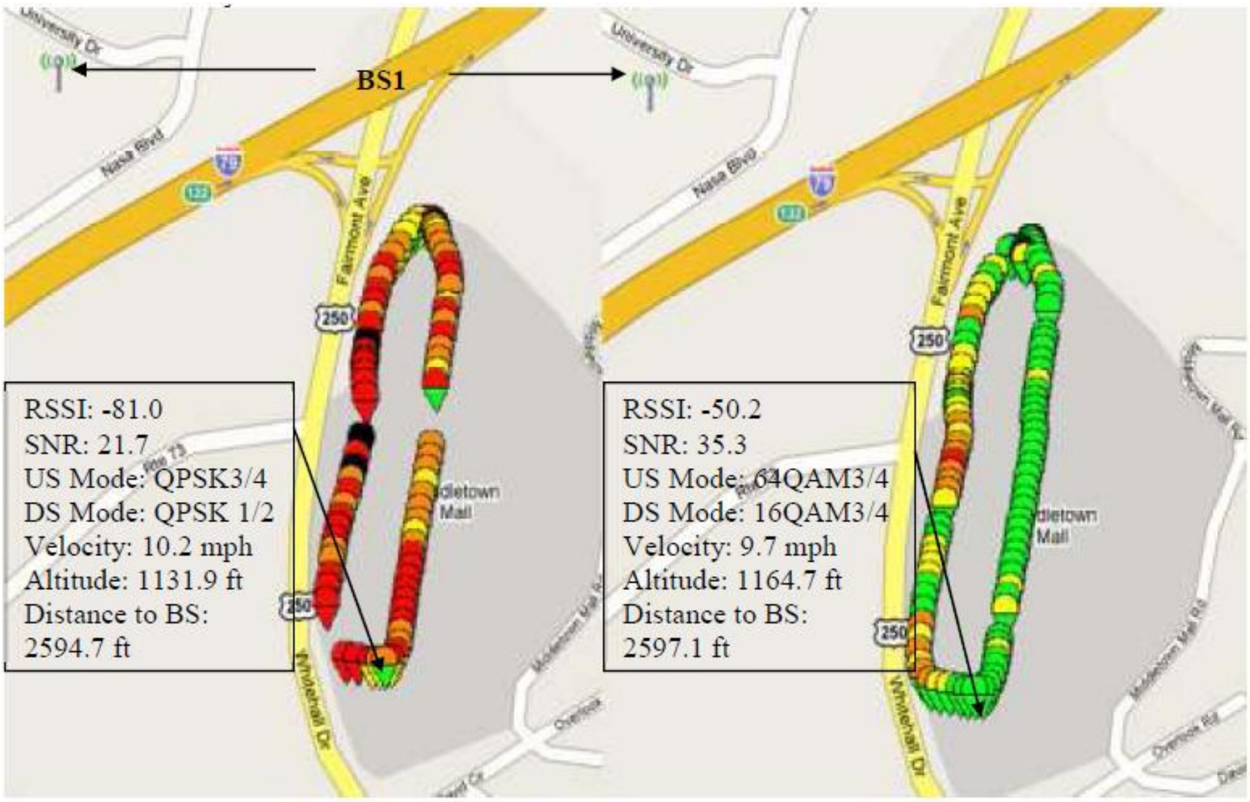


Figure 21 Connectivity comparisons between different client devices

5.1.4 Discussion of Power requirements

Supporting a large scale wireless network with wired power supply may negate the advantage of using wireless over wired applications. Additionally, wired power supply may not be available or expensive to install in rural areas where wireless communication is needed. Therefore, power supply must be considered as part of the systems planning and design when using WiMAX to support ITS applications.

Using traffic surveillance application as an example, this section proposes a solar power configuration to support both the traffic camera and required client radios along the highway. Solar power is a clean and renewable energy that uses solar panels to collect sunlight and convert the light into electricity for power supply (Mrsolar 2008). Each solar panel is comprised of many solar cells and absorbs the photons to initiate an electric current. Presently, solar panel arrays can be sized to support the most of demanding electrical load requirements and have been widely applied to home or commercial applications, such as remote traffic controllers, telecommunications equipment and facility monitoring.

The size of solar panel needed for traffic camera and client device depends on the power loads. For stakeholders to design and build their own solar supply traffic surveillance system, the first step is to calculate the current and voltage of the client WiMAX radio and traffic camera, and then to calculate the watts needed. Table 8 shows the proposed solar power size based on regional sun rate, solar module, solar rating and power needs of client radio and traffic camera. Sun rate stands for the amount of sunlight exposure throughout the year of different regions, normally measured in kWh/m^2. Using the southeastern area as an example, the average sun rate is 4.5 (Mrsolar 2008).

Power specification, such as the DC (direct current) voltage and watts, for the traffic camera and client radio have been estimated according to vendor advertisements and are summarized in Table 8 (ITERIS 2008, BP Solar 2008*)*, assuming the traffic camera is working 8 hours/day to support continued traffic monitoring.

Among several available solar modules, the authors chose SX-40 and SX-50 as examples, which are general-purpose modules suitable for single-module 12-volt applications with DC system voltage (BP Solar, 2008). Theoretically, the maximum power, P_{MAX} , of these two models are 40w and 50w. The warranted minimum P_{MAX} of these two are 36w and 45 w, respectively. Battery rating is a term used to measure cumulative energy going into or out of the batteries, which provides an estimate of state-of-charge (SPS, 2008). Solar array is a group of solar panel designed to support an application.

Table 8 Examples of solar power configuration for supporting traffic camera

Sun Rate	Traffic Camera		Client Radio		Base DC Voltage (v)	Total Load (watts)	Solar Module	Battery Rating	Solar Array
	Watts	Hours	Watts	Hours					
4.5	20	8	22	8	48	420	SX50	100 amp hours, 12V	4 modules in series 1 module in parallel 4 SX50 modules needed 52.7% larger than the required amount
4.5	20	8	22	8	48	420	SX40	100 amp hours, 12V	4 modules in series 1 module in parallel 4 SX40 modules needed 21.9% larger than the required amount.

As shown in Table 8, 4 SX-series solar modules are needed for each WiMAX wireless network supported traffic camera, 4 modules in series and 1in parallel. The proposed solar array is 52.7% larger than the required energy amounts when more numbers of SX-50 is used; the value decreases to 21.9% by using SX-40. Number of modules needed also changes while using other solar modules. The more numbers of devices required, the larger size of solar array is needed. Therefore, stakeholders need to consider the power requirements, operation hours and available installation to save energy consumption, installation space and the cost. Detailed size and cost information were not the focus of this analysis.

Cost of building a WiMAX network, which includes base stations, client radios and other related fees, is another important issue that needs to be considered for any deployment decision. Typical cost for a client station is about $2200 and a base station is about $10,000. However, these numbers can be deceiving as most vendors might make clients purchase other necessary tools, such as network management software, which will add to the deployment costs.

5.1.5 Summary of the field test

1. Considering the typical data requirements of a surveillance camera ranging between 64 Kbps to 384 Kbps, the test network using WiMAX is capable of supporting useful camera-based surveillance systems.
2. As revealed by the field test, several issues must be considered to deploy a WiMAX network for ITS applications. First, the location of the WiMAX tower is crucial. Second, client devices need to be tested beforehand to ensure the performance can meet the minimum communication requirements for different ITS applications.

5.2 Quality Requirements of Online Traffic Surveillance

Aim: To map the jitter and packet rate with real-time video quality, recommend tolerated jitter values and acceptable buffer sizes for effective online traffic surveillance.

Video streaming or supplying a receiving computer with the video by packets of data, usually in a real-time fashion, is becoming widely popular for many applications, such as video conferencing, online gaming, and delivery of educational or entertainment content (Wu 2001). The recent advances of wireless technologies and rapid development of video streaming applications enable the possibilities of using wireless Internet to access real-time traffic video. However, the transmission of real-time traffic video typically has different requirements than video conferencing and online gaming.

In the view-point of traffic surveillance, the streaming must be in real time in order to be effective for on-line traffic management and operations. This type of real time video streaming requires that all factors causing delays in live streaming video are kept under certain thresholds. These factors include 1) jitter 2) packet loss rate and 3) frame rate (Joe 1996). Jitter is the difference between the end-to-end delays of every two consecutive packets. If high jitter spikes occur, human eyes may see a jump in the video from one scene to another, skipping several frames in between (Hancock 2004). For example, the operators in front of the surveillance screen in a traffic management center (TMC) may not see a specific car moving through the traffic camera because of the lost frames, and such losses are not recoverable as the lost frames are never recorded. Using reliable transmission protocol such as TCP (Transmission Control Protocol) can recover such losses via retransmission; however, the requirement of transmitting an acknowledge packet to the video sender for each received video packet and retransmitting a video packet when its acknowledgement is not received incurs substantial delay and network load, rendering the resulting video performance even more unstable. The typical solution to remove such video quality fluctuation is to buffer video packets at the receiving end for a specified time before playback, such that the delay of retransmission of loss packets can be masked.

Possible reasons that might cause jitter in online traffic surveillance systems include the available bandwidth, number of users and required video image size. Next, a video can appear distorted if the packet loss rate, which is the percentage of lost data packets when compared to the total data packets sent, is too high (Endoh 2008). The third cause of jitter is the frame rate, the number of frames sent out in every second, which is also referred to as average packet rate per second. Jitter is difficult to completely eliminate when working with a live streaming video because no buffer or limited buffer is allowed. Jitter can be a key factor of video quality degradation if not properly mitigated, lowering the effectiveness of the real-time traffic surveillance (Joe 1996).

5.2.1 Test Setup for Online Traffic Surveillance system

- Date Conducted: May-July 2009
- Location: Clemson, South Carolina

A traffic camera provided by the South Carolina Department of Transportation (SCDOT), was located on one side of the State Highway 39 (Perimeter Road), and was wirelessly connected to a router located in a nearby building which was approximately 1000 ft away as shown in Figure 21. The router was then connected to the campus computer Ethernet (wired system), which connected to the research laboratory computers as shown in Figure 22. The research lab was about three miles away from the camera location.

Figure 22 Solar power supported mobile traffic camera

The video data was sent to our lab computers first over the wireless network link, and then using the wired network link. Figure 22 demonstrates the experimental setup in further detail. There are multiple trees in between the building and the camera, likely blocking the wireless signal. To overcome these sources of obstruction or interference and those from other wireless sources, there was a 500 mW amplifier installed on the camera side to amplify the signal. The case study provided an approximation of the potential obstruction of wireless signal transmission in the field, and the possible degradation of video quality of real-time traffic surveillance over the wireless link. At the lab computers, the authors recorded the data packets and their arrival rates using three computer programs; iperf, SoftDVR lite and Wireshark. SoftDVR lite is IP surveillance software that can record incoming video streams to files and allows a single connection with a camera (MOXA 2009).

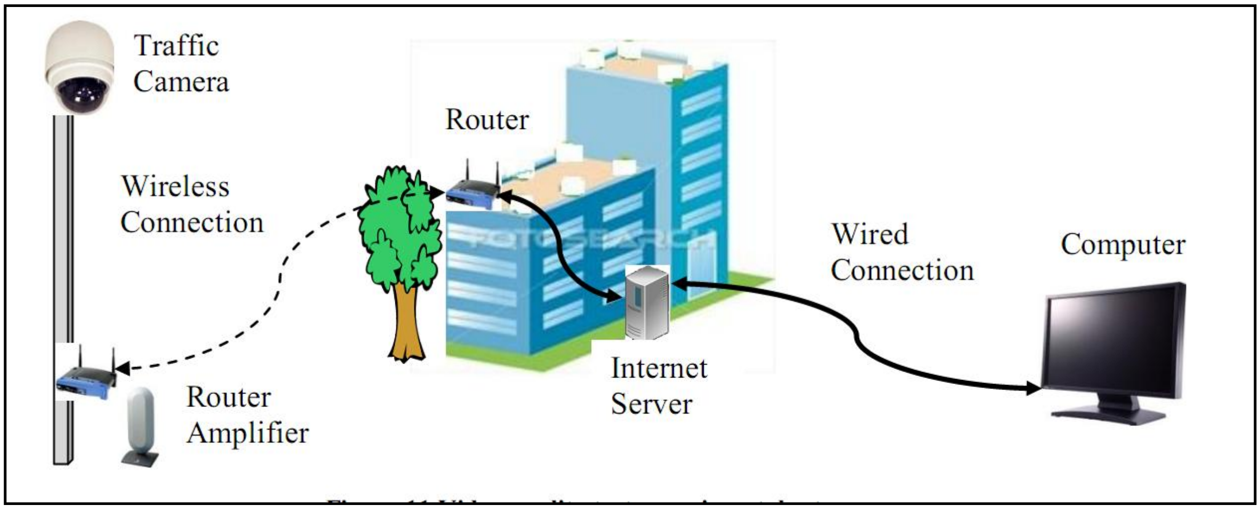


Figure 23 Video quality test experimental setup

For each experimental test, the researchers first used iperf to measure the overall throughput of the network link between the computer and the router connected with the traffic camera. Each iperf test was 60 sec in length with throughput measurements taken each second. The tests were repeated until a 95% confidence interval of the throughout fell within 5% of its estimated mean. After measuring the average network bandwidth, Wireshark was employed to track the data packets transmitted between to lab computer and the traffic camera to find the average throughput at the user end, average frame rate and packet travel time.

The incoming video was recorded through SoftDVR, where each test lasted 60 seconds, and average packet rates per second (frame rate) and average bandwidth were measured. The arrival time of each data packet was used to calculate the jitter (Joe 1996). As mentioned previously, given each packet's end-to-end delay, jitter is the difference between every two consecutive packets. Because the start transmission time of each packet is unknown, the difference of arrival time calculated based on Wireshark actually equals to the jitter plus the initial set up time. This time difference will be called jitter in the remainder of this paper. The recorded video was re-played after the tests to check the continuity and compare the measured jitter and packet rates to identify possible relations. The recorded video also includes time information, which is shown as a clock on the left corner of the image. Any video jump was identified as a discontinuity in the clock. Discontinuities greater than one second were considered as missed videos. All sixty-five cases were tested during five different days but under similar environmental conditions, such as the foliage coverage, temperature and weather. Traffic conditions, such as flow, speed and density were also measured to ensure the similarity of different test days.

5.2.2 Analysis of the Results of the Tests

- **Correlation analysis of jitter and missed video time:**

  In the very first test, the researchers conducted a correlation analysis of the jitter and missed video time in seconds. Table 9 demonstrates examples of the data collected during these tests. Due to our definition of jitter, the values of jitter extended to the order of few seconds.

  Each recorded video was replayed and compared to the number of video jumps and missed video times. These findings were then compared to the jitter calculated based on the Wireshark records and are displayed in Figure 23. The first significant jump, about 7 seconds, (see packet 84 in Figure 23) was caused by the initial link connection and was not considered in the video quality analysis. The second jump shown in Figure 24 (between packet 250 and 333) has a jitter value of about 3 seconds, and this matches with the 3 second missed video time, shown in the two snapshots in Figure 24. Similarly, the researchers found each of the other two jumps also caused approximately four seconds of video to be missing.

Table 9 Examples of jitter calculated and missed video time

Test No.	Jitter Calculated (second)	Missed Video Time (second)
1	3	3
2	5	5
3	10	10
4	6.5	7
5	16	24
…	…	…

Figure 24 also shows that a significant number of jitter values range between 0 to 0.2 second. Besides the four jumps, there are several other small jumps with values lower than 1 second. The recorded video showed that these small jumps didn't cause any discontinuity in the video.

The results of all sixty-five cases indicated that jitter values lower than 0.5 sec do not cause any data frame skips in the real-time video streaming, as shown in Figure 5. However, jitter between 0.5 to 1 seconds is likely to slow down the video, so actually user can see the vehicle slowly pass the camera view. These values are dependent on the distance between the camera and the DOT, the camera specifications and the bandwidth available. While carrying out similar tests, the above three parameters should be measured so that the system could be calibrated for further analysis. The value of jitter threshold would be then used for designing the play-out buffer sizes.

Also, the correlation coefficient of jitter and missed video sequence was 0.944, indicating a high correlation between them. These results thus indicate that jitter is a key indicator of the video continuity of the real-time video streaming, supporting the findings of previous studies.

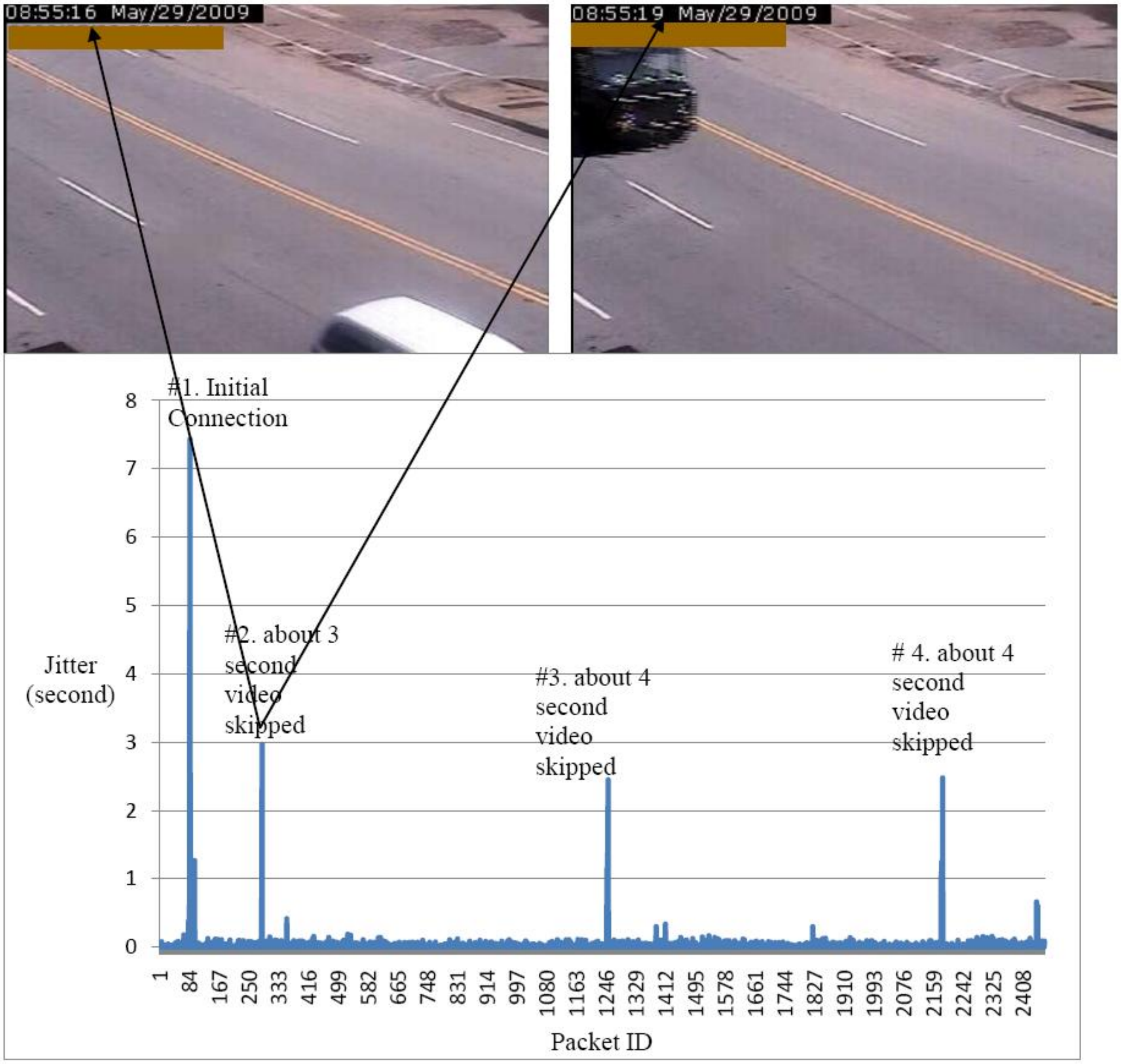


Figure 24 Example of the connection between jitter and video continuity

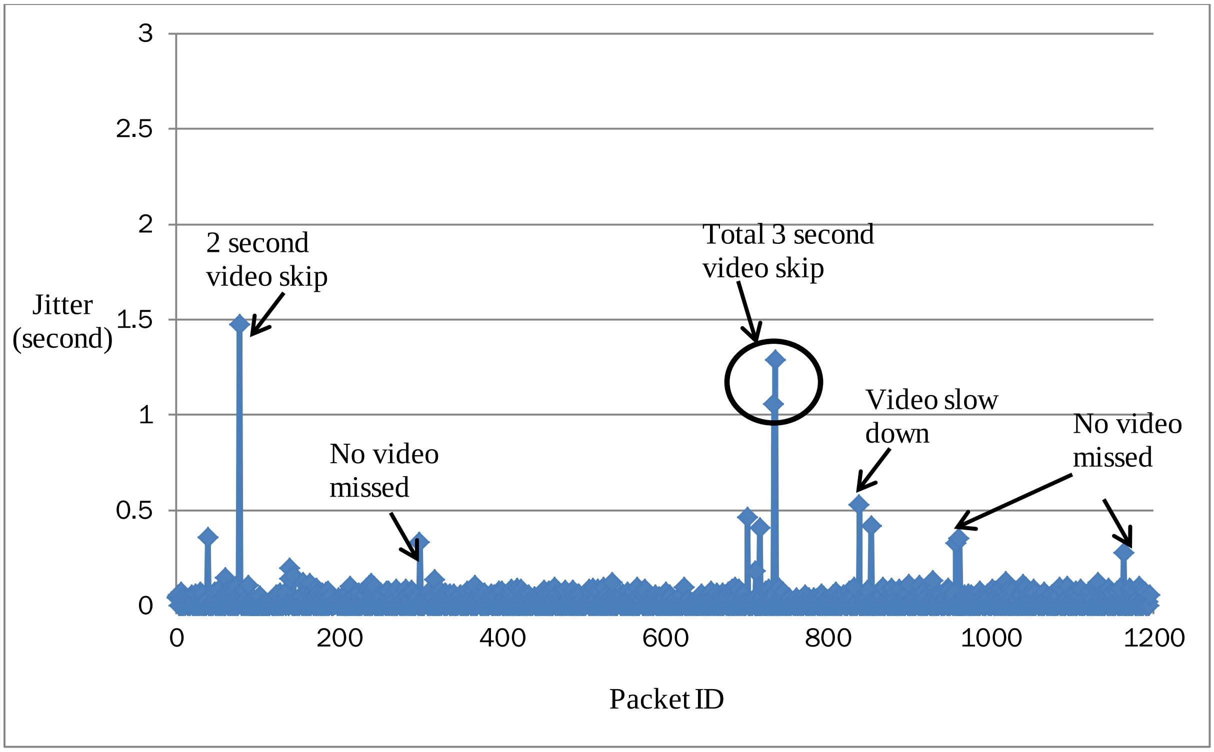


Figure 25 Example of the connection between jitter and video continuity

The following figure represents the factors deciding the size of play-out buffer.

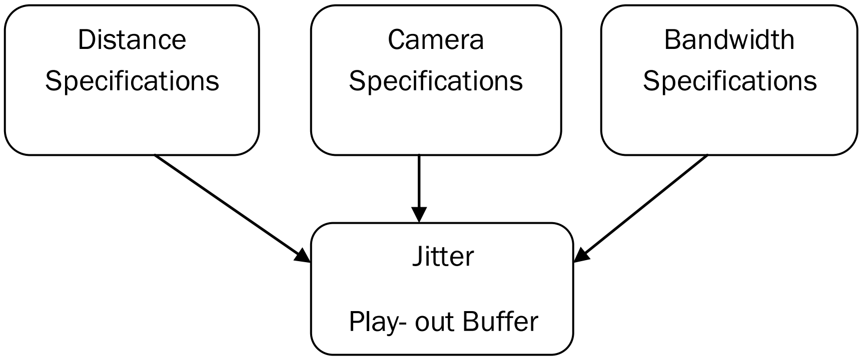


Figure 26 Factors affecting jitter

- **To identify the appropriate packet rate for the surveillance:**

The authors then assessed the packet rate range that provides acceptable quality of real-time traffic surveillance video. While analyzing the packet rates, it is important to consider the effect of different factors in the real scenario such as network throughput, number of users sharing the same bandwidth, and the image size (MOXA 2004). The frame size decided by the video transmitter for the traffic camera used in this field study is presented in the Table 10. This study chose quality level 'Standard' during the test period, so the corresponding theoretical bandwidth requirement was about 1784 Kbps.

Table 10 General frame size and required bandwidth (*14*)

Quality Level	Size of each frame	Bandwidth Required for 20 fps
Medium	9.3 Kbytes	1498 Kbps
Standard	11.15 Kbytes	1784 Kbps
Good	13.76 Kbytes	2202 Kbps
Detailed	16.35 Kbytes	2616 Kbps
Excellent	20.3 Kbytes	3258 Kbps

During this sub-test, average packet rate was calculated after every minute video transmission. Figure 26 shows the percentage distribution function (PDF) of the average packet rates in second (frame rate). As seen from Figure 26, although the packet rate varies within a wide range, from poor (~3 packets/second) to extremely well (~ 50 packets/second), the majority of observed packets were received at a rate between 23 to 33 packets/second. Average packet rate for the complete test was 26.3 packets/sec.

A manual inspection of the videos and the packet rates helped to investigate the rates for good perceptual quality video. When the rate was lower than 15, one or multiple disconnections were observed, while videos with rates higher than 40 packets/sec had no disconnections or slowdowns.

A cumulative distribution function (CDF) graph is generated as shown in Figure 27. The data indicated that most cases had packet rates around 23 to 33 since as indicated by the steeper slope within the circle in Figure 27. Visual observation of all study cases indicated those video has packet rate above 23 packets/sec delivered acceptable quality. Acceptable quality was defined as there are one to three small skips or slow down but no disconnection. This statement was based on the visual observation of all the study cases. Therefore, the authors concluded that the quality of the real-time traffic surveillance is acceptable when the packet rate is above 23 packets/sec.

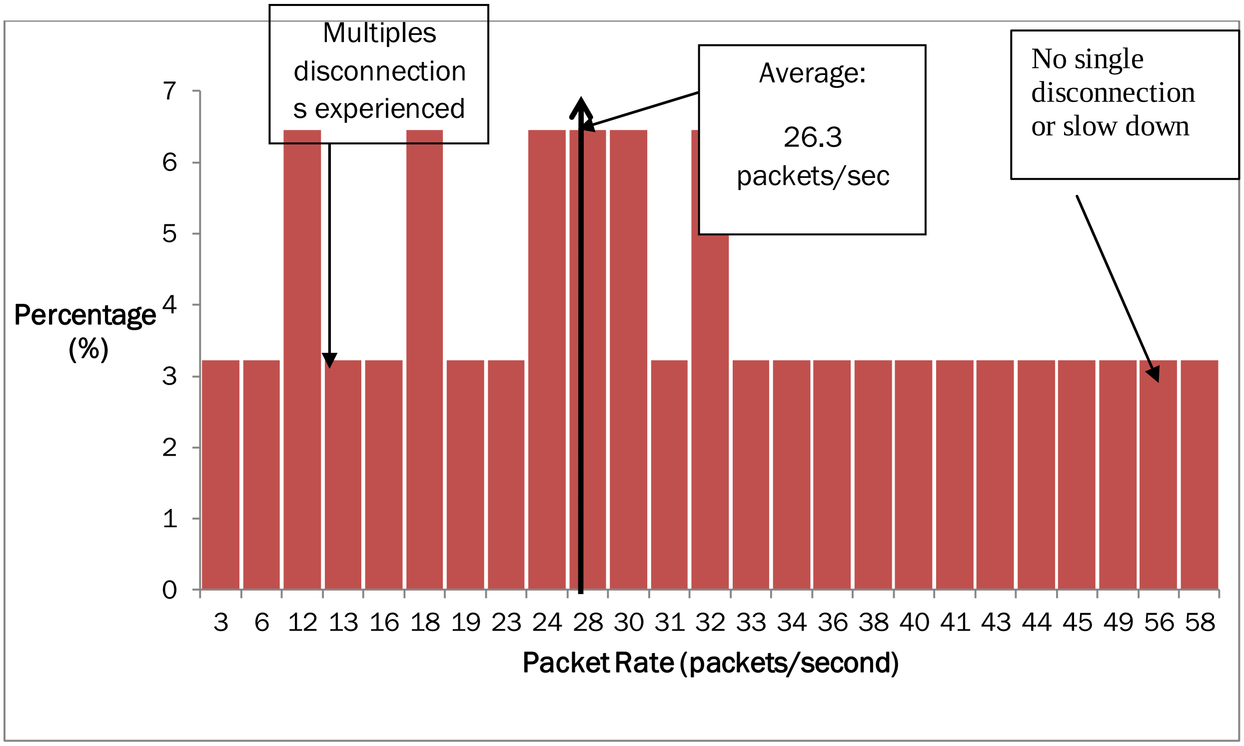


Figure 27 Percentage distribution function

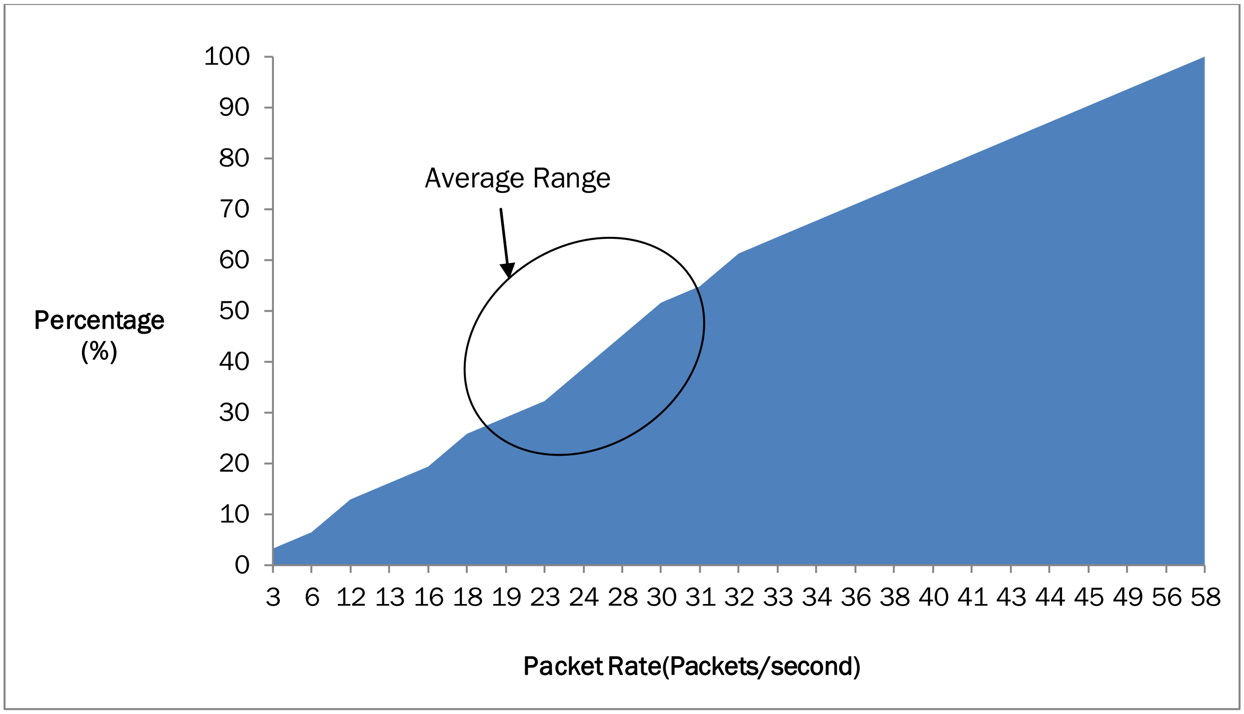


Figure 28 Cumulative distribution function of packet rate

- **Multiple Streaming:**

Considering the case of two computers receiving the real-time video image simultaneously, this study also assessed the degradation of the video quality. This case can be compared with two TMC computers checking the same traffic camera through a wireless system. The overall bandwidth of the wireless link measured by iperf is about 324Kbits/sec. This value was taken as the average of 90 runs done in 10 different days. The actual average throughput consumed of each video is about 201Kbits/sec for one receiving computer. Average throughput was taken at both of the two computers. The real throughput consumption of either one computer or two users or one user is much less than the theoretical throughput requirements shown in Table 10. However, the study results indicated that frame rate and jitter requirements are more significant requirements than the throughput for the case of real-time traffic surveillance. Smooth video image ensures the effective traffic surveillance and management.

Assume two receiving computers have the same video quality,

201Kbits/sec *2 = 402 Kbits/sec > 324 Kbits, The result indicated that two receiving computers may not receive decent traffic surveillance image during the same time.

Figure 28 compares the CDF curve of one receiving computers and two receiving computers. The cumulative distribution curve of two receiving computers reaches 100% much faster than one receiving computer. The majority of the packet rates of two receiving computers fell into the range of 9 to 19. The average packet rate was about 16.4 packet/sec. As previously presented, the acceptable real-time video quality requires rate at least 20 packets/sec for the standard quality. This implied that it was important to calculate the available bandwidth before streaming the video onto multiple computers.

During the case study, the researchers also observed that within the same test, it's likely to have one computer receiving smooth and continuous video image, but the video on the other computer is very slow or even disconnected. Even though there are two receivers, the case study probably still initiated two flows simultaneously. When two TCP flows compete for bandwidth, it is known that there may be short term inequality. When data is transmitting over TCP protocol, it reduces its window to slow down the rate once a packet drops.

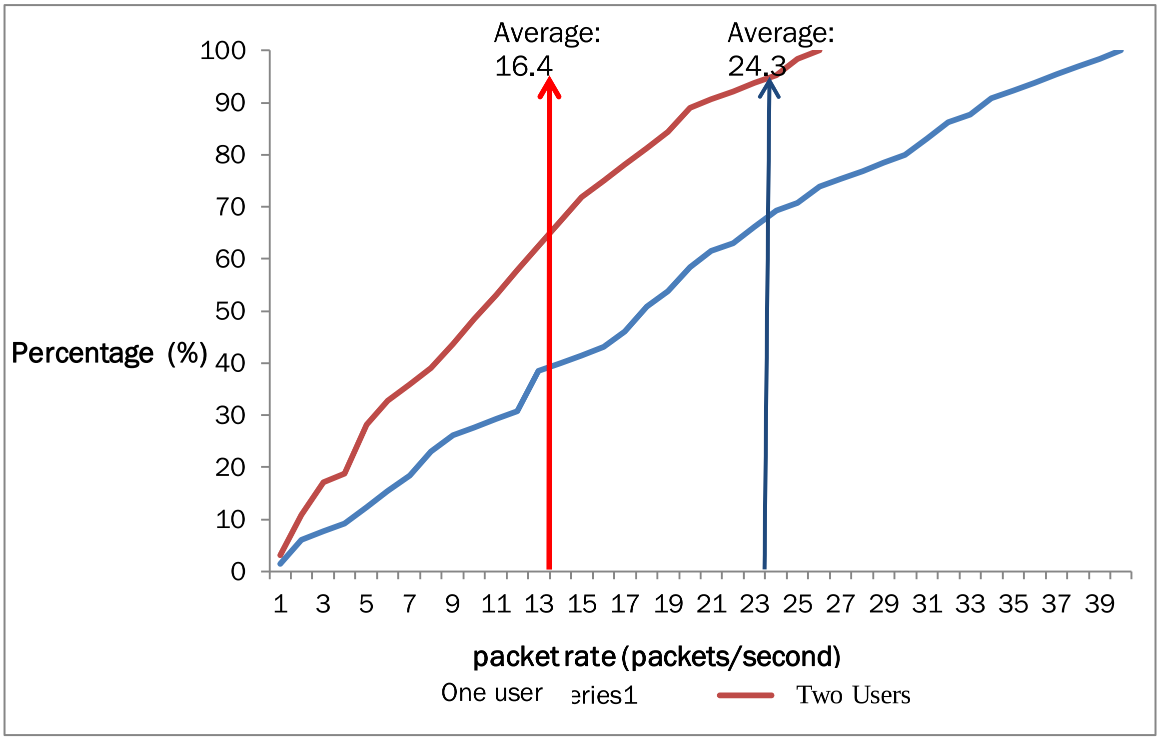


Figure 29 CDF Comparison of one and two receiving computers

To extend this test on a bigger scale, the team made use of the wireless LAN cards of the Laptops. In this experiment four laptops with identical W-LAN cards were used. The laptops/nodes were connected with each other over an ad-hoc network. The computers were arranged in such a way that one laptop was in the center and the three other laptops were at equal distance from the middle one.

VLC media player was used to transmit over multiple streams. The setup was so made that the center laptop was the source and the other outer 3 laptops were the receivers. Using *iperf* the usable bandwidth for transmitting to a particular computer was measured. Depending on the distance of the laptops from the center one, the available bandwidth changed with the highest of about 5 Mbps at distance of 10 feet from the center laptop. Now for the three streams, the bitrate for video was set to 2400 Kbps and 12 frames per second was set as the frame rate. The video quality was manually observed at the three receiving laptops. At the same time the received streams were also stored at the receiving computers. These files could be used for post analysis. Now the three laptops were equally moved away from the center laptop. Each time the received video was manually studied for the probable skipped sequences as well as jumps. Now a fourth laptop was brought in the scenario such that the bandwidth available for this new connection was barely 1 Mbps. Using a reduced bitrate of 1200 Kbps a video was streamed to this new computer. The video quality received by the forth laptop was obviously inferior. However the other laptops continued to receive a good quality video with very few jerks or misses.

The saved streamed videos were then compared with the originals using the MSU video quality assessment tool. Using peak signal to noise ratio (PSNR) and missed frames as the metrics the videos were analyzed. The results reiterated the findings of our visual assessment that with distance i.e. with reducing bandwidth the video quality degraded. This setup was entirely wireless and demonstrated the significance of calculating the available bandwidth before deciding the data rate i.e. frame size and frames per second.

To extend this finding further, the authors made use of the Axis Communications' Video Design Tool to estimate the bandwidth requirements for an exemplary scenario. Table 11 presents the summary when a single camera was used, Motion JPEG was chosen as the encoding standard and 10% compression was used. The camera had a 802.11g/b wireless interface and supported all the necessary IP protocols like Ipv4, HTTP, TCP, RTP etc

Table 11 Bandwidth Requirements for Axis IP camera

Resolution	Bandwidth with Motion JPEG encoding, 10% compression		
	12 fps	18fps	24fps
320X240	959 Kbps	1436 Kbps	1913Kbps
480X360	2157 Kbps	3232 Kbps	4304 Kbps
640X480	3834 Kbps	5745 Kbps	7652 Kbps

For state agencies interested in transmitting video images back to TMCs using a wireless link, especially for the mobile traffic cameras, this experiment provides basic requirements to ensure an acceptable video quality. Besides evaluating the video quality and proposing threshold buffer size and frame rates, the results presented in this section can also lead to future work related to the study of the quality of service of several TMCs collaborating with each other and monitoring the same highway segments during the emergencies.

5.2.3 Summary of the On-Line Surveillance

1. As a result of this field study, the authors concluded that jitter is an important metric which needs special attention while dealing with online traffic surveillance systems. A buffer of one second proved sufficient to eliminate impacts of jitter.
2. The field tests confirmed that the quality of real-time traffic surveillance is acceptable when the packet rate is above 23 packets/sec.

6 CASE STUDY

The case study is intended to provide guidance to SCDOT in the design of a wireless network for traffic surveillance application. The design procedure identified important parameters for wireless communication. Using a clustering approach, wireless communication networks for the existing ITS infrastructure for seven major cities of South Carolina was designed employing the Wi-Fi and WiMAX technologies.

A comparative analysis suggests that WiMAX mesh architecture required a smaller number of fiber optic connections as compared to Wi-Fi Mesh architecture. The hop count for WiMAX mesh network was lower. In section 8 we analyzed the cost of these architectures.

6.1 Description

Aim: To setup guidelines for the DOT personnel for designing wireless networks supporting ITS infrastructure.

A case study was conducted to present a process of planning for a wireless infrastructure to support an existing traffic surveillance system (comprising of traffic cameras, radar detectors, and DMS) in seven metropolitan areas in South Carolina, as shown in Figure 28. Two types of technologies, Wi-Fi and WiMAX combined with two network topologies, mesh and non-mesh (identified as infrastructure in the rest of the report) were considered. Cost analysis of each of the architectures is discussed in Section 8. This section presents case studies for two sites, Columbia and Greenville as examples. Data from the other case studies can be found in Appendix C. The output of the case study served as the foundation for the simulation study presented in Section 7.

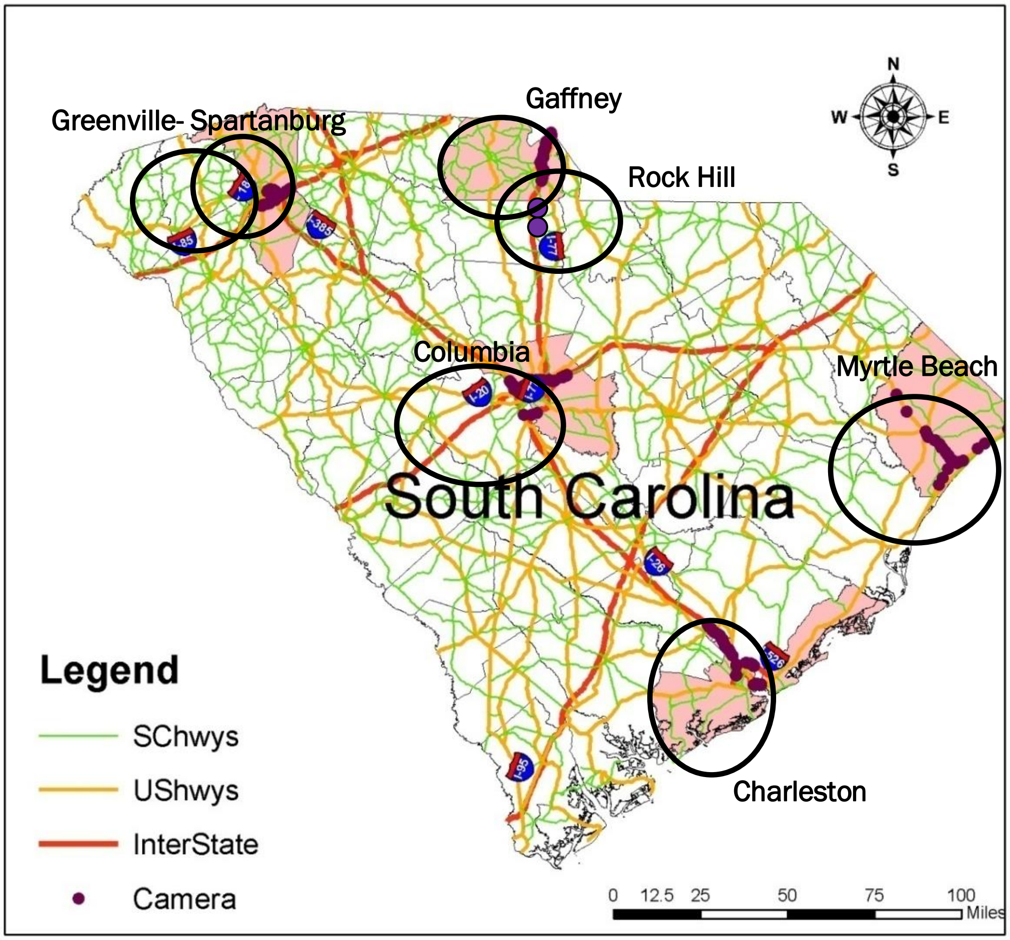


Figure 30 Seven study sites in South Carolina

6.2 Network Design Procedure: Clustering approach

The planning process for the study sites was proposed in [Zhou et al. 2009], and shown in Figure 29. This process presents a systematic method for planning a wireless network for traffic camera monitoring. Several implementation plans were considered, using a combination of different technologies, network topologies, and approximate costs.

There are four main aspects to planning a wireless traffic monitoring network. First, it is important to know the number and type of traffic surveillance devices (i.e Cameras or radar detectors) being connected to the network and the exact location of each. This is described as the “device locations” in the flowchart. After the location and number of cameras is known, the bandwidth required to support all of the cameras in the network should be calculated. Next, the topology of the network, the distances between the cameras and their configuration, is calculated. Finally, a repetitive process called “clustering” was conducted, allowing the cameras to form groups that are within radio range and that reduce the number of fiber optic connections required. After repeating the clustering process, until all cameras have their bandwidth supported, the preliminary design is complete. If the clustering process leads to no solution, either an additional access point can be added or the bandwidth requirements for each camera need reductions. Either of these choices leads to a restart of the clustering process.

The process of clustering involves reducing the number of access points in the system until the number of access points required to support the cameras is at a minimum. The procedure begins with each camera using its own access point, and then the access points are removed one-by-one and checked to ensure the system is still functional. After each iteration, the total bandwidth required at each access point is calculated and checked to ensure network stability. This process is repeated until a solution gets identified where each camera is connected to one access point and each access point serves multiple cameras.

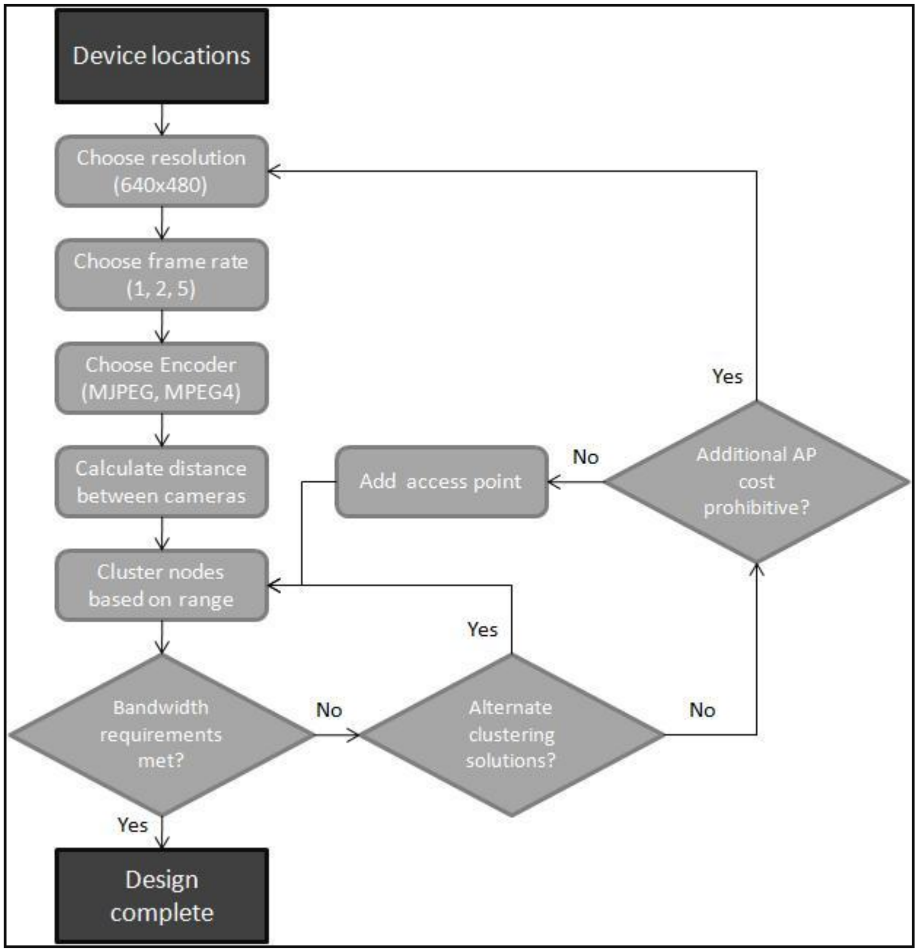


Figure 31 Flowchart for preliminary network design [Zhou et al. 2009]

There are three types of traffic surveillance devices, traffic cameras (CCTV), radar detectors and DMS, considered in this section. Radar detector and DMS normally are implemented with traffic camera on the same pole, so each node considered in the study networks might consists of several different types of devices. Table 12 summarized the number of traffic surveillance devices and their location in these seven major cities according to the data provided by SCDOT by October, 2008.

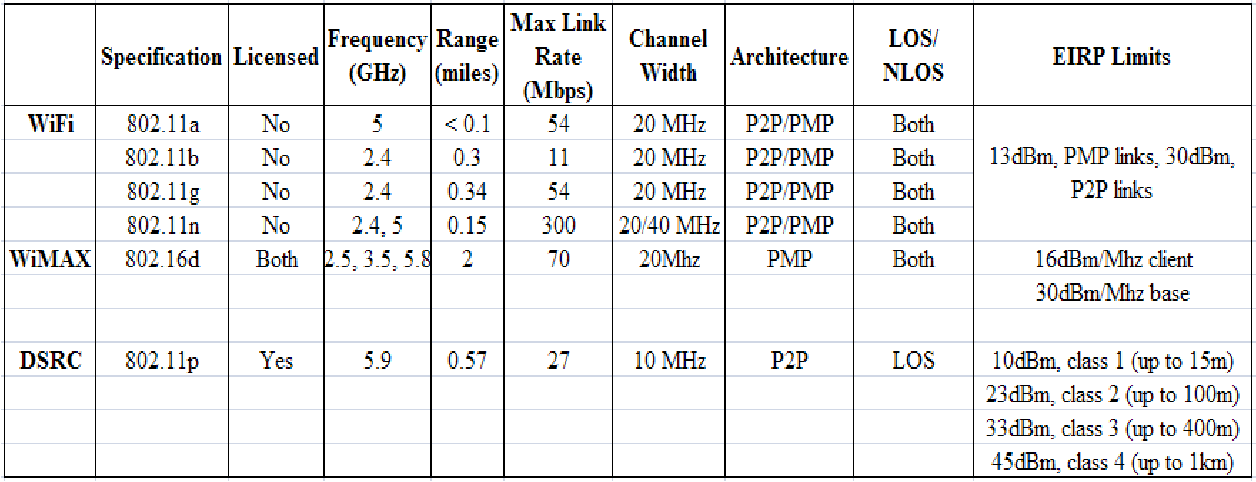
Table 12 Number of traffic monitoring devices in seven major cities in South Carolina

City	CCTV	Radar	DMS	Location
Columbia	52	37	2	I-26, I-77, I-20
Charleston	42	36	3	I-26, I-526
Greenville	14	0	0	I-85, I-185
Spartanburg	18	0	0	I-85
Myrtle Beach	20	4	0	US 501, US 17
Rock Hill	26	25	0	I-77
Gaffney	28	20	0	I-85

6.3 Technical specifications of the Wireless Technologies

As stated earlier, the two wireless technologies considered are Wi-Fi and WiMAX, and each can provide enough throughput to support most, if not all, of the current needs of an ITS network. However, they each have their own benefits and drawbacks that can be used to help guide network engineers during the planning stages. Each of the wireless technologies previously discussed carries certain technical specifications that determine the applications it can reasonably support. Table 13 was synthesized in [Zhou et al 2009] with columns containing pertinent information for a network engineer designing an ITS communications environment. To aid in comprehension of this information, an explanation regarding how each column affects ITS network design is shown.

Table 13 Technical Characteristic of Studied Wireless Technologies



	Specification	Licensed	Frequency (GHz)	Range (miles)	Max Link Rate (Mbps)	Channel Width	Architecture	LOS/ NLOS	EIRP Limits
WiFi	802.11a	No	5	< 0.1	54	20 MHz	P2P/PMP	Both	13dBm, PMP links, 30dBm, P2P links
	802.11b	No	2.4	0.3	11	20 MHz	P2P/PMP	Both	
	802.11g	No	2.4	0.34	54	20 MHz	P2P/PMP	Both	
	802.11n	No	2.4, 5	0.15	300	20/40 MHz	P2P/PMP	Both	
WiMAX	802.16d	Both	2.5, 3.5, 5.8	2	70	20Mhz	PMP	Both	16dBm/Mhz client
									30dBm/Mhz base
DSRC	802.11p	Yes	5.9	0.57	27	10 MHz	P2P	LOS	10dBm, class 1 (up to 15m)
									23dBm, class 2 (up to 100m)
									33dBm, class 3 (up to 400m)
									45dBm, class 4 (up to 1km)

- ***Specification*** – Each technology discussed is derived from an Institute of Electrical and Electronics Engineers (IEEE) standard. For a technological specification to become standardized, it must go through a rigorous process that includes numerous requests for comments (RFC) from industry and research leaders. Once a specification becomes a standard, it is released and various companies can design products that implement the standard. This is a key advantage over deploying a proprietary system because standards-based solutions allow for custom-off-the-shelf (COTS) equipment to be used; whereas custom designed equipment would be required for a proprietary solution. In this regard it is advisable to deploy a standards-based solution in an ITS environment.

- ***Licensed*** – The frequency that is used during transmission can be either licensed, by the Federal Communications Commission (FCC), or unlicensed. The unlicensed spectrum, where the various 802.11-based specifications reside, has been opened to all users for numerous technologies; and can be crowded. Because of this overcrowding, there is always the concern that signal quality on the wireless link can be degraded because of interference. The FCC has imposed limitations on the maximum allowable transmit power in an effort to reduce this interference. The unlicensed band is relatively small compared to the amount of licensed frequency space; and numerous technologies, including both WiMAX and DSRC, use licensed frequencies.

  In an ITS setting, it is important to weigh the cost of obtaining licenses for licensed bands with the potential interference faced if using unlicensed frequencies. However, according to the survey results, most of states are currently using non-licensed bands due to the cost of licensed implementation.

- ***Frequency*** – Wireless technologies transmit their data throughout a range of frequencies specified by the FCC. The frequency shown is the center frequency of the band for the technology. The frequency band utilized by the technology plays a major role in determining both the range and penetration of the wireless signal. As a rule of thumb, the lower the transmitting frequency, the better the signal will perform in terms of foliage and wall penetration. In addition, the range of transmitted signals will increase as the transmitting frequency decreases. The frequencies currently used by states that responded to the survey include 200MHz, 700MHz and 900MHz.

- ***Range*** – The range shown is the maximum obtainable range for the wireless technology; however, that range is not necessarily the obtainable range at the maximum link rate. The ranges quoted in Table 13 were calculated using non-specialized omni-directional antennas. It is also important to keep in mind that the range of a wireless access point can be increased by altering the antenna. In an ITS environment, this means that the coverage can be greatly tailored to suit the architectural needs by adjusting both the type of and gain on the antenna.

- ***Link Rate*** – Each wireless technology is capable of transmitting a certain amount of information in bits per second, accounting for both control overheads and user data. Each technology supports multiple link rates, while the achievable rate at any time and location is determined by many factors, such as the signal strength and interference present in the environment.

- ***Throughput*** – Throughput is the actual amount of user-generated data that can be transmitted per second. The value is often considerably less than the link rate due to the transmission and network protocol overheads, interference and noise, and contention with other radios.

- ***Architecture*** – Wireless radios can be interconnected and relay information following different topologies and routes. Referred to as their choice of architecture, our study considers three such architectures that are possible for ITS deployments:

    - *Point-to-point (P2P)* – This architecture involves a single wireless link between two radios and is often used for data backhaul or transmitting over long distances (when used in conjunction with a directional antenna). A typical P2P network deployment is shown in Figure 31.

Figure 32 A typical P2P architecture link

- *Point-to-multipoint (PMP)* – This architecture involves multiple point-to-point wireless links with one access point kept in common among the links. Commonly referred to as the infrastructure model, it mirrors the architecture of a cellular infrastructure network. The PMP architecture is used when multiple nodes connect to a single access point. A typical PMP network deployment is shown in Figure 32.

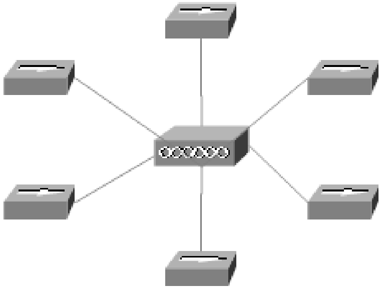


Figure 33 A typical PMP architecture link

- *Mesh* – A mesh network allows any node in the network to transmit to any other node. Both Wi-Fi and WiMAX networks can be operated in a mesh configuration. A primary benefit of mesh networking is that it provides redundant, reconfigurable paths between nodes, allowing the network to reroute traffic to maintain network robustness if any nodes were to fail. Mesh networks can be deployed to provide a larger area of coverage than would typically be possible with PMP architecture. A typical mesh network deployment is shown in Figure 33

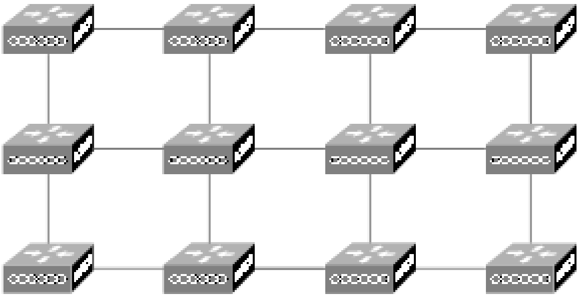


Figure 34 A typical mesh architecture link

- ***Line-of-sight (LOS) Requirements*** – A clear LOS between two communicating radios enhances the signal strength and, thus, the achievable link rate and throughput. Certain technologies, such as DSRC, recommend LOS operation in their standards; nevertheless, they usually can still operate under obstructed, i.e., non-LOS (NLOS) conditions. It is important to note as a rule of thumb that lower frequencies generally penetrate walls and foliage better and are more tolerant to NLOS operation.

- ***Effective isotropically radiated power (EIRP)*** is a measurement utilized by the FCC to quantify the power level transmitted by a radio given different antenna gains and supplied transmitter power. The FCC has set up EIRP guidelines to limit the amount of interference in the unlicensed spectrum. The maximum EIRP is sanctioned by the FCC depending on the network architecture (P2P or PMP) and frequency range. Within the EIRP constraints, it is possible to adopt the proper architecture, transmission power, and antenna gain to obtain a custom area of coverage.
- ***Range vs. Link Rate*** – The achieved link rate of a wireless connection is directly related to the signal strength received at the receiver. Thus, the distance between the sender and receiver has a primary effect on the link rate. For example, an 802.11g Wi-Fi radio can adapt according to the received signal strength to transmit at multiple distinct link rates between 6 Mbps and 54 Mbps. As an example, Figure 34 is generated using measured range and throughput data (Cisco 2009).

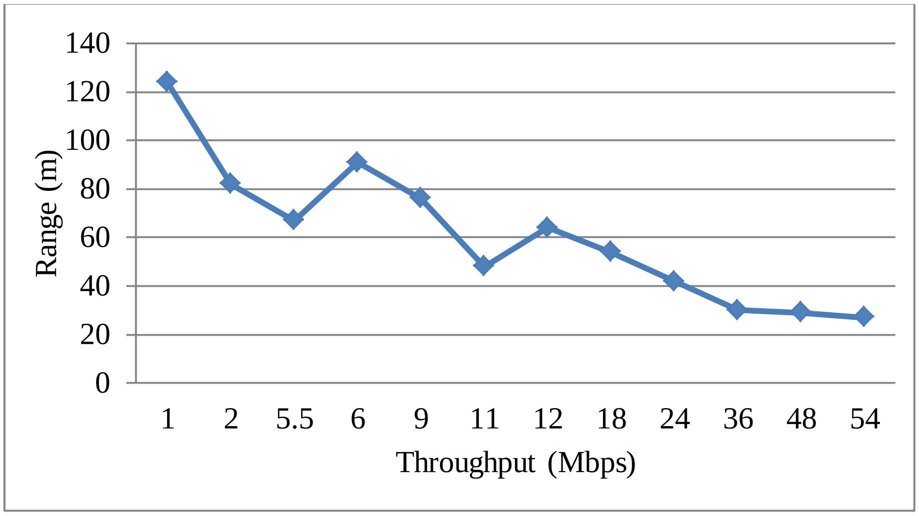


Figure 35: Range vs. Throughput for IEEE 802.11g (Cisco 2009)

***Mesh vs. Infrastructure* –**

Two network architectures (topology) are considered in the following case study for each wireless technology (Wi-Fi and WiMAX), the mesh network architecture and the infrastructure, or PMP, model. Both WiMAX and Wi-Fi support mesh mode, allowing data to be passed through various nodes in route to the Internet access point, instead of requiring each node to have its own Internet connection. In an infrastructure model, each access point would have a connection to the Internet, requiring more fiber optic connections.

There are advantages and disadvantages to deploying each of the wireless architectures; the two major factors that are considered in this case study are price and reliability. In terms of cost, a mesh solution will be superior to an infrastructure deployment, simply because the number of fiber optic Internet connections required in a mesh deployment is considerably lower. However, in terms of reliability the infrastructure model is expected to perform better because each of the node clusters has its own connection and there is no forwarded traffic. In an infrastructure model, if an access point were to fail only the nodes that directly connect to that access point would be lost. This is drastically different than a mesh network, where if a node were to fail it could cause a large number of other nodes to fail that was previously forwarding traffic through the failed node. On the other hand, a mesh network has the advantage of easily achieved redundancy in network topology for avoiding such single point of failures.

For the purposes of throughput requirement calculations, the following specifications have been determined for each camera. The traffic cameras are expected to produce a motion JPEG (MJPEG) stream with various frame rates and sizes, see Table 13 for exact requirements. These are experimentally calculated figures, and should provide a rough tool that can be used for future design purposes.

Table 14 MJPEG video bandwidth requirements for various sizes and frame rates

Quality	Resolution	Frame Rate (Fps)	Required Bandwidth (Mbps)
High	640*480	1	0.571
High	640*480	5	2.853
Medium	480*360	1	0.357
Medium	480*360	5	1.784
Low	320*240	1	0.220
Low	320*240	5	1.100

For the Wi-Fi cases, the access point deployed will be based on parameters of Cisco 1410 [Zhou et al 2009], with an estimated range of 865 feet at 54 Mbps and a range of 3465 feet at 11 Mbps when using an omni-directional antenna. For the WiMAX test cases an M/A-Com base station [Zhou et al 2009] is expected to produce a line-of-sight range of approximately 2.5 miles with an omni-directional antenna.

6.4 Columbia Traffic Surveillance System

The traffic surveillance system in Columbia, SC consists of 52 traffic cameras, 37 Radar detectors and 2 dynamic message signs to be wirelessly connected. All these devices are located on I-20, I-26 and I-77, shown in the Figure 35.

The distance between each node is calculated to form sub-networks (also called clusters) that each device is within radio range and also to minimize the numbers of fiber optic connections.

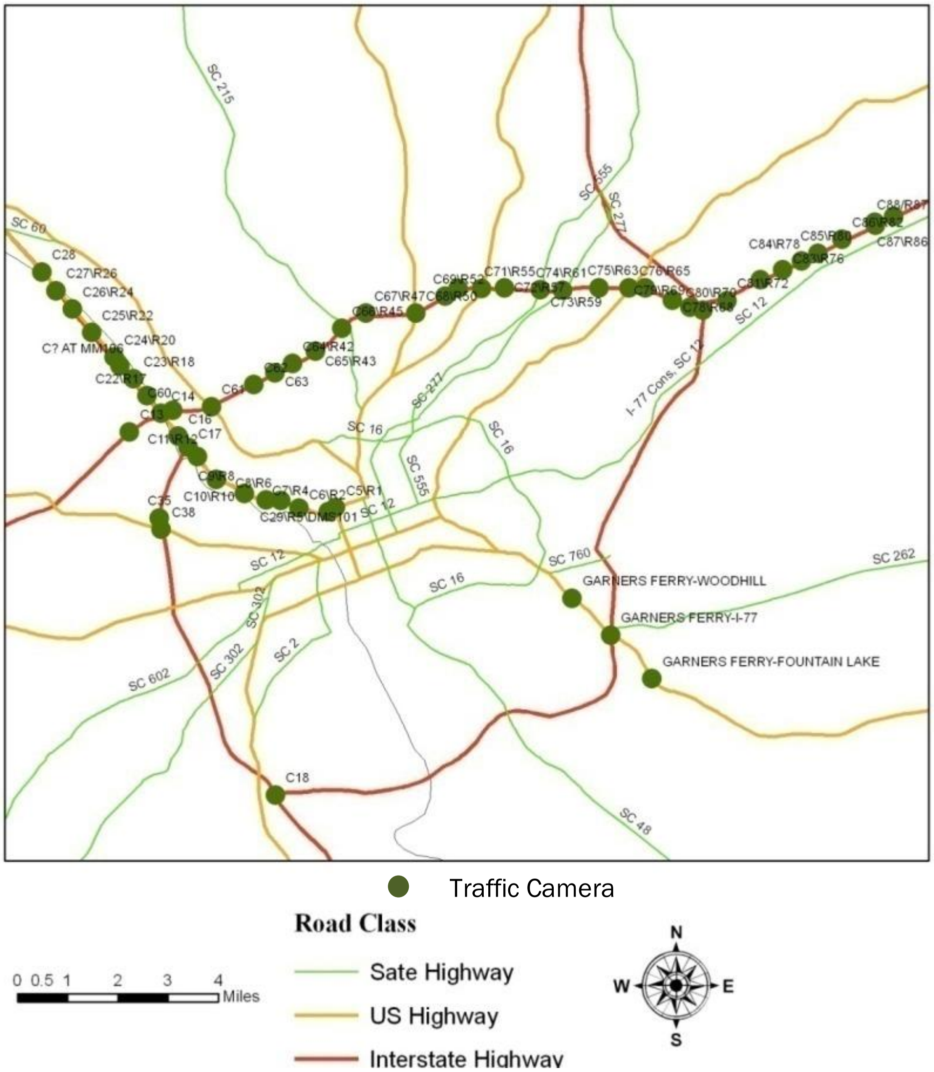


Figure 36 Traffic Surveillance Devices in Columbia, South Carolina

There are a total of four network deployments considered in this case study. There is both a Wi-Fi and a WiMAX solution for each of the two deployment architectures, mesh and infrastructure. Below we discuss the network model for each deployment, show the expected coverage area on the map, and discuss the benefits and concerns for the model. It should be noted that in Figures 35-39, the stars signify that they are connected to a fiber optic Internet connection.

6.4.1 WiMAX Infrastructure Models

First, based on the real performance of the WiMAX base station, the researchers assume that each base station can support up to 10 devices, which include 5 traffic cameras and 5 radar detectors. The bandwidth requirement of each camera is assumed as about 1.7 Mbps (medium level), while the radar detector is assumed to consume about 0.6 Mbps bandwidth. The DMS requires negligible bandwidth. In this model, all these devices were grouped into 13 sub-networks, each containing at a maximum five nodes within 2 miles, shown in Figure 36.

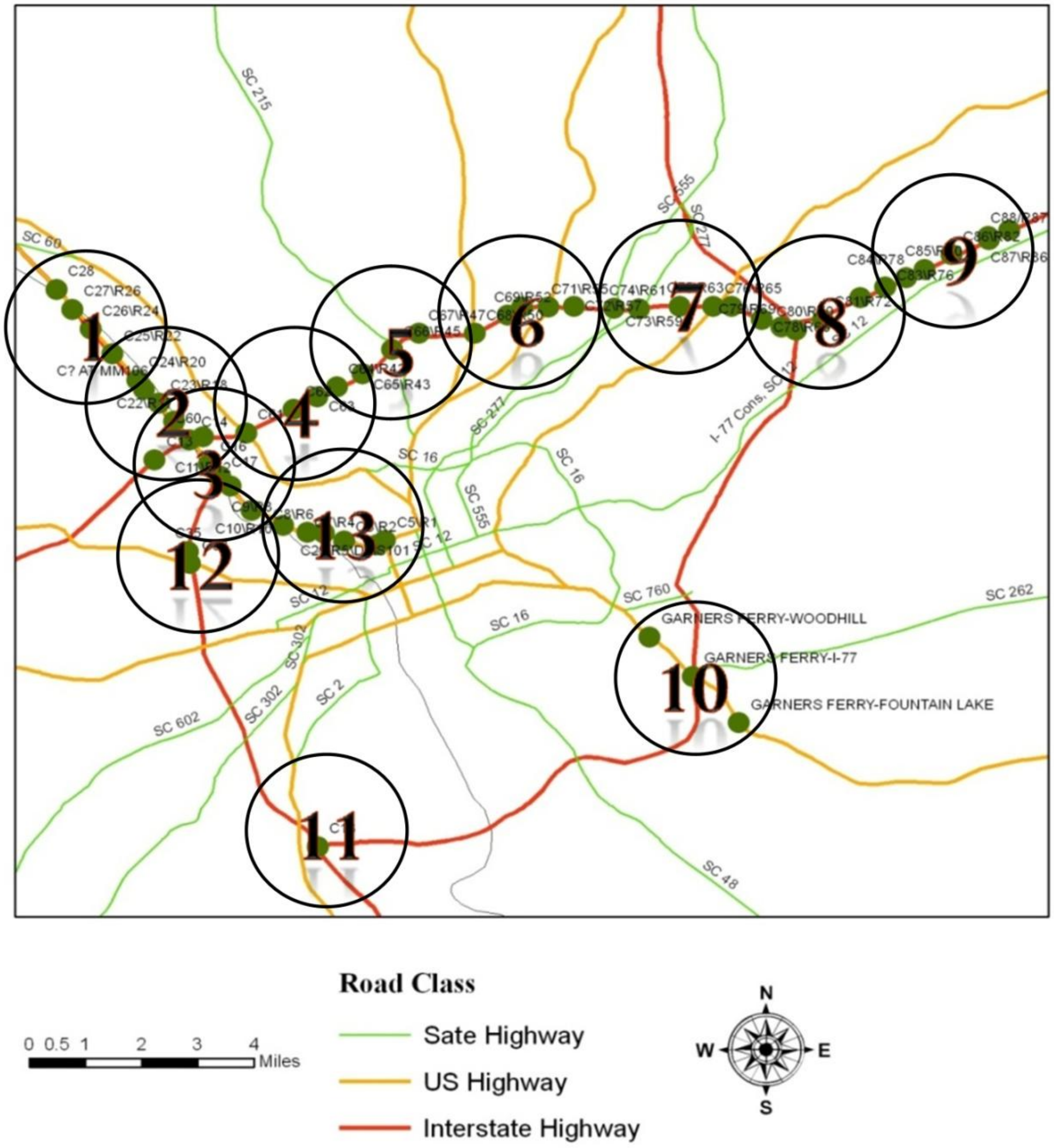


Figure 37 WiMAX infrastructure model of Columbia site

As seen in the Figure 36, the WiMAX infrastructure model includes 13 clusters, with overlapping coverage areas between each. Each cluster would have its own Internet access, via a fiber optic connection, which would provide a high level of bandwidth to each cluster. This architecture is the traditional method of deploying WiMAX equipment to provide wireless coverage to an area.

In this scenario, there would be a total of *13 fiber optic Internet connections* required, and *fifty-two WiMAX radios*. However, in this architecture towers need to be built first to support the WiMAX base stations, where each cluster connects to the internet via a fiber optic connection.

Although this implementation would provide a large coverage area that could be leveraged to provide connectivity to other ITS equipments, due to the construction and implementation costs of the towers, it would provide the highest-cost solution to wirelessly enabling the traffic surveillance cameras. To decide which node to locate the base station which provides the fiber optic internet connection for each cluster, the distance between the each node is calculated, and the base station is suggested to be co-located with the camera which has the minimum average distance to other nodes.

As an example developed in [Zhou et al 2009], Table 15 illustrates how the base station location for group one in Columbia site is selected. As shown in the table, each entry shows one camera/radar location, and C26\R24 (CCTV 26 and Radar detector 24), has the minimum maximum distance and average distance to other nodes, it is chose to be the fiber optic connection for group one, shown as a blue star in Figure 37. The two rows (C24\R20 and CAT MM106) highlighted in black are located on the boundary of the coverage range of this cluster. They were covered by another cluster to ensure the connection, so they were not included in the selection in this cluster. The internet connections of other group were decided using a similar process. Group 11 is a satellite node, which is remote from other grouping and requires its own fiber connection. The authors use the term “Satellite node” describe a node (traffic camera) that is far from the other clusters, but could reach one cluster by the use of a directional antenna.

Table 15 Traffic monitoring devices of Columbia network: group one

Group 1	**C27\R26**	**C25\R22**	**C24\R20**	**C28**	**C26\R24**	**CAT MM106**
C27\R26	0.0000	1.0925	1.7569	0.4733	0.4880	1.9651
C25\R22	1.0925	0.0000	0.6646	1.5655	0.6046	0.8725
C24\R20	1.7569	0.6646	0.0000	2.2296	1.2689	0.2092
C28	0.4733	1.5655	2.2296	0.0000	0.9609	2.4380
C26\R24	0.4880	0.6046	1.2689	0.9609	0.0000	1.4771
C AT MM106	1.9651	0.8725	0.2092	2.4380	1.4771	0.0000
Max. Dist.	*1.0925*	*1.5655*	*2.2296*	*1.5655*	*0.9609*	*2.4380*
Avg. Dist.	*0.5135*	*0.8157*	*1.4800*	*0.7499*	*0.5134*	*1.6882*

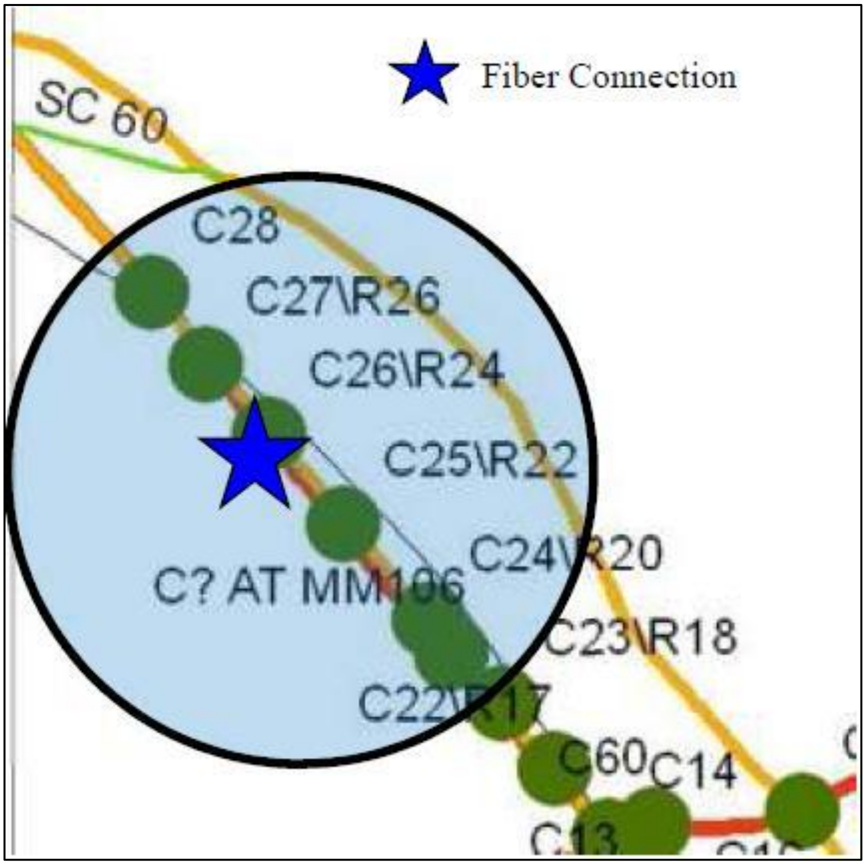


Figure 38 Fiber Optic Connection of Group One of Columbia Network

6.4.2 Wi-Fi Infrastructure Network

The Wi-Fi infrastructure model shown in Figure 38 divides the fifty-two nodes into *twenty-eight clusters*. Some groups have three nodes, while others have two or only one. Each cluster would have its own Internet access, via a fiber optic connection, which would provide a high level of bandwidth to each cluster.

In this scenario, there would be a total of *28 fiber optic Internet connections required*, and *52 Cisco 1410 access points*. This would provide a medium-cost solution to wirelessly enabling the traffic surveillance cameras, because each fiber optic connection can be both expensive and possibly create a recurring cost. A key benefit of this architecture is that it provides considerable expandability. The, maximum of three, traffic surveillance cameras would take up very little of the total bandwidth so additional ITS equipment could be connected to the access points.

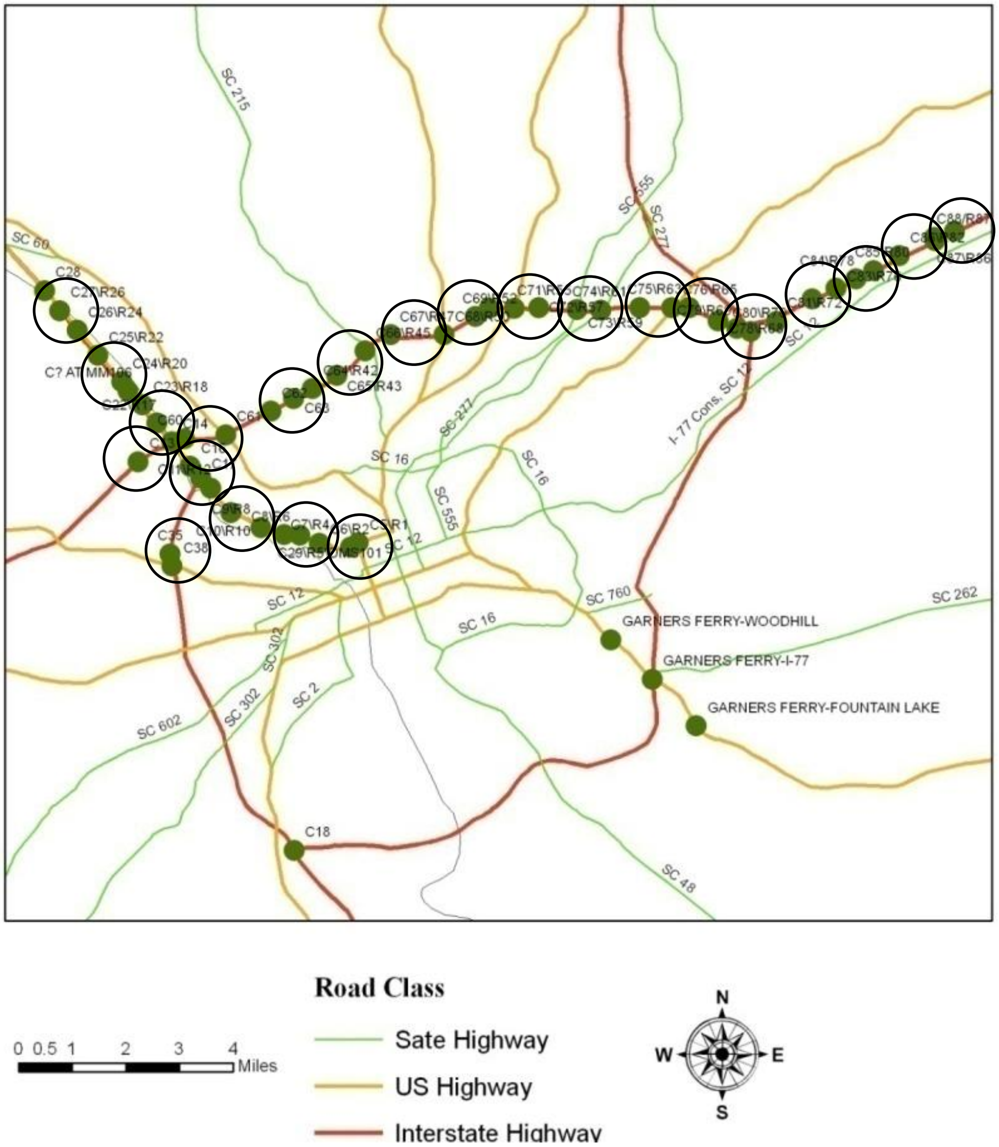


Figure 39 Wi-Fi Infrastructure Model of Columbia Site

6.4.3 Wi-Fi Mesh Network

The Wi-Fi mesh model is shown in Figure 39, and divides the twenty-eight clusters into *four mesh clusters*, one supporting a group of fifteen clusters, another connecting group of nine, third of four and a final cluster to support one satellite node. The reason is the distance between the satellite node and other mesh clusters is farther than distance the standard Cisco access point can reach at a minimum of 11Mbps. This is a two–layer solution that contains the cluster and mesh cluster. There are two types of access point needed. One is for connecting cameras within the same cluster, which covers approximately 2 miles. The other one is for the connecting all cluster-gateways to the wired access point that has a fiber connection.

A directional antenna is used for wired primary access point which has a coverage range of approximately 10 miles. However, the distance between cluster 11 and cluster 10 is too far, which is over 5 miles, so the cluster 11 would be better served having a separated fiber access instead connected to the access in the cluster 10 to avoid significant communication traffic delay. Moreover, there is a high-gain directional antenna connected to the satellite node that allows it to forward its data to the rest of the wireless mesh cluster.

Satellite node is a term used to describe the node (traffic camera) that is far from the other clusters, but could reach the cluster by the use of a directional antenna. For this case study the access point locations with Internet access were chosen to minimize this maximum hop-count. The mesh cluster with the fifteen clusters has a maximum hop-count of five, which is the highest hop-count for the network.

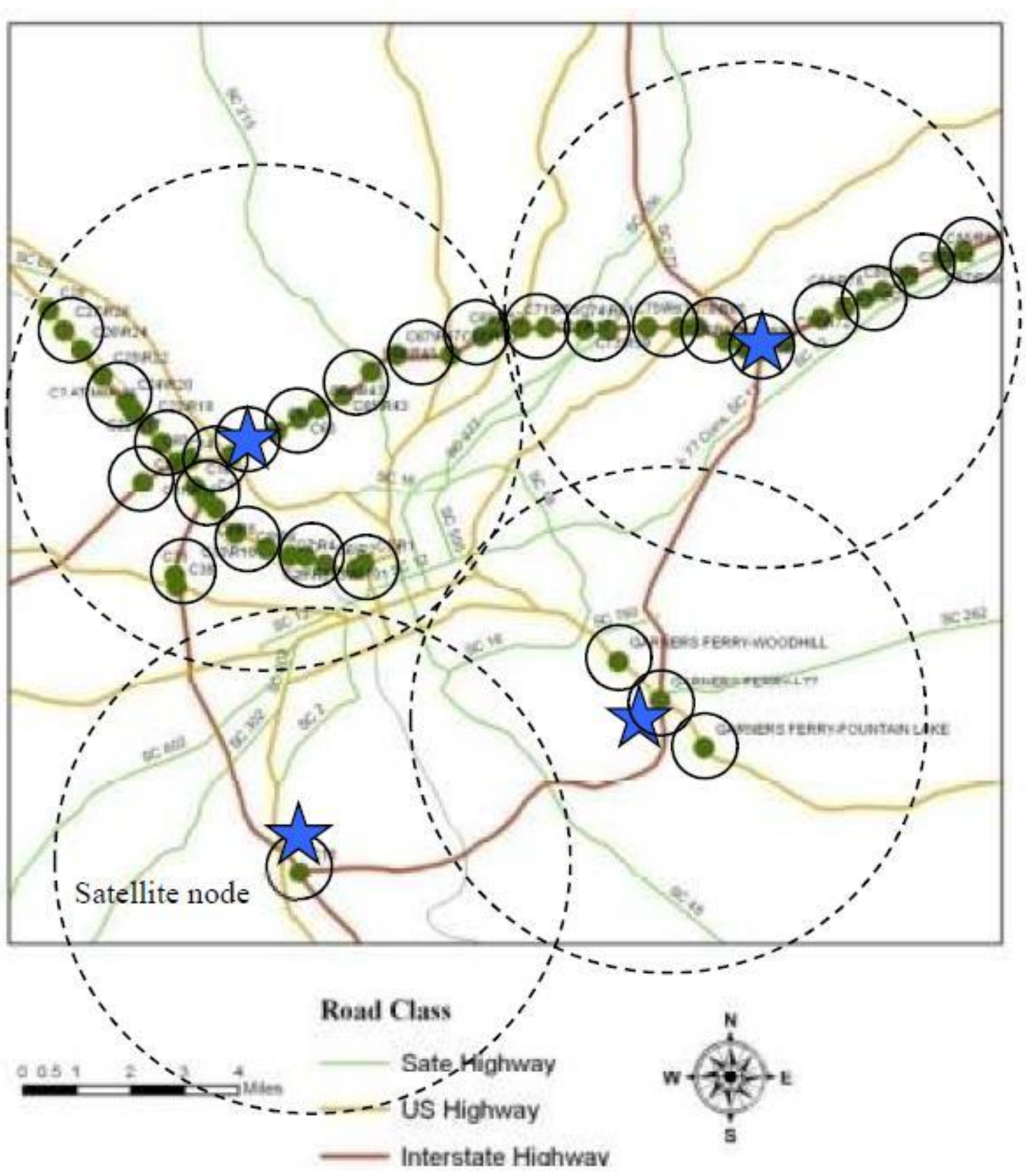


Figure 40 Wi-Fi Mesh Network Model for Columbia, SC

In this scenario, there would be a total of *four fiber optic Internet connections* required, and *fifty two Cisco 1410 access points*. This would provide a relatively low-cost solution to wirelessly enabling the traffic surveillance cameras; however, this solution does not allow for much expandability, as most of the throughput the network could support is already taken.

6.4.4 WiMAX Mesh Network

The WiMAX mesh model shown in Figure 40 divides the twenty-eight clusters in the same manner as the Wi-Fi mesh model; with into *four mesh clusters*. Each node would have its own Motorola WiMAX base station, with each node in the two clusters forwarding data from the other nodes. For this case study the access point locations with Internet access were chosen to minimize this maximum hop-count. In this network there are three nodes that are a *hop-count of four* from the Internet access location. For instance, Figure 41 demonstrates the data transmission flow with one mesh cluster which contains cluster 6, 7, 8 and 9.

In this scenario, there would be a total of three fiber optic Internet connections required, and fifty-two Motorola WiMAX base stations. This is a relatively expensive solution to wirelessly enable the traffic surveillance cameras, and has the same expandability concerns as the Wi-Fi mesh network.

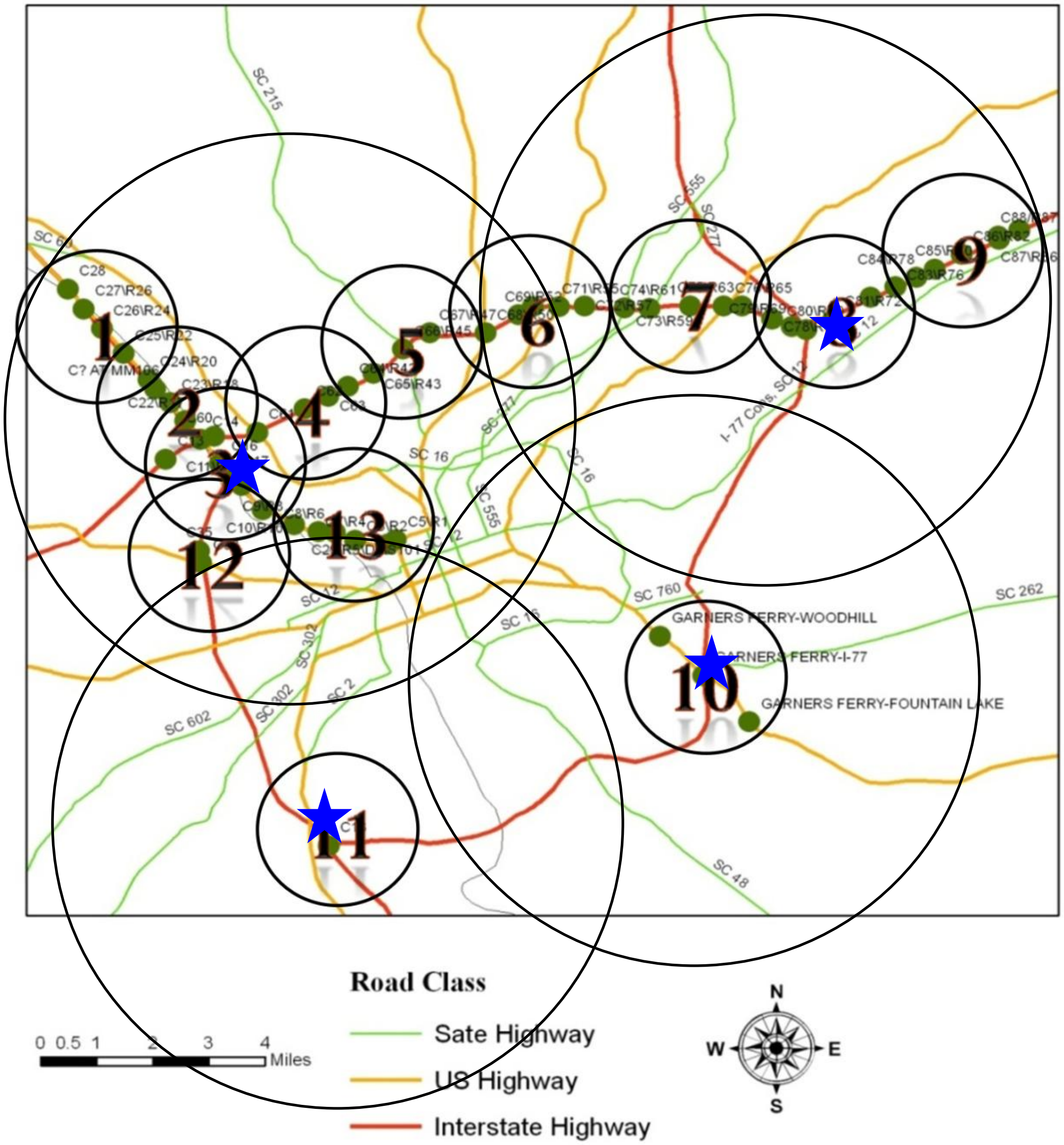


Figure 41 WiMAX Mesh Network Model for Columbia, SC

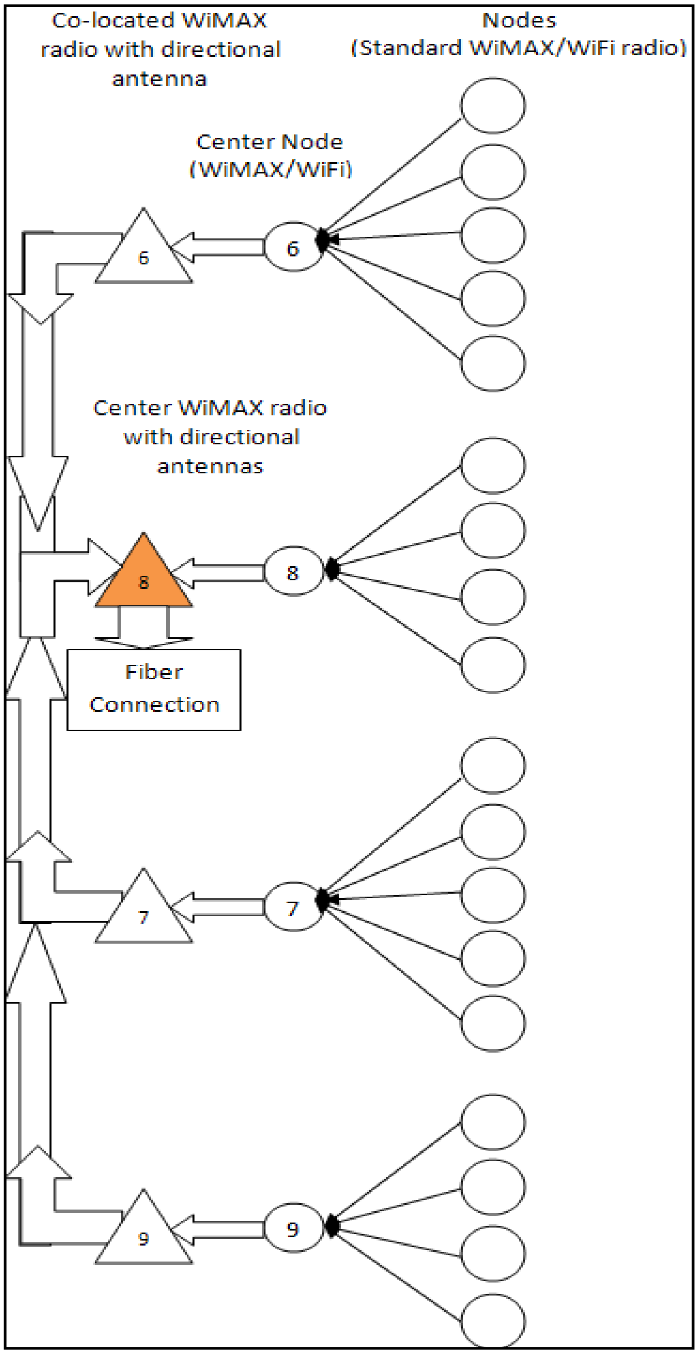


Figure 42 Data transmission within one mesh cluster

6.5 Greenville Traffic Surveillance System

Compared to the Columbia metropolitan area, the Greenville network is much smaller. The section of traffic surveillance system in Greenville, SC consists of 14traffic cameras. No radar detectors or dynamic message signs were recorded in the data-base provided by SCDOT. There is a research interest to identify which network topology suits for different network considering the number of devices and coverage range. All the traffic monitoring cameras considered in Greenville are located on I-385, north of I-85, with a satellite camera located on I-85 approximately 2.5 miles north of the I-385 / I-85 intersection. In total, there are fourteen cameras requiring wireless connection in this case study. A map of these cameras is shown in Figure 42.

Figure 43 Traffic Surveillance Systems in Greenville, SC

For each location, a standard antenna is almost always an omni-directional antenna that comes pre-integrated into the router. The exact range is hard to define because it depends on a number of factors, including the network topology. The estimated range considered in this case study is approximately 2 to 3 miles. Distance between each node is calculated to form sub-networks (also called clusters) that each device is with radio range and also to minimize the numbers of fiber optic connections.

6.5.1 Wi-Fi Mesh Models

As discussed previously, a primary concern that was considered when designing either of these mesh networks is the maximum number of hops required to get from the farthest edge node to the Internet gateway. In a mesh network, each non-edge node is required to forward other node's traffic; therefore, the total amount of non-forwarded data that can be handled by the network is significantly lower than the total throughput.

The Wi-Fi mesh model is shown in Figure 43. A high-gain directional antenna is connected to the satellite node that allows the forwarding of data to the rest of the wireless mesh cluster. The satellite node, which is the node farthest from the other clusters (traffic camera #1), can reach the cluster through the use of a directional antenna. As shown in Table 14, the distance between the two mesh clusters, at a minimum of 11Mbps, is farther than the reach of the standard Cisco access point. For this case study, the access point locations with Internet access were chosen to minimize this hop-count. The mesh cluster with the satellite node has a *maximum hop-count of four*, which is the highest hop-count for the network.

In this scenario, two fiber optic Internet connections are required, and fourteen Cisco 1410 access points are required. Though this provides a relatively low-cost solution to wirelessly enabling the traffic surveillance cameras, it does not permit much expandability, as most of the available network throughput of the network is already utilized.

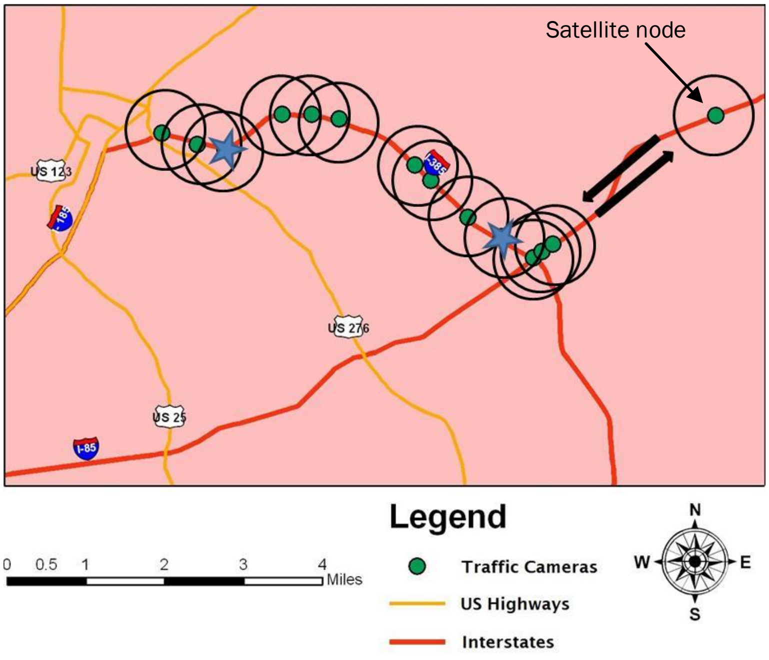


Figure 44 Wi-Fi Mesh Network Model for Greenville, SC

6.5.2 WiMAX Mesh Network

The WiMAX mesh model is shown in Figure 44. This configuration is identical to the Wi-Fi mesh model. Each node possesses its own Motorola WiMAX base station, with each node in the two clusters forwarding data from the other nodes. The access point locations with Internet access were chosen to minimize this maximum hop-count. Within this network there are three nodes requiring four hops to/from the Internet access location.

In this scenario, there are a total of *two fiber optic Internet connections* and *fourteen Motorola WiMAX base stations*. This is thus a relatively expensive solution to wirelessly enable the traffic surveillance cameras and has the same expandability drawbacks as the Wi-Fi mesh network.

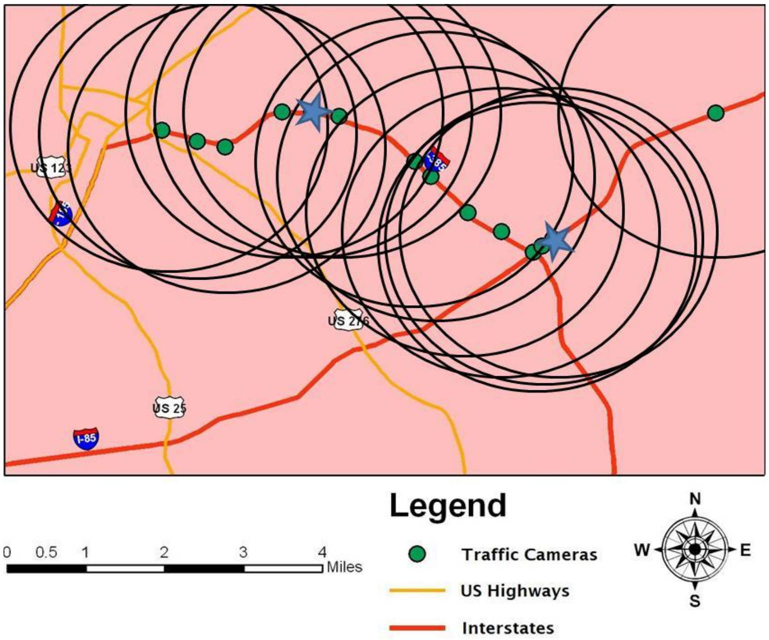


Figure 45 WiMAX mesh network model for Greenville, SC

6.5.3 Wi-Fi Infrastructure Models

The Wi-Fi infrastructure model, shown in Figure 45, divides the fourteen traffic surveillance cameras into *six clusters*: three groups of three, two groups of two, and one group of one. Each cluster has its own Internet access, via a fiber optic connection, which provides a high level of bandwidth to each cluster.

In this scenario, there are a total of *six fiber optic Internet connections* required, and fourteen Cisco 1410 access points. This configuration provides a medium-cost solution to wirelessly enabling the traffic surveillance cameras, as each fiber optic connection can be both expensive with possible recurring costs. However, this architecture is advantageous in that it provides considerable expandability. Because no more than three traffic surveillance cameras are linked to each access point, this configuration encompasses very little of the total bandwidth so additional ITS equipment could be connected to the access points.

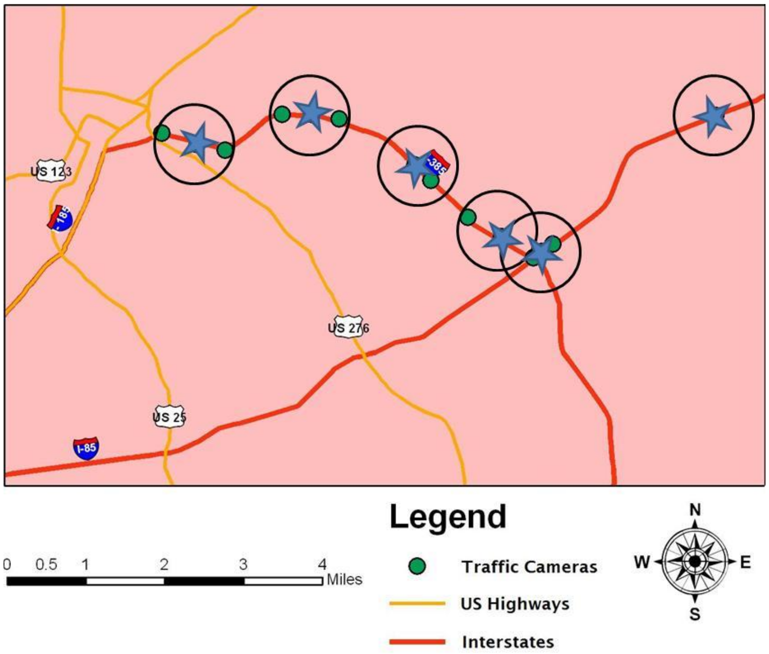


Figure 46 Wi-Fi infrastructure network model for Greenville, SC

6.5.4 WiMAX Infrastructure Models

The WiMAX infrastructure model, shown in Figure 46 divides the fourteen traffic surveillance cameras into *two clusters*, with overlapping coverage areas. Each cluster has its own Internet access, via a fiber optic connection, which provides a high level of bandwidth to each cluster. This architecture is the traditional method of deploying WiMAX equipment to provide wireless coverage to an area.

In this scenario, there are a total of *two fiber optic Internet* and *fourteen WiMAX radio connections* required. Although this configuration requires the highest construction cost to build WiMAX towers to support the wireless traffic surveillance system, it yields a large coverage area that can be leveraged to provide connectivity to other ITS equipment.

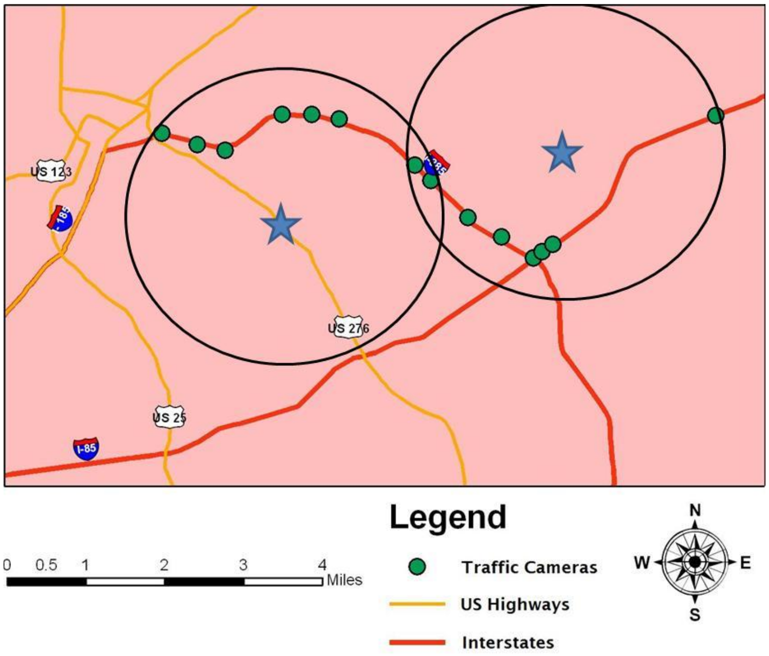


Figure 47 WiMAX Infrastructure Network Model for Greenville, SC

6.6 Summary of Case Study

1. Through these case studies, the authors demonstrated the network designing procedure for a large and small ITS network in metropolitan areas. Moreover, this section also showcased how the DOT could deploy Wi-Fi and WiMAX technologies to adequately cover the region and support the required surveillance performance.
2. It also allowed for the comparison between Wi-Fi and WiMAX architectures when dealing with a relatively sparse camera density. Table 16 represents a comparative summary of Columbia Network**.**

Table 16 Case Study summary for Columbia Network

Sr. No	Criteria	Wi-Fi Infrastructure	Wi-Fi Mesh	WiMAX Infrastructure	WiMAX Mesh
1	Number of Fiber Optic connections required	13	4	13	3
2	Number of Access points	52 Wi-Fi Access Points	52	52 WiMAX radios	52
3	Hop Count	NA	5	NA	4

Table 17 Case Study summary for Greenville Network

Sr. No	Criteria	Wi-Fi Infrastructure	Wi-Fi Mesh	WiMAX Infrastructure	WiMAX Mesh
1	Number of Fiber Optic connections required	6	2	2	2
2	Number of Access points	14 Wi-Fi Access Points	14	14 WiMAX radios	14
3	Hop Count	NA	4	NA	4

For more case studies refer to Appendix C

7 SIMULATION ANALYSIS

Computer simulation can be utilized for system level analysis of the wireless ITS network. Two strategies were employed in this context; a communication level analysis, and an integrated traffic and communication analysis.

The communication simulator ns-2 was used to model the Greenville traffic surveillance system. For the case of mesh topology, the authors studied the effect of environmental parameters on the multi-hop behavior of the system to evaluate its performance. Wi-Fi technology was tested in this simulation.

In the integrated simulation, ns-2 along with traffic simulator Paramics were used to study the performance of the system in case of an incident in terms of the detection rate, communication latency and false alarm rate. It was observed that sensor spacing of up to 0.5 miles for Wi-Fi provided desirable results for incident detection. It was also observed from the integrated simulation analysis that communication latency is a less significant performance measure for a wireless traffic sensor network.

7.1 Description

Through the field tests the authors quantified the effects of the different factors in a highway environment, such as modulation rate, inter-sensor distance and transmission power, which traffic agencies can use as a reference for future ITS applications. However evaluating the performance of a large scale traffic sensor network calls for an elaborate simulation study. This study will be helpful for performance-cost analysis presented in next section.

The authors use Wi-Fi as an example to conduct two types of simulation studies. The first one evaluates the communication reliability and performance of a traffic sensor network using communication simulator ns-2. The other simulation study simultaneously assesses both the traffic operation performance and communication performance of a wireless traffic sensor network. For this purpose, an integrated simulator platform was developed. The following section illustrates the methodology of ns-2 simulation; the integrated simulation used in this study, and then discusses the simulation site selection and evaluation scenarios in detail.

7.2 Ns-2 Simulation

Aim: To obtain a comprehensive quantitative assessment of the dependency of a wireless traffic sensor network on the communication errors and topology decisions.

To support online traffic management, wireless sensor networks have to collect and relay real-time traffic information from a wide area transportation network. However, limited research has been done to study the wireless communication performance and reliability for use in a traffic monitoring network. Potential environmental disturbances, such as adverse weather, foliage, and interference can induce transmission errors in the communication network. Real highway network and traffic camera density were modeled in the simulation for use in guiding future implementation. Figure 46 shows the methodology for analyzing the communication network performance with selected measures of effectiveness (MOEs). The MOEs for the communication system for ITS applications should be selected in terms of the proper Quality of Service (QoS) metrics with respect to the communication performance requirements of traffic cameras (Peterson and Davis, 2003). After selecting the important MOEs, the sensor locations, network topology and wireless link properties were determined. Specifically, a range of link error rates were selected based on an initial simulation analysis that depicted those rates after which performance no longer can support the video surveillance system studied in this research. The injected data rates were selected based on typical data streaming requirements in traffic surveillance system.

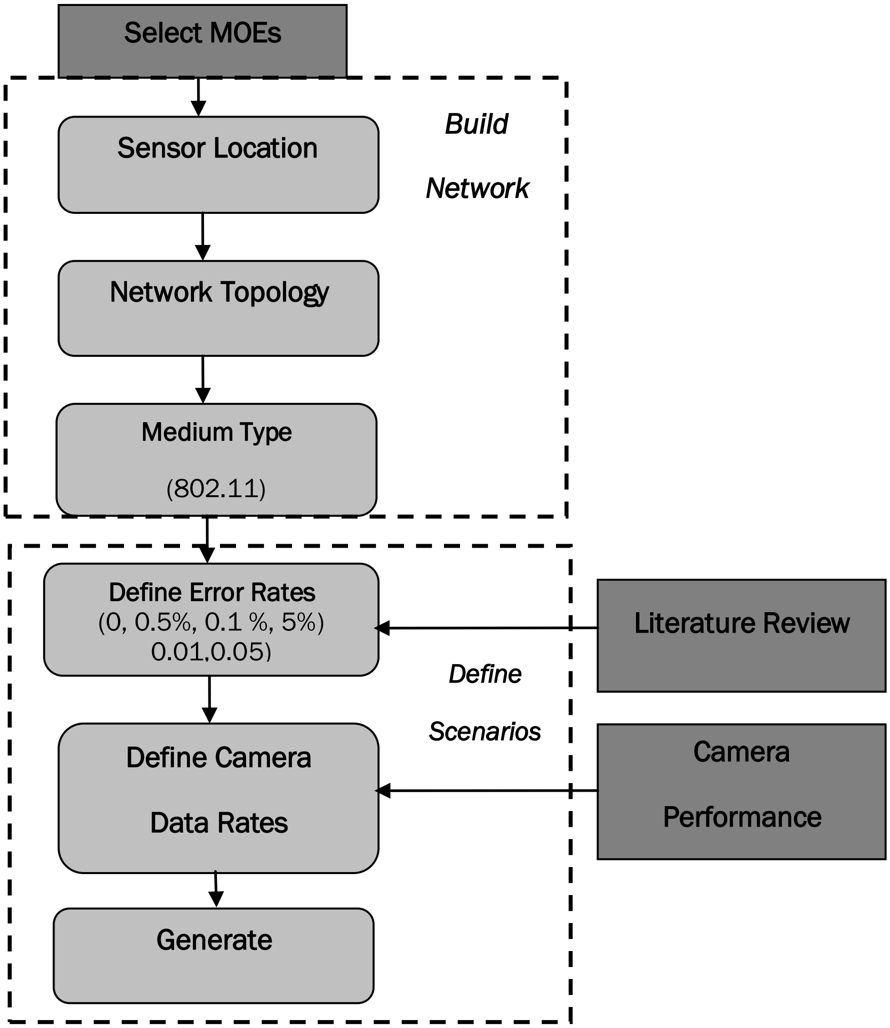


Figure 48 Ns-2 simulation methodology

A video surveillance camera requires higher bandwidth than other traffic devices such as highway advisory radio (HAR) and dynamic message signs (DMS). The traffic surveillance system studied in this research consists of traffic cameras (also referred to as sensors), wireless relays, local controllers, and a TMC. Because of the wireless transmission distance limitation, relays are necessary between cameras (sensors) to forward data from one sensor to a nearby camera (sensor) and eventually to a local controller, which forwards the data to the TMC using wired Internet connectivity.

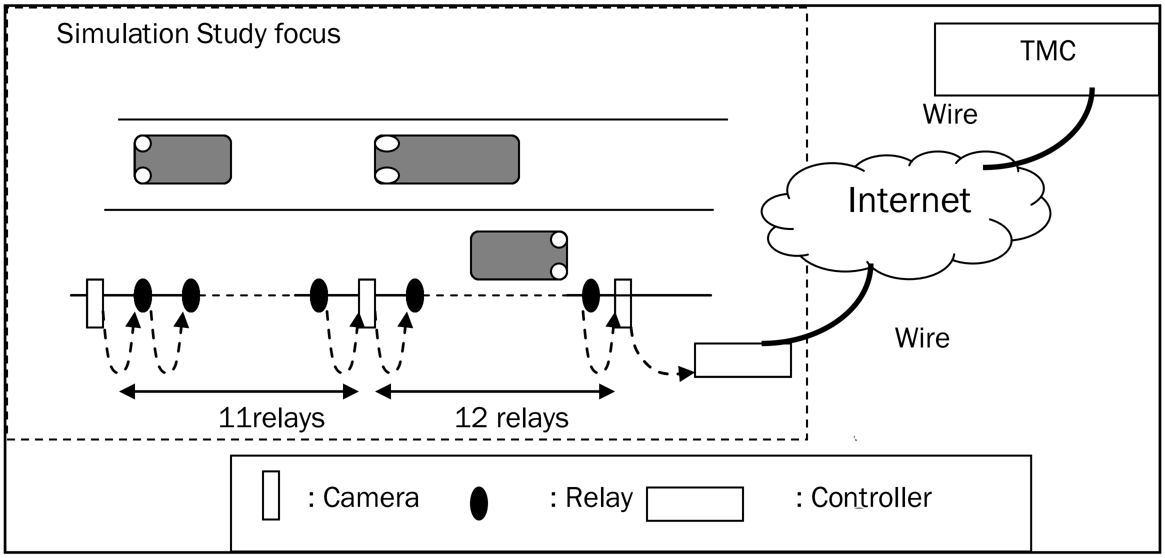


Figure 49 Ns-2 simulation network for on-line traffic management

7.2.1 MOE Selection

A communication system for on-line traffic management must transfer information from field components to the traffic operations center, which would then transmit responses and commands back to various field components (Gordon et al 2005). According to the respective components' functionalities, MOEs for the communication system can include its bandwidth and data rate.

Timely traffic monitoring and effective response operations rely on reliable traffic information. The wireless network performance is affected by many factors, such as adverse weather conditions, network load and terrain conditions, which might introduce communication errors within the network. One important property of a wireless network is that, despite the potential errors, the network can operate at a fraction of its full performance level as long as the devices are operational. Thus, the selected MOEs must be able to illustrate, for a continuous range of operating conditions, how and at what level these conditions can affect communication link capacity and reliability. In ns-2 simulation, the transmission errors under adverse conditions are modeled.

Similar to the field test, ns-2 simulation selected two MOEs related to communication reliability for on-line traffic management requirements, the *saturated throughput* and the *successful delivery ratio*.

Delay was not selected as a MOE because generally the magnitude of communication latency is relatively small compared to the time scale of traffic management. Given adequate capacity of support communication links, the impacts of communication delay on the operational effectiveness and efficiency of a traffic surveillance system are negligible. Using the selected two metrics, this simulation study would be able to systematically analyze the communication performance under different scenarios with varying error rates.

7.2.2 Simulation Setup

Communication network simulator ns-2 was used to model the behavior of a large-scale traffic surveillance network system. Network protocols are modeled with individual source files in C++ and TCL languages. User-defined functions can be inserted at any protocol layer with plug-in C++ source files.

The simulation first started with defining sensor locations. The authors simulated a 3-mile highway section with roadside traffic cameras wireless connected and communicated one by one. In this simulation, cameras were deployed in one mile distance with relays deployed in between. Each relay was located 650 ft (200m) from its neighboring peer, and the maximum communication range was configured as 250m in ns-2. As shown in Figure 48, there were a total of 25 relays, 3 sensors and one local controller in the simulated network.

The study assumed that traffic surveillance operating agencies will utilize IEEE 802.11b protocol with a bandwidth of 11MHz for communication among sensors and controllers in the field. Traffic surveillance data is generated at constant bit rate and sent across the network in User Datagram Protocol (UDP) flows due to its lower network overheads and latency. For time-critical applications such as video traffic surveillance, UDP is considered to be a more appropriate option for data transmission (Peterson and Davis, 2003).

Different error rates can be configured for each communication link in ns-2 to simulate link performance under various adverse conditions. While an accurate error model for weather conditions is not available, the authors choose a range of different link error rates to identify the trend of their performance impacts. Four different scenarios were selected based on the error rates, which are 0% error rate (ideal condition), 0.5% error rate, 1% error rate and 5% error rate. The researchers did not simulate error rates higher than 5% because the respective communication performance could no longer support effective and reliable traffic surveillance (assuming video-based surveillance). The system capacity and data delivery ratio were examined under four chosen adverse conditions. The network was simulated with increasing the data load until the network was saturated. First 50 seconds out of entire 300 seconds simulation was designated as warm-up period and not used for analysis. It was assumed that the random packet errors and the resulting communication throughput followed a normal distribution. The experiments were repeated in 10-run increments until the 95% confidence interval of the respective MOE were within 5% of its estimated mean (Bartin et al., 2006; Ozbay et al., 2004; Law and Kelton, 2000).

7.2.3 Ns-2 Simulation Analysis

The following sections presents ns-2 simulation analysis related to communication performance of wireless traffic sensor networks (1) under two network topologies, and (2) different adverse environmental conditions.

- **Effect of the number of relays on the saturation throughput:**
  IEEE 802.11 has a randomized and shared medium access scheme implying that as the number of relays increases, so does the chances of collision among nearby wireless links (i.e. more colliding transmissions and retransmissions). Since packets sent from the camera farthest must traverse more links to reach the controller, it has the most chances of collision and least expected throughput.
  As Figure 48 shows, with 23 relays with 2 cameras (25 traffic components), the farthest camera reached saturated throughput at 256 Kbps and began to drop more at higher rates; rendering 256 Kbps as the throughput that can be reliably supported if all cameras operate at the same standard rate. For this scenario the communication error per link was considered as 0.5%.

- **Effect of adverse conditions on throughput and delivery ratio:**

  Environmental effects and noise severely affect successful transmission on a wireless network. The performance of the farthest camera was evaluated in this simulation. Figure 49 and Figure 50 show the saturated throughput and packet delivery ratio with different wireless link packet error rates.

  Interestingly, the 0.5%, 1%, 5% error rates caused the saturation throughput to drop by 80 Kbps, 100 Kbps, and 230 Kbps respectively as compared to the ideal condition. This finding suggests that the network performance is sensitive to error rates when they are small. The saturated throughput can drop about 25% even with 0.5% error rate per link. However, the network is robust in the range of 0.5% to 1% error rates; the throughput did not drop by half when the error rate doubled. These quantitative measures of throughput degradation are essential for bandwidth planning of a wireless roadway traffic surveillance network designed for on-line traffic management. When the error rate is 1%, the farthest camera's saturating throughput was 200Kbps, sufficient to support a full motion video transmission (Gordon et al. 1993). However, the delivery ratio at this point is just above 80%, meaning that about 20% of the packets were lost due to transmission errors.

  The throughput trends beyond saturation throughput are less important. With a 5% error rate, the saturating throughput dropped below 64 Kbps; since the typical traffic camera rate ranges from 64 Kbps to 384Kbps (Gordon et al. 1993), the system will not support all cameras when any adverse condition causes more than 5% communication link error rate. This fact suggests that even for existing traffic cameras requiring very low data rates, traffic agencies must keep the error rates of the communication link within a certain threshold to ensure that every camera in the system is working properly.

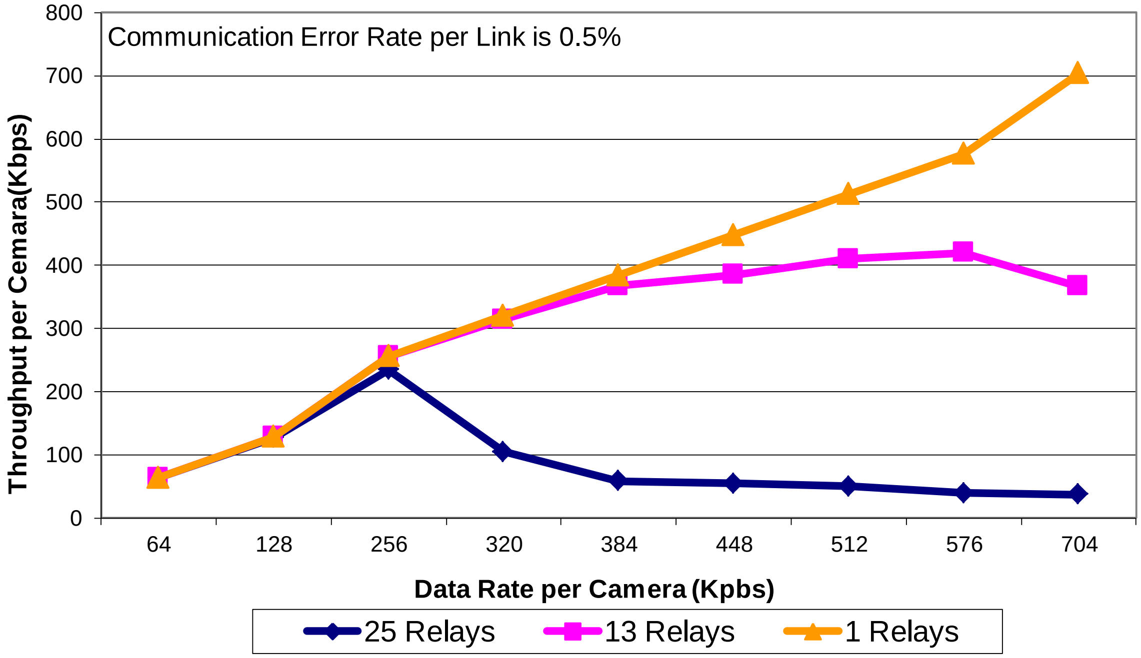


Figure 50 Farthest camera throughput with different number of relays

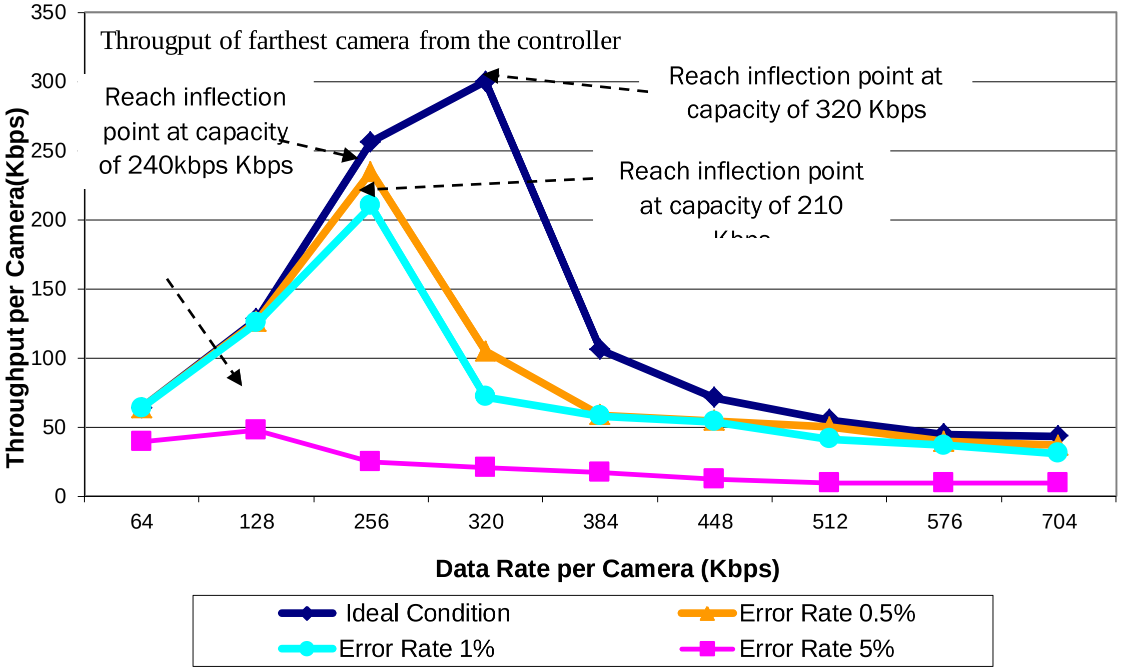


Figure 51 Farthest camera throughput at different error rates

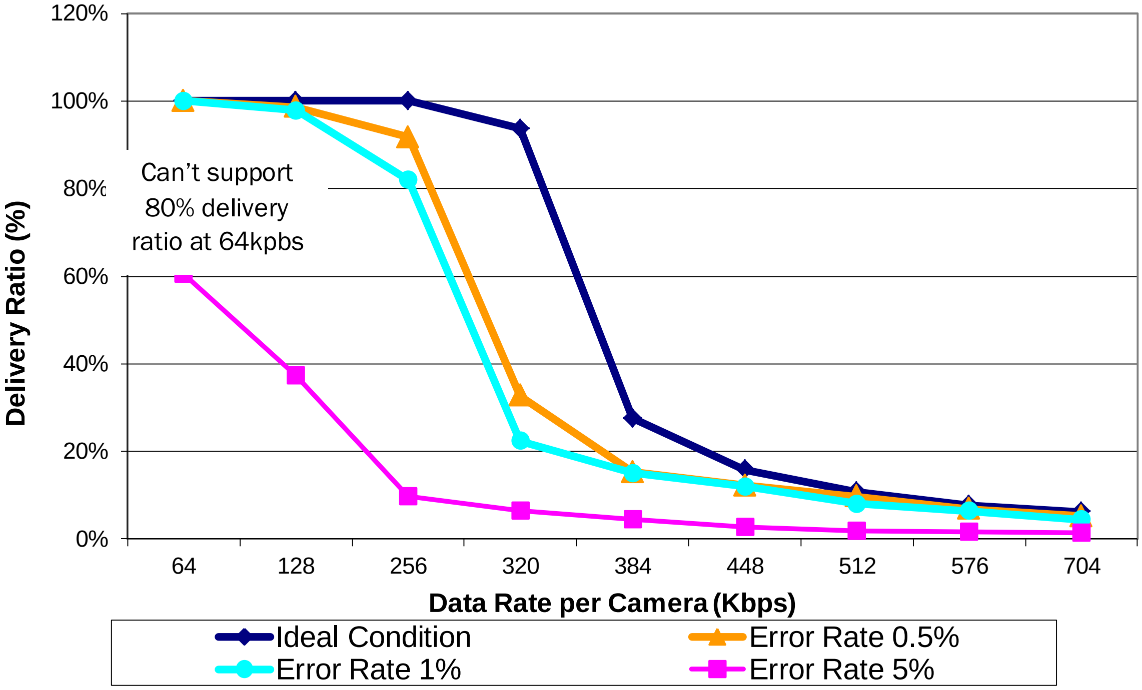


Figure 52 Farthest camera delivery ratio at different error rates

- **Effect of environmental phenomenon in collision free transmission:**
  In the case where only one camera was deployed, its saturated throughput was measured with different error rates and number of relays, as shown in Figure 52. When only one camera is connected to the controller, the network performance is more tolerant to the use of more relays. This is mainly because the errors due to collisions are totally avoided. The throughput decreased with increasing relays but only minor differences with different error rates.

  With a 1% communication error rate, the network can support a saturating throughput of 928 Kbps when the camera is 5 relays, or hops (3280 ft) away from the controller. The throughput decreased to 484Kbps when the camera is 25 relays (16400 ft) away. Moreover, the throughput decreased more rapidly when the number of relays increased from 5 to 15 than from 15 to 25.

  In general, a trade-off analysis is necessary for making investment decisions for additional communication infrastructures to meet specific performance requirements.

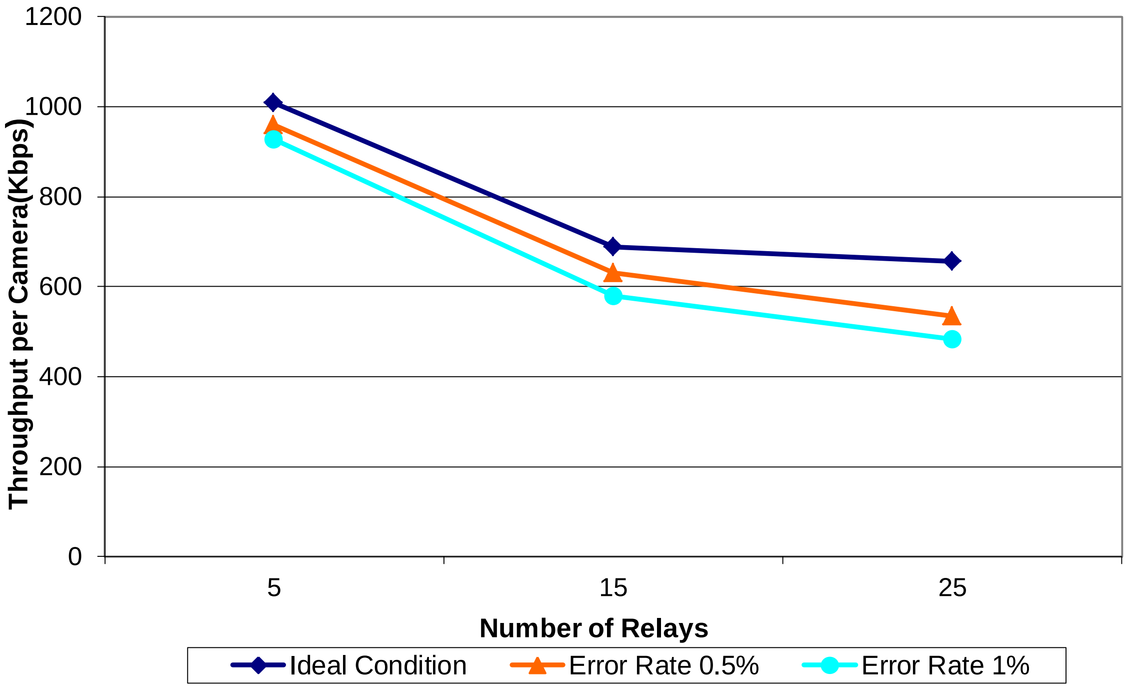


Figure 53 Throughput of one camera at different locations with different system error rates

7.2.4 Summary of the ns-2 Simulation Analysis

I. The implication of less relays is an increased number of required controllers that must have direct Internet connection. While a major benefit of adopting wireless sensor networks is the reduction in the amount of wired connections needed for a system, this poses a trade-off between the cost of the system and the required bandwidth of a system.

II. The throughput and error rate relationship studied in this section provides a template for such analyses. For example, Table 18 lists the tolerable wireless error rates with respect to different camera quality requirements.

Table 18 Tolerable error rates for different camera quality and different number of relays (with one camera)

Quality	Required Bandwidth (Kbps)	No. of Relays		
		5	15	25
High	1204	0%	*	*
Medium	384	5%	3%	2%
Low	256	7%	4%	3%

** The system cannot support this saturated throughput*

As shown, for a single low quality (256Kbps) camera network, the tolerable error rate decreases from 7% to 3% when the distance increases from about 0.62 miles (5 relays) to 3 miles (25 relays).

III. For the analysis based on the number of camera, with a network where the farthest camera is 15 relays away, Table 19 shows the tolerable error rates with different quality and number of cameras.

Table 19 Tolerated Error Rate at Different Number of Cameras (15 relays to the controller)

Quality	Required Bandwidth (Kbps)	No. of Cameras		
		1	3	5
High	1204	*	*	*
Medium	384	3%	0%	NA
Low	256	4%	3%	1%

** The system cannot support this saturated throughput*

This finding implies that the medium quality camera that supported transmission over 25 relays cannot be used in an environment with more than 3 cameras. A trade-off between the number, quality of cameras and the cost incurred is inevitable.

7.3 Integrated Simulator

The second type of simulation study utilized an integrated simulation platform which integrates the microscopic vehicle traffic simulator PARAMICS and the communication simulator ns-2. PARAMICS is a state-of-the-art detailed microscopic simulator that provides realistic traffic flow and detector modeling, with capabilities to plug in customized control procedure and external interface through extensive application programming interface (API) (Quadstone 2009). Ns-2, as discussed previously, is an open-source simulator for event-driven network protocol simulation, also allowing modular incorporation of newly developed protocol components and interface with other software (ISI 2006).

A simulation network created in PARAMICS was composed of a number of network files that define all aspects of a transportation system, including its infrastructure geometrics, traffic control methods, ITS components, driver characteristics, and traffic volumes. User-defined functions are implemented as a number of dynamic link library (DLL) files compiled from a C++ source file named plugin.c. The plugin.c file is also used by PARAMICS to perform synchronized coordination with ns-2. Microscopic traffic data, such as flow, speed and occupancy, are collected and stored into individual sensor log files, which can later be utilized for real time incident detection and clearance decisions. On the other side, ns-2 is composed of a single executable core, which is compiled from a large number of TCL and C++ source files for modeling individual network protocols. Ns-

2 models events occurring in each network protocol at each node, allowing users to extend procedures into any protocol by inserting code into the corresponding protocol source files and recompiling the core.

In this simulation, all incident detection algorithms are implemented in ns-2 module, for which real-time data acquired by a PARAMICS detector is transmitted towards its matching nodes in ns-2. The detection procedure is defined in ns-2 and it can initiate communication on demand with other sensors and controllers using the ns-2 communication support. Moreover, nodes in ns-2 achieve network consensus on detection and control decisions and convey that back to the matching PARAMICS detector. For more implementation details refer to appendix F.

7.3.1 Simulation Network Setup

The authors selected the I-85 corridor in Greenville, South Carolina as the simulation network, which consists of approximately 11 miles of freeway and 6 interchanges. This segment of I-85 is the major corridor connecting Atlanta, Georgia, and Charlotte, North Carolina.

After site selection, the PARAMICS microscopic traffic simulation software was utilized to build, calibrate, and validate the roadway network. Network building began by collecting various data including geometry, traffic control, and traffic volume. The geometric layout data for the roadway network was obtained from South Carolina Department of Natural Recourses in GIS format. Next, aerial photos from multiple sources and information collected from site visits were used to verify correct geometric conditions, such as number of lanes, lane widths, lane allocation, and curvature. The specific location of each traffic camera was also added to the network according to the SCDOT GIS data base.

The authors collected vehicle volume and incident data from the SCDOT and local planning organizations. The SCDOT provided hourly and average daily traffic count data, traffic signal timing data, and incident location, severity and duration data. The local planning organizations provided a planning model for use in predicting the origins and destinations matrix of the future network traffic. Other data needs such as speed limits, rights of way, and stripping, were met through observation during site visits. All this information was used to build the traffic simulation model in PARAMICS.

To ensure that the simulation model reflects traffic conditions accurately, the calibration and validation steps are of the utmost importance. The calibration step is to compare the simulated and measured traffic volume. The validation of the system performance output was carried out by comparing observed travel times and queue length with the simulated ones. Expert opinions from the local traffic management centers' staff was also used to confirm that the traffic model was a realistic representative of the real world. In addition, the overall simulated vehicular traffic volumes were within one percent of the measured, the highest individual volume error was no more than ten percent, and most of the individual volume errors were less than five percent. Furthermore, there was no significant difference between the observed and simulated queue lengths at the bottleneck segment, which were at the signalized off ramp intersections. Therefore, the simulation model accurately reflected the observed travel times within one percent.

The average annual daily traffic was obtained from the SCDOT and converted to hourly volume according to the typical traffic volume profile of an average weekday. The traffic scenario for this simulation was PM peak period during an average weekday because the peak traffic flow occurred between 4:30 PM and 6:30 PM at the study site. The simulations were started at 4:00 PM and allowed at least half an hour of warm up time. After the traffic volumes were fully loaded into the network, incidents were generated at locations and random times between 4:30 PM and 5:00 PM.

In ns-2 communication simulator, the authors assumed that wireless traffic surveillance operating agencies will implement IEEE 802.11b protocol with a bandwidth of 11MHz for communication among sensors and controllers in the field. The study considered traffic surveillance data generated at constant bit rate and sent across the network using the User Datagram Protocol (UDP).

7.3.2 Simulation Scenario

The integrated simulation implemented a two-layer hierarchical traffic sensor network, capable of both centralized and distributed incident detection in the integrated simulator. The following content first describes the hierarchical network architecture, which manifests itself in the routing protocol implementation. Then, the incident detection algorithm and different incident simulation scenarios are explained.

There are 15 traffic sensors and three controllers covered the entire simulation network, while each controller is in charge of five sensors. Traffic sensors collect the traffic information, and send it to the presiding controller in every pre-defined time interval. Each controller gathers the information from sensors and implemented an incident detection algorithm based on the information. Distance between each sensor was modeled as half a mile. Controllers are typically located at or close to the major interchange, where incidents are most likely to occur. The ad hoc wireless network formed was modeled in ns-2 to connect all sensors, controllers and relays in between. Figure 53 demonstrates the network and modeled traffic sensor deployment.

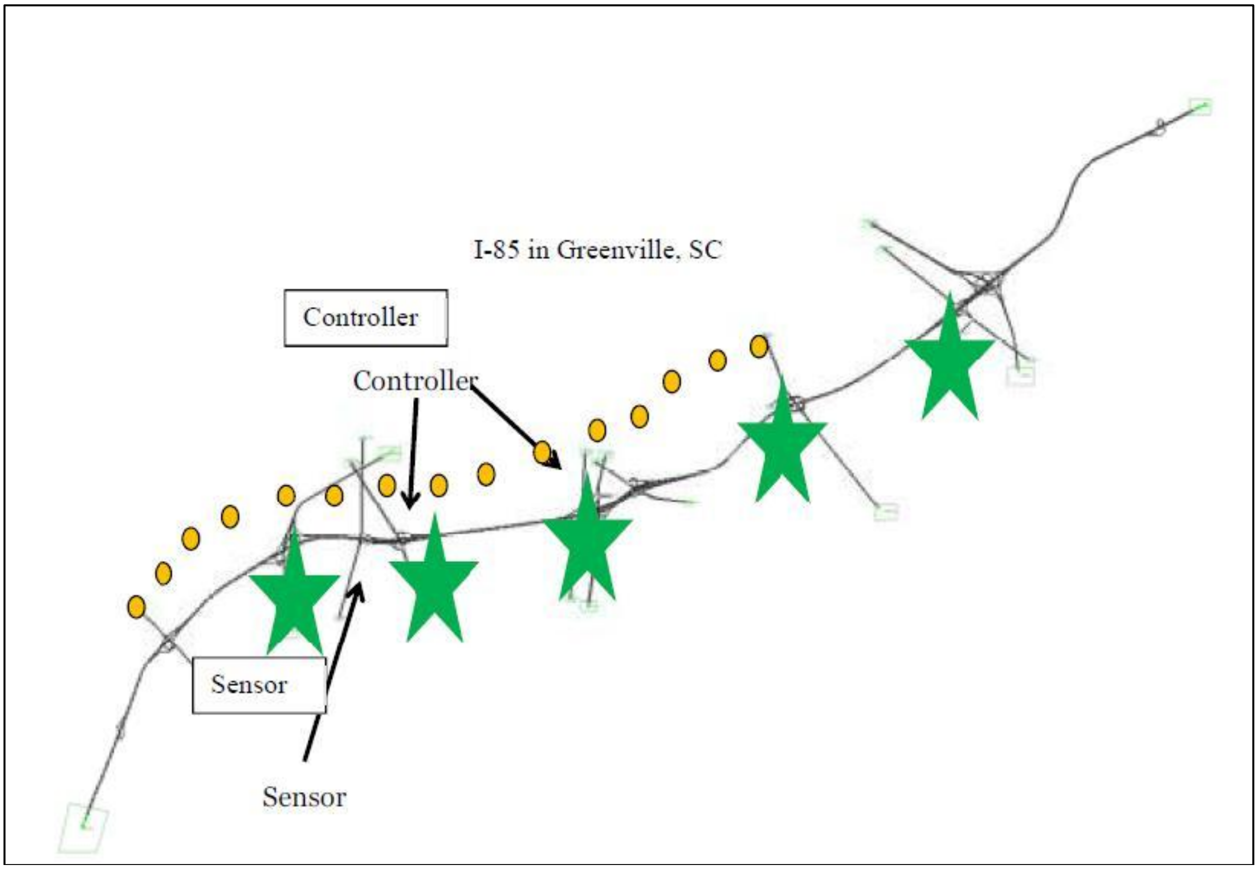


Figure 54 Simulation Network Deployment

Each sensor or controller (Type) has unique number and its location is uniquely identified with its mileage from the road's starting point. The address format is

[Highway No., Location, Type, Direction]

A device can have one or multiple addresses, according to whether it is located on one or multiple highways (at an intersection), oversees one or both sides of a road (bi-directional traffic sensors), and conducts tasks belonging to one or multiple hierarchical levels. In this simulation, each traffic sensor only detects one side and one direction of the highway traffic. Each controller only gathers the information and implements the detection algorithm but does not record all traffic information.

Message routing among sensors and controllers is done in the hierarchical address space with specific emphasis on simplicity for sensors. For centralized control strategy, each sensor only talks to its presiding controller.

7.3.3 Incident Detection Algorithm

The authors implemented one of the first incident detection algorithms in ns-2, California algorithm, to detect incident. The algorithm is utilized to detect an incident based on the measured occupancy from two adjacent detectors (Martin et al. 2001).

7.3.4 MOEs Selection

The vehicular traffic simulator randomly generated incidents on segments under surveillance of traffic cameras. Various incident occurrence times, locations and severities are also random generated by an API program to assess the detection and communication performance of the wireless traffic sensor network. PARAMICS also provides the duration of incidents through a simulation of interaction including the vehicles involved in incidents and the vehicles in the queue. The duration of incidents, which is defined as the time period between incident occurrence and the return to normal traffic condition, directly affects the communication cost in terms of data rate, which can be altered by the ns-2 during the simulation.

In order to assess the traffic operational and communication performance, several measure of effectiveness (MOEs) were selected including 1) incident detection rate, 2) false alarm rate, and 3) communication latency. Communication latency defined here is related to the incident detection and verification time. The latency is the time from the first sensor reporting abnormity to the controller until the incident is identified. Table 20 summarized the study scenarios and MOEs.

Table 20 Simulation Scenarios and MOEs

Incident Scenarios	Simulation Output	Category	MOEs
Severity: 4 lanes block	Occupancy (s)	Traffic Operation	Incident Detection Rate (%)
			False Alarm Rate (%)
Duration: 30 minutes		Communication	Latency (s)

7.3.5 Integrated Simulation Analysis

This section presents the results of integrated simulation, which includes the communication and traffic operational performance. In order to mimic the data transmission needed for traffic operation before and after a traffic incident, the simulation used two different data rates. Before incident, the sensor only sends regular traffic data such as flow, speed and density, which is assumed to be at a speed of 32 Kbps. Once the incident occurs, sensors close to the incident location start to send high quality video image to the TMC with a data rate 1024 Kbps.

- **Measure the communication latency for different data rates**

With sensor spacing 0.4-0.5 mile, Figure 54 shows an example of variation of communication latency in 600 second simulation time after an incident.

As shown in Figure 60, the communication latency with 32 Kbps as well as 1024 Kbps data rate varies in the range of 0.2- 0.35 sec with an average 0. 266 sec. Analysis of variance (ANOVA) results indicated there is no significant difference between the communication latency of these two different rates (P =0.80 >0.05). However, we need to ensure that the communication throughput is not saturated when sending 1024 Kbps because we only measured the latency of the data package that successfully received by the controller.

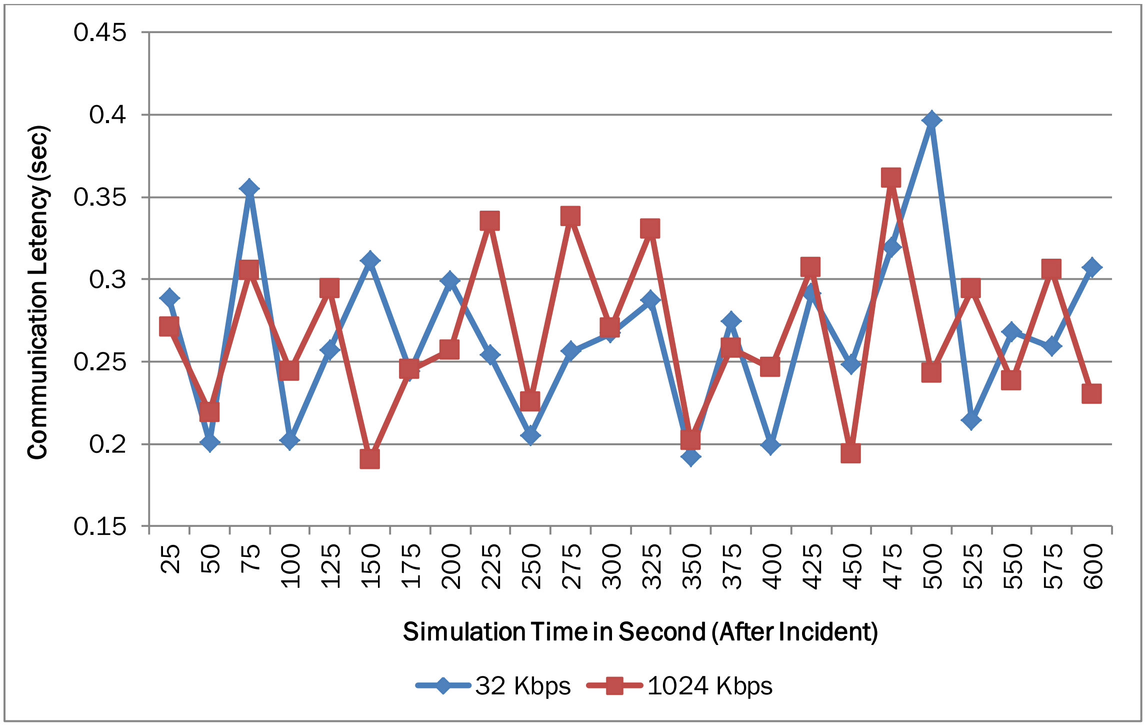


Figure 55 Examples of Communication Latency at Different Data Rates

- **Study the communication and traffic operational performance:**

Ns-2 simulation results indicated that when three cameras connected with each other and finally connected with the local controller, the delivery ratio is lower than 10% when data rate close to 1024 Kbps. Many data packets were lost during the transmission because the link was over saturated.

Therefore, it was confirmed that communication latency only shows how fast the packet can be transmitted from a sensor to the controller, it does not indicate whether the system reaches the capacity. Once the system reaches capacity, the data packets starts to drop, so traffic agencies in TMCs are likely to experience video slow down or disconnection. Table 21 summarizes the communication and traffic operational performance.

Table 21 Communication and Traffic Operational Performance

Sensor Spacing (mile)	Communication Latency (sec)	Detection Rate (%)	False Alarm Rate (%)
0.4-0.5 mile	0.266	99%	<0.5%
0.8-0.9 mile	0.524	99%	0.5%

As seen from Table 20, the incident detection time is almost doubled when the sensor spacing increases from 0.4 mile to 0.8 mile. According to this detection algorithm, the automatic incident detection time depends on the distance between the incident locations to the closest upstream sensor.

The detection algorithm works well for this incident scenario with a 99% incident detection rate and 0.5% false alarm rate. These results indicated the feasibility of using wireless sensor network to automatically detect and verify an incident in a timely fashion.

However, the incident scenario studied is the most severe case which blocks all the traffic lanes in one direction. The traffic queue builds very fast and no vehicle is passing in the downstream direction. Therefore, the sensor network alarm the incident once the queue reaches the closest upstream sensor. If the incident does not block all the lanes, and vehicles still can travel to the downstream, the threshold values need to be adjusted to enhance the detection rate. This integrated simulation did not test other incident scenarios in terms of incident severity because algorithm evaluation was not the scope of this study.

7.3.6 Summary of the Integrated Simulation Analysis

1. Even though the Analysis of variance technique indicates that the communication latency for data rates of 32Kbps and 1024 Kbps is roughly same, ns-2 simulation helped to identify that successful delivery rate drastically reduced at 1024 Kb indicating that the system was saturated. Thus while carrying out any analysis for communication networks, it is recommended to have more than one evaluation metric.
2. The incident detection algorithm is sensitive to the inter-sensor spacing. However the tests indicate that the detection rate is impressive and false alarm rate is also minimal encouraging the utility of the algorithm for the discussed wireless setup.

8 PERFORMANCE COST ANALYSIS

Performance /Cost analysis serves as a vital factor in deciding on the cost- effective communication technology and topology. In this report, this analysis used the output of the simulation experiments to estimate the performance. The cost information was gathered from the wireless equipment vendors and USDOT ITS cost database.

Accordingly for Greenville network, without considering the fiber cost it was observed that Wi-Fi mesh and infrastructure provided the highest throughput/cost. WiMAX infrastructure on the other hand provided the lowest throughput /cost.

8.1 Description

Based on the simulation results, the authors performed performance-cost analysis for the selected strategies using the benefit and cost information from literature review, case study, field test and simulation analysis. This section analyzes the cost effectiveness of using 802.11g wireless technology to support traffic surveillance systems in Greenville, SC, as proposed in the case study session.

Besides literature review, cost information was also referenced from the typically used default values from the ITS Deployment Analysis System (IDAS) and ITS Cost Database maintained by Federal Highway Administration (FHWA) (USDOT 2007). IDAS is a computer tool developed by USDOT to provide direct benefit and cost information based on future travel demand and other required inputs (USDOT 2003). Both IDAS and the database maintained by the FHWA are updated periodically. Cost information from these two databases, as well as the cost information of the existing systems from different state agencies through interview, were combined to provide the most logical and realistic estimate.

This section will use the Greenville network as an example, where the benefit was considered as the total throughput needed to support all the surveillance devices. Similar to what has been conducted in ns-2 simulation study, simulation provided the throughput of each device under 802.11 g technologies within two different network topologies, mesh and infrastructure. The cost has several components including the devices, maintenance, operation, installation, and personnel. Total annual costs were also calculated for the two network topologies. Finally the cost effectiveness was computed as the throughput/cost ratio. The overall cost effectiveness analysis procedure is shown in the flow chart in Figure 55.

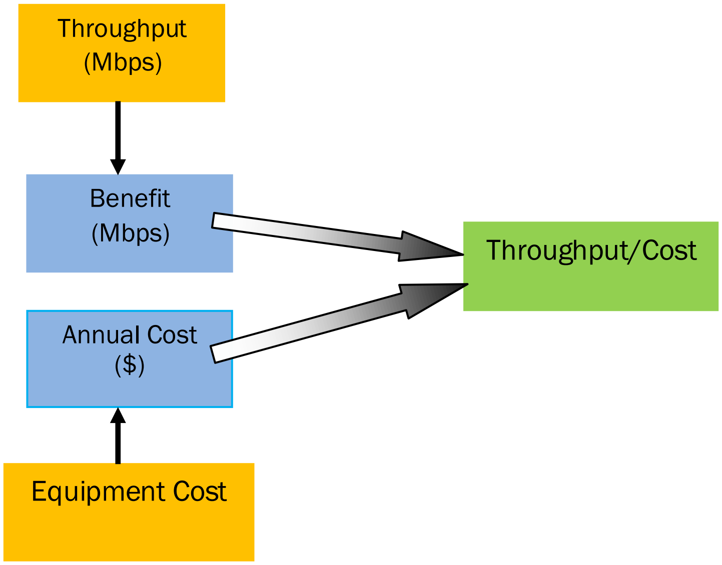


Figure 56 Throughput/Cost analysis procedure

Maintenance cost, operation cost and transmission power cost can be easily converted to a yearly value. The equipment costs, including both the device cost and infrastructure cost, were converted into annual cost using the following formula.

$$\text{Annual cost} = \sum C \frac{d(1+d)^n}{(1+d)^n - 1} + O$$

Where C is the capitalized cost of network topology; O is the annual operational cost; d is the discount rate; n is the life time of the equipment in years.

The traffic surveillance system in Greenville mainly consists of traffic cameras and radar detectors, which are normally mounted on the same equipment pole. Therefore, for each location, one client radio cost was considered. The maintenance and operation cost was assumed to be 15% of the total infrastructure cost (USDOT 2009). The fiber optic cable cost, installation, operation, and maintenance cost were also taken into consideration at fiber drop locations as needed by the network topology. Moreover, the transmission power cost was also considered using the commercial electric price in South Carolina for 2009. This analysis assumed that traffic camera works 8 hours a day, and 365 days a year.

8.2 Performance-Cost Analysis

First, using Greenville network as an example, a cost analysis was conducted for each of the four architectures discussed in the previous section, and then the four scenarios were ranked per their throughput/cost ratio. Since pricing fiber optic connections can vary greatly, depending upon the specific location and the selected Internet Service Provider (ISP), these variables were omitted from the cost comparison._The number of fiber optic connections required for each of the architectures is shown in Table 22. Moreover, the number of fiber optic connections required should be considered during the network design phase, as adding connectivity can add both a significant one-time and recurring cost. Table 22 does not consider any recurring cost resulting from leasing the connectivity from an ISP, nor does it show any maintenance related costs. Because this cost should be same for all four scenarios, it would not affects the comparison outcomes.

For Greenville network, Table 22 lists the cost and number of base stations and client radios required for both the mesh and infrastructure architectures. For the Wi-Fi infrastructure network, seen from Figure 45, within each cluster, each traffic camera directly sends traffic video information to the one connected to the fiber system. There is no connection between clusters, and each cluster would have its own fiber optical access. There are six fiber drops needed for this scenario. Each camera is equipped with a Cisco Aironet 1410 wireless bridge (Wi-Fi base station), which has a built-in directional antenna. The typical used Cisco 1310 model was not chosen because it does not have built-in antennas which will bring an extra cost. The Cisco Aironet 1400 Series Wireless Bridge is an 802.11a radio with 24 dBm (250 mW) maximum transmit power, -70 dBm receive sensitivity at 54 Mbps data rate (Cisco[1] 2009). Unit cost is around $3200-$3700, which was referenced from Cisco product information in 2009.

In Wi-Fi mesh network, one camera within the cluster first gather all the video data from other cameras, then passes the information out to the camera in charges the other clusters, until reaching the pre-selected cluster which has one camera connected to the fiber system. Therefore, instead of having fiber connection for each small cluster, there are only two connection needed. In this case, each camera is both receiving and sending data from/to neighboring sensors, so two directional antennas are needed for each camera. The authors chose to use Cisco Aironet 1524(Cisco[2] 2009) which has two built-in directional antennas instead of having two Cisco 1410 radios for each camera to minimizes the equipment cost. Therefore, Wi-Fi infrastructure requires 14 Cisco 1410 radios, while Wi-Fi mesh scenario needs 14 Cisco 1524 radios. The difference between these two scenarios is the number of fiber connection, which is not considered in the cost.

Similarly, the WiMAX mesh scenario requires 14 base stations because each camera needs to communicate with the neighboring cameras. As seen from Figure 46 WiMAX infrastructure network needs only two base stations but 14 client radios because each camera only transmits data to the base station without communicating with other cameras. However, the base station used in mesh scenario is different from the one used in infrastructure network because of different transmission power and coverage range characteristics.

Detailed information can be found in Table 22. With this information we can see that the Wi-Fi Mesh architecture provides the lowest cost solution, while the WiMAX infrastructure architecture is the most expensive.

Table 22 Cost Analysis for Greenville Network

Architecture	**Technology**	**Base Stations**	**Unit Cost**	**Client Radios**	**Unit Cost**	**Total Cost for Radios**	**Fiber Connections**
Mesh	Wi-Fi (802.11g)	14	$3,500	N/A	N/A	$49,000 [1]	2
	WiMAX	14	$10,595	N/A	N/A	$148,330	2
Infrastructure	Wi-Fi (802.11g)	14	$3,500	N/A	N/A	$49,000	6
	WiMAX	2	$125,000	14	$2,200	$280,800 [2]	2

[1] – This cost includes one directional antenna to connect the satellite camera to the mesh network

[2] – Quoted estimate for one WiMAX base station and a transmission tower, including construction

The ns-2 communication simulator was used to model the network and communication between devices. For the Wi-Fi scenario, the study assumed IEEE 802.11b protocol with a bandwidth of 11Mbps is used to support the data transmission.

In the infrastructure network, data is only transmitted within the same cluster, hence there is no capacity sharing between devices in this particular case.

However, wireless performance can be affected by many factors such as terrain, foliage coverage, and weather, as discussed in pervious chapters. The real link rate that each device received cannot reach as high as 11Mbps (Zhou^2 et al. 2009). The ns-2 simulation result indicates there the average throughput per device is about 8.6 Mbps. In the mesh network scenario, data is being transmitted from one camera to another until it reaches the fiber connection set-up earlier; the link capacity is shared by several devices. As shown in the ns-2 simulation results, the link between the last devices to the fiber drop suffers the most during heavy loading of data because it carries all the information from previous cameras along the communication link, as the example shown in Figure 56 (Ma et al. 2009). The results of the previous section on ns-2 simulation analysis, also indicated that the average link rate that each camera can receive depends on the rate of the last link within the same mesh cluster, as illustrated in Figure 56.

For WiMAX scenario, the average throughput is referred to the field measurements, assuming using 5 Mhz channel (DeBeasi 2008). This was not simulated in the study. Due to the nature of the WiMAX technology, the throughput that a client can receive depends on the distance between client and base station. Similar to the previously discussed two Wi-Fi scenarios, average throughput in WiMAX mesh network depends on the last link within the same cluster, while there is no bandwidth sharing in WiMAX infrastructure network.

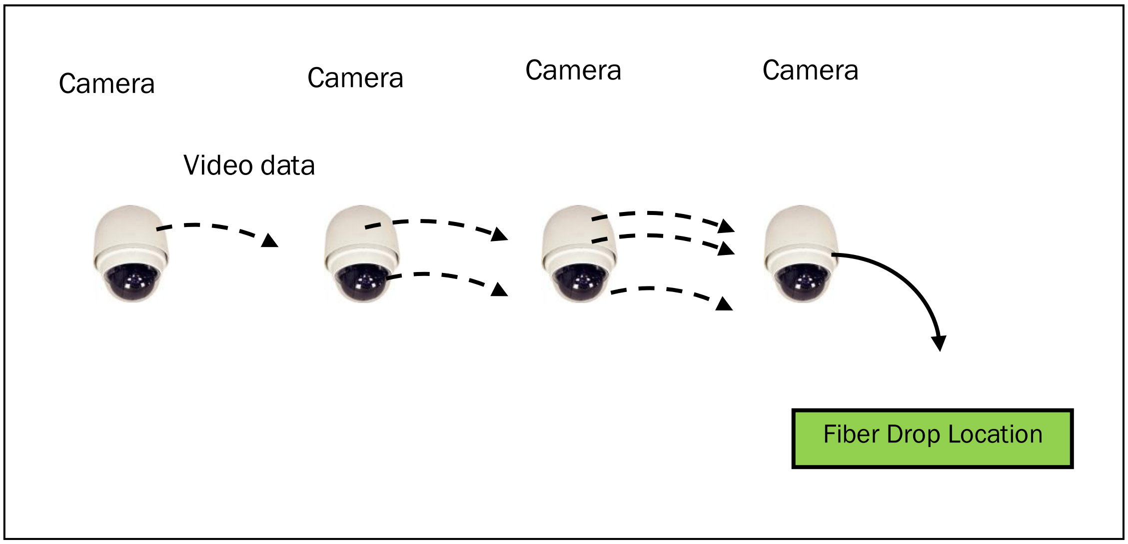


Figure 57 An Example of Data Transmission within One Mesh Cluster

Typical traffic cameras' data rates range from 64Kbps to 384 Kbps, whereas some high quality traffic cameras may require more than 1 Mbps bandwidth (Gordon et al. 2005). The researchers assume each camera requires 384 Kbps data rate, so the throughput requirements of the entire network is the 384Kbps multiplied by the total number of cameras.

Although the infrastructure provides more bandwidth per device, the researchers used the actual demand rather than highest throughput possible for each Wi-Fi and WiMAX network topology. Therefore, throughput-cost ratio was calculated by dividing the actual throughput requirements by total equipment cost. Table 23 compares the average throughput of each devices and the cost effectiveness under four network architectures.

Total throughput of the entire network equals the throughput of all devices within the network.

Table 23 Comparison of Four Network Architectures

Technology	Architecture	Average Throughput (Mbps)	Throughput Requirements (Mbps)	Total Cost ($)	Throughput/Cost (Bits/Dollar)
Wi-Fi	Mesh	2.9	5.38	49,000	109.79
	Infrastructure	8.6		49,000	109.79
WiMAX	Mesh	3.8		148,330	36.27
	Infrastructure	9.15		280,800	19.16

Table 23 indicated that the Wi-Fi infrastructure and mesh network had the same throughput-cost ratio. Considering the number of fiber drops needed, a Wi-Fi mesh solution has highest throughput-cost ratio for Greenville traffic camera systems, while the WiMAX mesh is the next highest option. Because the WiMAX mesh was found to have a higher throughput-cost ratio than WiMAX infrastructure, this case study showed that the total cost is always cheaper with a mesh solution. However, as the authors discussed in the case study section, compared to infrastructure option, the mesh option has less expandability for future ITS devices deployment.

This section also did not compare the amount of excess bandwidth for each of the architectures, as it is extremely network specific. According to earlier mentioned typical data rates of traffic cameras, both of the two infrastructure-based network architectures provide a significant amount of excess bandwidth for use in supplying connectivity to future ITS components. The WiMAX infrastructure provides the greatest amount of excess bandwidth which benefits the system future expansion. When several ITS devices are located on a same pole sending information simultaneously and sharing the bandwidth, WiMAX infrastructure can provide the most bandwidth upgrade space, even though it is the most expensive.

9 ASSET MANAGEMENT

The asset management analysis indicated that Enterprise Based GIS systems offer the best fit for the SCDOT to manage its ITS infrastructure. The key factors supporting this recommendation include the SCDOT's current use and experience with similar software and the potential benefits of system integration. For example, other applications such as pavement management already utilize GIS technology and existing personnel experience can be leveraged when using enterprise GIS for ITS asset management. Although the software NexusWorx was rated highly, overall it ranked slightly less than enterprise GIS. MS Access by far carried the lowest rank due to its limited visualization and customization abilities.

9.1 Analysis Summary

Aim: To recommend a suitable ITS Asset Management system.

This section briefly introduces the methods employed to evaluate asset management systems for managing ITS infrastructure. The first step of the analysis involved setting the requirements for evaluating an ITS asset management system. Asset management systems were identified based on findings from previous studies, the case study herein, and discussions with SCDOT officials. Three groups of systems were selected for evaluation: an ITS customized system, an Enterprise based GIS and a typical database management system. NexusWorx, Enterprise based GIS (SDEGIS) and Microsoft Access represented these groups respectively.

To assess the capability of the three systems, each system was individually evaluated and rated accordingly to its performance by practicing engineers and technicians. Finally, the last part of the analysis includes the comparative evaluation of the three systems using multi-criteria decision analysis. This analysis was chosen because it provided a visual representation of system capabilities and deficiencies. A multi-attribute utility model was developed as part of the multi-criteria decision analysis.

There is a strong possibility that ITS deployment agencies will include wireless communication systems in the future as a part of their ITS surveillance system. The asset management systems that are currently based on wired communications will need to support the wireless network at that point. While evaluating asset management systems, both wired and wireless assets required evaluation. In this section, the wired communication network was evaluated as the existing SCDOT Greenville, South Carolina, ITS network. Because the current study site does not have any wireless communication networks deployed, a network design of a wireless system is presented as a case study and used to evaluate the asset management tools.

9.2 Selection of MOE

Measures of effectiveness (MOEs) were selected based on the requirements of the ITS asset management system determined from the interviews with SCDOT ITS engineers, database managers, and GIS experts. After these MOEs were identified, interviewees rated their importance. The average importance of each metric was then used to evaluate each asset management system. Researchers used a multi-attribute utility model to value each MOE appropriately and determine a weighted score for the performance of each tool examined. Figure 57 shows the MOEs selected for the project and the categories they were divided into.

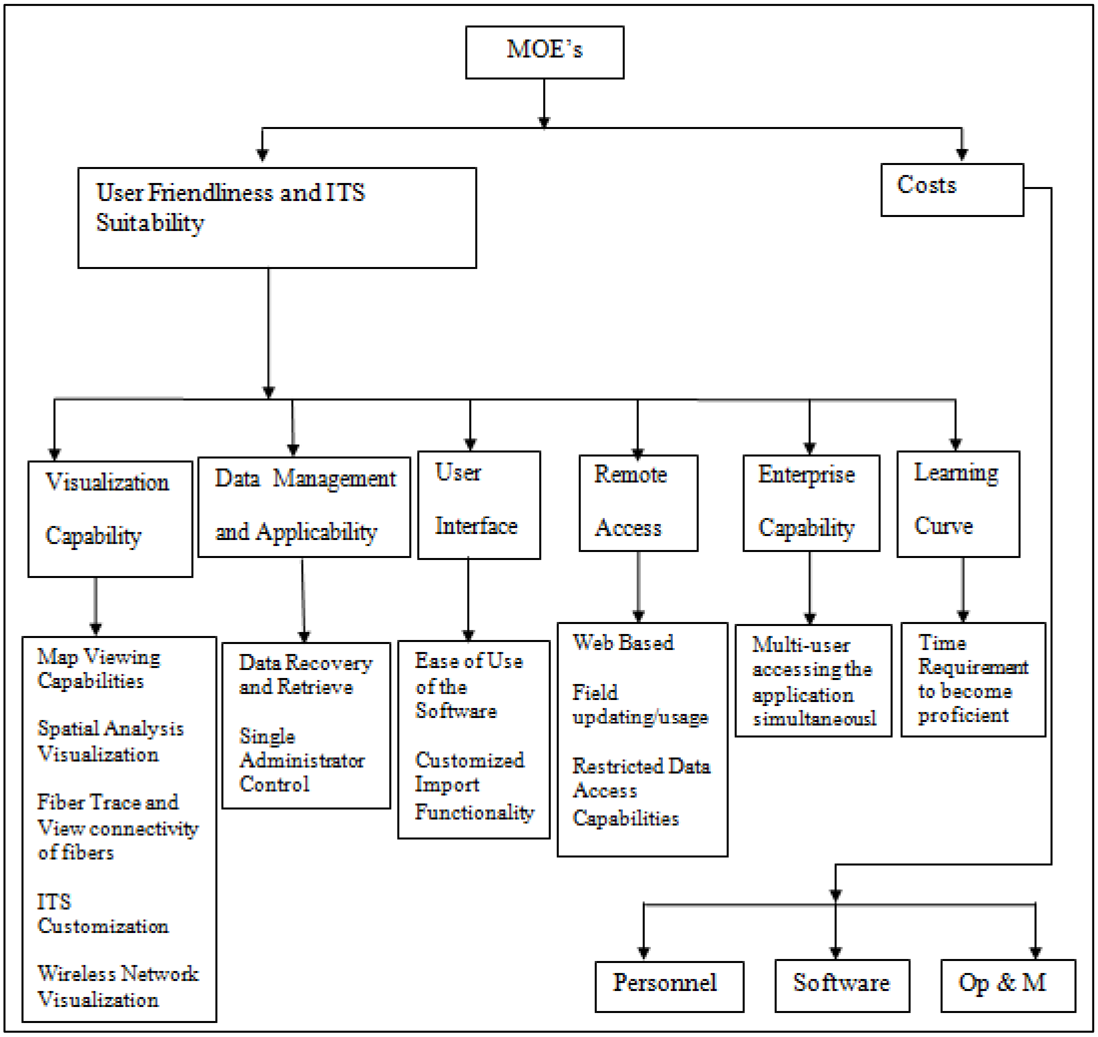


Figure 58 Selected measures of effectiveness for asset management evaluation

The MOEs are broadly classified into two categories: User Friendliness/ITS Suitability and Costs. Each category was broken down further based on the individual criteria's involvement with each category. Based on those subcategories, an interview was created to compare all three systems by asking for a quantitative ranking of each attribute for each software.

9.2.1 User Friendliness and ITS Suitability

Researchers divided the first category into visualization capability, data management and applicability, user interface, remote access, enterprise capability, and learning curve. The following sections present how each of these seemingly-qualitative factors were measured objectively and quantitatively.

9.2.1.1 *Visualization Capability*

Visualization was considered one of the most important factors for ITS asset management. It plays an important role in decision making through visual observation and interpretation of a scenario. The visualization capabilities includes map viewing capability, visual representation of spatial queries, visualization of fiber traces, connectivity of fibers, ITS customization for enhanced visualization, and wireless network visualization.

Measuring the map viewing capability focused on the system's ability to manage a geographic location system. A point with known coordinates was entered into the system to evaluate how the system located the point and displayed it on the map. Accurately locating data points was considered a prerequisite for data visualization.

Spatial analysis visualization measured the ability of the software to translate assets into a visual form. Multiple queries were conducted based on factors such as attributes and location. The results were compared among the three systems and rated based on their performance.

Since communication connectivity is an important attribute to display, each tool was evaluated for their ability to show visual connectivity of fibers. The systems were tested to determine their ability to 1) trace a physical fiber's path along the network and 2) display its connections to other devices.

ITS customization refers to the ability to customize a system to support the ITS assets and their associated attributes. Personnel from different fields need standardized symbols and icons to clearly distinguish and recognize different ITS devices and components. Each system was checked to determine what customized symbols and icons were useful for the ITS applications provided. The capability of the symbols and icons to represent specific devices and structures were also assessed.

The last criterion to evaluate visualization capability was wireless network visualization. The ability to visualize detailed wireless networks was determined. An important factor is the simplicity of the display of the network because it can allow a quick and easy understanding of the entire network. Each system was checked to see whether it had the specific tools to visually represent the wireless network. Then each system was judged to see how simple and clear the network was displayed.

9.2.1.2 *Data Management and Applicability*

Data management is an important issue to ITS asset management, particularly to allow single administrator control. Researchers evaluated the ability of each system to recover and retrieve data to protect against system failures of the data storage components. The method of data storage and the reliability of the data storage network were judged for each system.

The capability of having a single administrator who validates all the field updates before they become final assumes importance when there is a concern that database changes from field users or technicians might not be correct. Therefore, an administrator is responsible to validate the updates before they become permanent. For each system, the ability to possess single administrator control was judged and rated.

9.2.1.3 *User Interface*

The user interface evaluation focused on user-friendliness of system access and workability. The level of simplicity and speed of the system to allow the user to perform a specific task is considered in this MOE. Specifically, ease of use of the software was measured as how well users could manage ITS assets efficiently assuming that a user is proficient in the use of that software. Each system was judged on how well users could understand and immediately begin using the software. Researchers qualitatively evaluated each tool and provided one subjective rating for the user-friendliness of the user interface of each software tool.

Next, the customized import functionality was reviewed. This feature is the capability to import files in different formats such as shape files, as-built drawings and AutoCAD files without having to reformat the database. Each system was judged based on their capability to import and support different forms of import files. This MOE was divided into two groups: namely straight out of the box import functionality and supporting user specific customization. Straight out of the box customization can be enough to support the user’s needs in most cases. However users require the flexibility to customize the imported attributes into a useable format. So for this MOE, both cases were evaluated and these characteristics are noted in Figure 57.

9.2.1.4 *Remote Access*

Remote access is important especially when multiple agencies are sharing data in order to integrate different transportation divisions for more efficient management and budget allocation. Remote access covers the capability to access the system via the web, conduct field updates/usage of the system, and restrict access as necessary for data security and integrity.

Web based access is the capability of using a web browser to access the system instead of being forced to install the software on each individual computer. Each system was evaluated based on whether it had full capabilities when accessed via the web using standard web-browsing software (such as internet explorer).

Because field updating and usage of databases is essential in some field work, each system was evaluated based on the ability to update the database from the field or add new data entries from a field location.

Lastly, each system was reviewed for its restricted data access capabilities. Restricted data access means that all the users do not have the same privileges to modify the data. Defined upper level users should be able to edit and view the database and maintain full access of the database. Users that only need to view the data should be allowed limited access capabilities. Researchers evaluated the ability to have varying “read only” or “read/write” formats for different users or user groups. The capability was tested by attempting to view the database only (read only) for some users, and to view and edit the database (read/write) privileges for other users.

9.2.1.5 *Enterprise Capability*

This MOE rated the capability of a system to support multiple users at the same time and allow simultaneous access to the database that is saved in a central location. Each system was evaluated based on its ability to be accessed simultaneously from different computers.

9.2.1.6 *Learning Curve*

The last MOE evaluated under the user friendliness and ITS suitability category was learning curve. Since software training can be time-consuming and costly to agencies, this measure of effectiveness was reviewed separately from the user interface evaluation.

9.2.2 Costs

The second primary branch of MOEs includes costs of asset management tools. Following established economic evaluations, researchers broke the costs into three categories: personnel, software, and operation/maintenance. The values of cost used for this analysis were obtained from software vendors and expert opinion and are not based on actual cost data from prior projects. The next section presents how each of these MOEs are used to evaluate the three asset management softwares for ITS applications.

9.3 Evaluation of Asset Management Systems Available for ITS

The goal of this analysis was to identify a system that can manage ITS assets in an efficient, cost effective and convenient way. Because ITS consists of different devices and systems such as cameras, radar detectors, variable message signs, wireless and wired communication systems; it becomes challenging to manage the network with traditional asset management systems. The three systems evaluated; Nexusworx, Enterprise Based GIS, and Microsoft Access; are representative of three groups of ITS asset management systems and were evaluated to determine their relative compatibility to meet the MOEs. The evaluation was performed by developing a utility model, calibrating the parameters and ranking the alternatives based on interviews with SCDOT ITS engineers, database managers, and GIS experts.

9.3.1 Evaluation Team Selection

An in-house evaluation team was developed with consideration to the fact that team members should have exposure to all three systems. The team members attended a workshop on the NexusWorx ITS asset management system after NexusWorx was selected as one of the ITS asset management systems for the project and the criteria for evaluation were set. All the members had knowledge of GIS and have worked with GIS systems for various projects. Members were also proficient in the use of Microsoft Access. For Enterprise GIS capabilities, the research team consulted with SCDOT officials and Clemson University GIS specialists.

9.3.2 Study Site Selection

The site selected for the test is located on I-85 near Greenville, South Carolina. All the information for the study site was collected from the SCDOT using as-built drawings of the study site. These drawings contained all necessary information regarding ITS devices. A sample of an as-built drawing is shown in Figure 58, which depicts the study site with the ITS devices. The highlighted portion in Figure 58 shows the study area that includes one HUB (router or similar device that connects many other devices or computers to a single computer), nine cameras, and one Dynamic Message Sign (DMS).

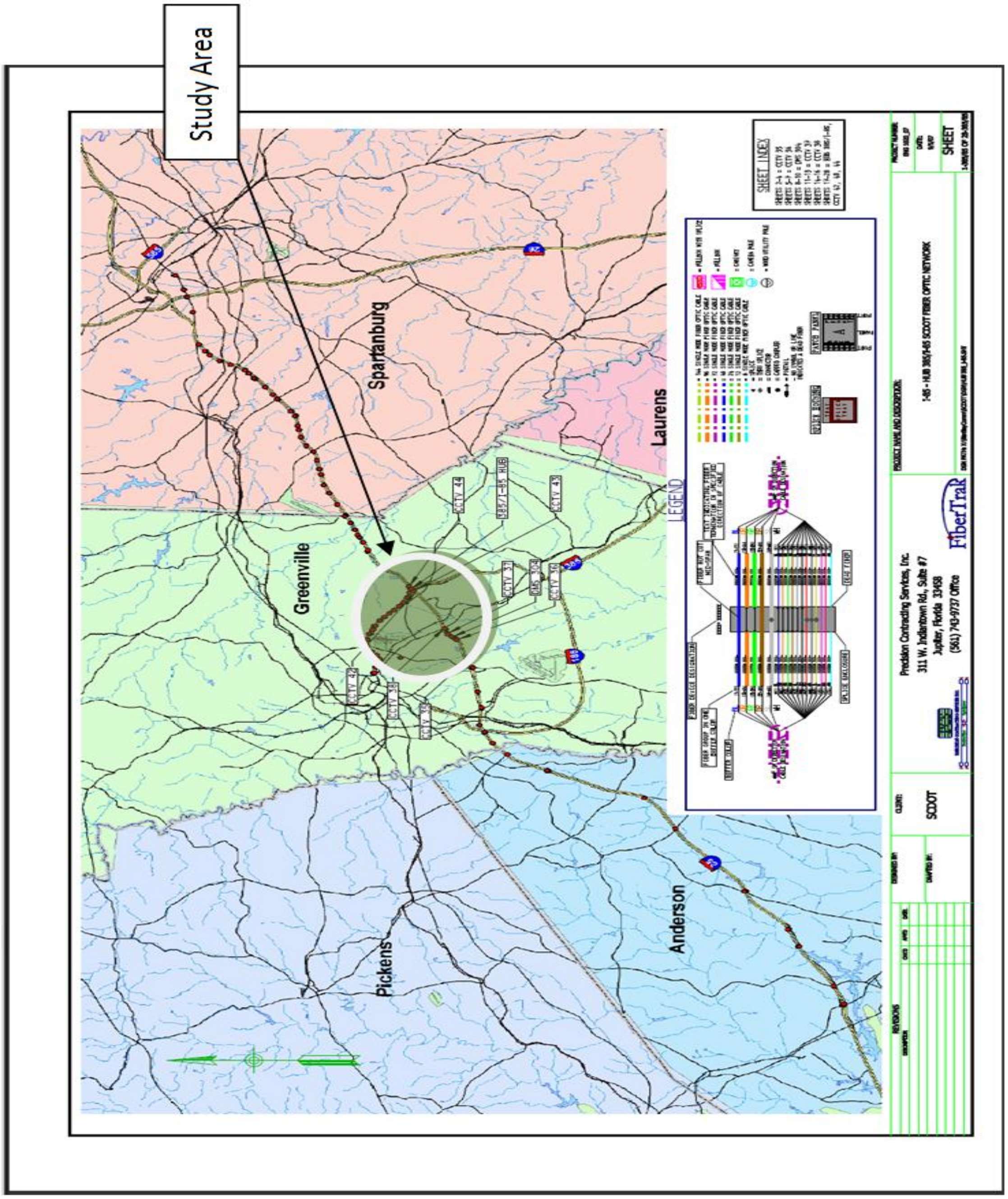


Figure 59 As-built drawing for the ITS Facilities (SC DOT)

9.3.3 Test Plan Development

For each MOE, an individual test was planned. The test plan was based on the site selected for the project study site and the research team performed the tests for each MOE separately and then ranked the system. The main objective was to develop a complete ITS asset management plan for the selected site and observe whether the three software could perform the asset management functions for ITS. Based on their performance in the tests, a rating was assigned to each system for each MOE, and then used in the multi-attribute utility model analysis to find the utility values of each MOE.

9.3.4 Testing the Systems

The research team judged each of the systems based on the developed test plan to justify whether they could support the requirements of ITS asset management. The test performed for each system was based on the selected study site with ITS devices and different communication systems (wired and wireless). The test covered the wired network and different wireless networks (Wi-Fi and WiMAX) since wireless is becoming an emerging application for ITS traffic surveillance systems.

9.3.5 The Rating of the Systems

The research team made use of a relative rating to evaluate the performance of the three systems in terms of the defined measures of effectiveness. The system that did not possess the capability for a selected MOE was rated zero. The system having the capability and meeting all the needs associated with a specific task and that is best suited to achieve the goal was rated as five. Once the research team had the initial rating based on the test, Clemson University GIS experts were consulted to validate ratings. Two types of evaluations were performed: 1) considering the system capabilities only and 2) considering the system capabilities with the cost of the systems. Table 24 shows the rating scale that was used for the system rating

Table 24 rating Scale for the systems

Rating	Significance
0	Does not have the capability
1	Has the capability but not very good
2	Satisfactory
3	Good
4	Very Good
5	Excellent

9.4 Multi-Attribute Utility Model Methodology

A multi-attribute utility model was chosen because a simple, clear-cut comparison between the customized ITS system and other alternatives were not possible. Additionally, a typical benefit cost analysis might not reflect some of the basic qualities of an asset management system for ITS because some of the components were difficult to quantify and a simple benefit cost analysis will not be able to reflect the overall performance of an alternative. Multi-criteria decision analysis incorporating these cost and performance components and quantifying them in terms of utility value is an appropriate technique. The multi-attribute utility model is used with the evaluation of three asset management systems to help choose the best alternative for the SCDOT.

The multi-attribute utility model followed the steps shown in Figure 59. The goals were first identified, and then the measurement of effectiveness (MOE) needed to accomplish those objectives was assigned. The MOEs are those previously selected for the evaluation of ITS asset management system, as presented in Figure 57. The alternatives were defined by the three asset management tools selected and previously discussed. Finally, the multi-attribute utility model is applied to help select the best alternative. The multi-attribute analysis was conducted twice, considering two scenarios: 1) only system capabilities and 2) system capabilities as well as the costs of the systems. These scenarios are presented to provide two views of asset management systems. In particular, software cost is significantly different between the tools evaluated and these different views of the analysis clarify the uniqueness of their values.

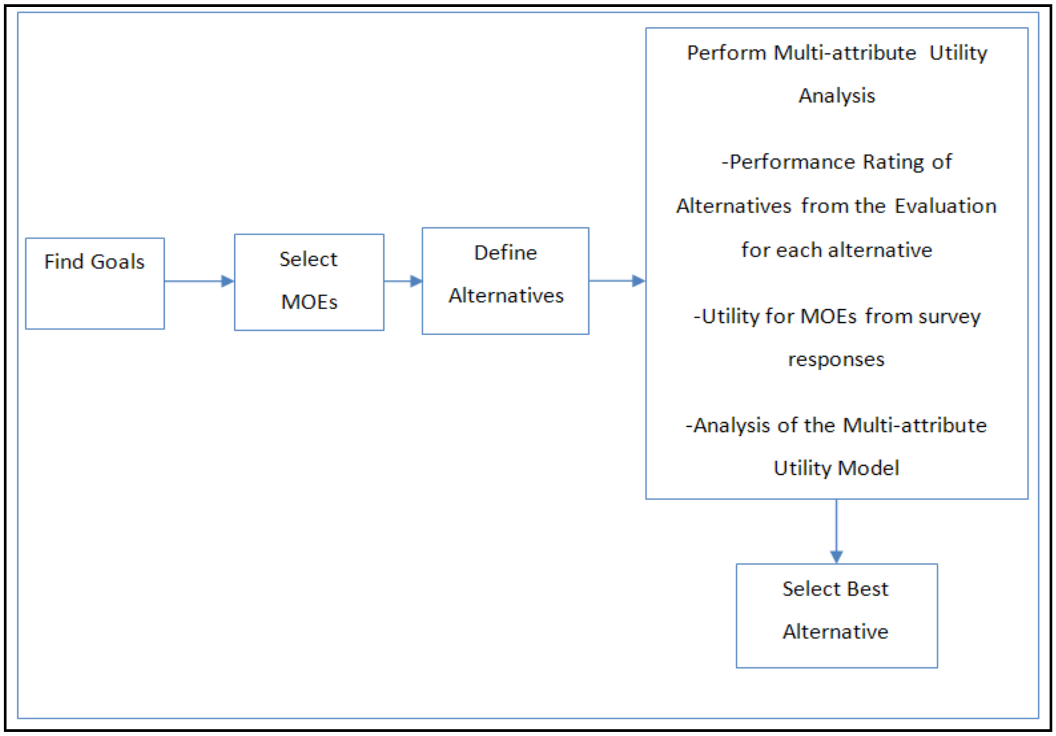


Figure 60 The Process for Multi-Attribute Utility Model

9.4.1 Defining the Goals

The research team identified the goal as selecting the preferred alternative that will be cost effective and will meet the system capability requirements for ITS asset management in South Carolina. As part of this goal, the model's objectives were to independently analyze user friendliness and costs.

9.4.2 Selection of MOE

The selected MOEs were those best suited to evaluate the three competing systems. The lists of the MOEs that will be used for the multi-attribute utility analysis are listed in the textbox below.

Measures of Effectiveness

1. Map Viewing Capability
2. Visual Representation of Spatial Query
3. Visualization of Fiber Trace and Connectivity of the Fibers
4. Customized ITS Symbology for Enhanced Visualization
5. Wireless Network Visualization
6. Data Recovery and Retrieval Strength
7. Single Administrator Control
8. Ease of Use of the Software
9. Customized Import Functionality (out of box)
10. Customized Import Functionality (supporting user specific customization)
11. Web Based Applicability
12. Field Update/Usage Support
13. Restricted Data Access Capabilities
14. Support to Enterprise Environment
15. Cost of Personnel
16. Cost of Software
17. Cost of Operation and Maintenance

For the analysis based solely on system capabilities, MOEs 1-14 were used, whereas 1-17 were used for the analysis where system capabilities and the costs were both considered. Costs considerations involved MOEs that assessed the cost of using the three different systems.

9.4.3 Defining Alternatives

The alternatives are the systems to be evaluated stated in the previous section. The alternatives for ITS asset management system are:

- NexusWorx (a representative of customized ITS AM system)
- Enterprise Based GIS (a representative of GIS based ITS asset management systems)
- Microsoft Access (a representative of typical database management systems)

Nexusworx is considered to be an alternative because it represents a customized ITS asset management system (ITS Facility Management System Product Evaluation, FDOT 2006). The Enterprise based GIS is considered because the users of the ITS asset management systems will be from mostly DOTs and public agencies. This software is a natural selection because most agencies already have an Enterprise based GIS system for other types of projects, infrastructure, or assets. Through some additional plug-ins, enterprise GIS systems could be a potential ITS asset management tool. Microsoft Access was considered an alternative because it is a well-known database management tool, user friendly, and already owned by the SCDOT in many offices.

9.4.4 Implementing Multi-Attribute Utility Analysis

The multi-attribute analysis consisted of several steps. First, the rating of each MOE was assigned, indicating which characteristics of asset management tools were most valuable to practitioners. A utility equation was developed for each alternative (software), and the analysis was conducted based on the utility and the performance rating of the MOEs. The multi-attribute utility analysis was performed on the two communication network system scenarios presented earlier: existing (wired) and the proposed communication network (wireless) system. Thus, this analysis will provide recommendations for asset management tools for wired systems and wireless systems. The following subsections provide further details on the methods used in the analysis.

9.4.4.1 *Assigning Utility Values of the MOEs*

The utility values of the MOE's were extracted from the results of the nationwide survey of ITS engineers, database managers, and GIS experts. The survey questionnaire is demonstrated in Appendix G. The survey was collected from DOTs and other government agency participants. They rated these factors on a scale of 0-10 based on their perception of the importance of each factor in an asset management system for ITS, where 10 represented the highest importance and 0 the lowest. Once the survey was completed the data was transformed into the utility values of the factors where the sum of all values added to one. For the analysis where only the system capabilities were considered, the utility component contains 14 MOEs according to equation 9.1. The utility for the analysis where the system capabilities and the costs were considered consists of 17 MOEs according to equation 9.2. Note that the numbering of these utilities is consistent with the order of the measures of effectiveness presented in the textbox in section 9.4.2.

$U_1+U_2+U_3+U_4+U_5+U_6+U_7+U_8+U_9+U_{10}+U_{11}+U_{12}+U_{13}+U_{14}=1$ (**Equation 9.1)**

$U_1+U_2+U_3+U_4+U_5+U_6+U_7+U_8+U_9+U_{10}+U_{11}+U_{12}+U_{13}+U_{14}+U_{15}+U_{16}+U_{17}=1$

(Equation 9.2)

9.4.5 Multi-Attribute Utility Analysis

The overall utility for each alternative was calculated using equation 9.3 for the analysis of only the system capabilities. Equation 9.4 was used for calculating the overall utility for the analysis where both the system capabilities and the costs were considered. While the utility values were based on survey results, the performance measures (PR) were rated by the evaluation team.

MUA= U1PR1+U2PR2+U3PR3+U4PR4+ U5PR5+ U6PR6+ U7PR7+U8PR8+ U9PR9+ U10PR10+U11PR11+U12PR12+U13PR13+U14PR14 (**Equation 9.3)**

MUA=U1PR1+U2PR2+U3PR3+U4PR4+U5PR5+U6PR6+U7PR7+U8PR8+U9PR9 +U10PR10 +U11PR11+U12PR12+U13PR13+U14PR14+U15PR15+U16PR16+U17PR17 (.**Equation 9.4)**

The following textbox defines the variables in equations 9.3 and 9.4.

PR_1 = Performance Measure of Visualization Quality of Map Viewing Capability
PR_2 = Performance Measure of Visualization Quality of Spatial Query
PR_3 = Performance Measure of Visualization Quality of fiber trace and connectivity of the fibers
PR_4 = Performance Measure of Visualization Quality of Customized ITS Symbology Quality for Enhanced Visualization
PR_5= Performance Measure of Visualization Quality of Wireless Network Depiction
PR_6= Performance Measure of the Quality of Data Recovery and Retrieval System
PR_7= Performance Measure of the Quality of Single Administrator Control
PR_8= Performance Measure of the Quality of Ease of Use of the Software
PR_9= Performance Measure of the Quality of Customized Import Functionality (straight out of the box)
PR_{10}= Performance Measure of the Quality of Customized Import Functionality (supporting user specific customization)
PR_{11} = Performance Measure of the Capability to Support the Web Based Application
PR_{12} = Performance Measure of the Capability to Support Field Updates/Usage
PR_{13} = Performance Measure of the Capability to Restrict Data Access
PR_{14} = Performance Measure of the Capability to Support Enterprise Environment
PR_{15} = Performance Measure of the Capability to Minimize the Cost of Personnel
PR_{16}= Performance Measure of the Capability to Minimize the Cost of Software
PR_{17}= Performance Measure of the Capability to Minimize the Cost of Operation and Maintenance
MUA = Total Multiple Measure Utility of Alternative ‘A’
U_i = Utility of the ith utility

Based on the overall utility, the best alternative was selected. The alternative with the maximum overall utility will be the system that best meets the asset management system’s requirements.

9.5 ASSET MANAGEMENT SYSTEM ANALYSIS FINDINGS

The systems were evaluated by comparing the relative performance of each with regard to meeting the requirements set for an ITS asset management system as previously described.

9.5.1 Evaluation Based on System Capabilities

The system capabilities were rated based on their relative performances to achieve the requirements of an ITS asset management system. A scale of 0-5 was used to rate the systems for each MOE. The system received a 0 if the requirement could not be met and 5 when it could meet the requirement completely. The three different asset management systems were also evaluated in terms of their licensing fee, operation and maintenance costs. The comparison of the NexusWorx, Enterprise based GIS, and Microsoft Access is shown in Table 25. The MOEs that are related to system capabilities were evaluated through research based on the case study of a proposed wireless network integrated with an existing wired communication network and ITS assets. ITS assets included cameras, radars, HUB, DMS etc. The following sub sections address the evaluation outcomes.

Table 25 Relative Ratings for User Friendliness and ITS Suitability

MOE		Relative Rating		
		NexusWorx	Enterprise based GIS	Microsoft Access
Visualization	Map Viewing Capability	**3**	**5**	0
	Spatial Query	5	5	0
	Fiber Trace and Connectivity of the Fibers	5	5	0
	Customized ITS Symbology	5	5	0
	Wireless Network Visualization	5	5	0
Data Management and Applicability	Data Recovery and Retrieve	5	5	3
	Single Administrator Control	**3**	**5**	1
User Symbology	Ease of Use of the Software	**4**	**3**	3
	Customized Import Functionality[1]	4	4	1
	Customized Import Functionality[2]	**3**	**5**	0
Remote Access	Web Based	**5**	**3**	2
	Field Updating/Usage	5	5	0
	Restricted Data Access Capability	5	5	0
Enterprise Capability	Multiple User Supporting Capability	5	5	1

[1] (Straight out of the box)
[2] (Supporting user specific customization)

9.5.1.1 *Visualization*

NexusWorx and Enterprise based GIS have similar capabilities to support map viewing and spatial query visualization, however Microsoft Access is not able to support these functions. Depicting fiber trace and representing connectivity in a visual form, NexusWorx has customized tools to perform this fiber connectivity and tracing function. Enterprise based GIS can have this functionality with some plug-in tools designed for communication utility comapies.

Customized ITS symbology is a very important feature for any ITS asset management system because it allows standardized icons and tools for ITS system components. This also allows the icons to convey the same meaning throughout the agency and between personnel involved with ITS assets. NexusWorx has a built-in ITS customized symbology and Enterprise based GIS has some additional plug-ins so this customization can also be performed. Along with the plug-ins, the icons and tools for ITS assets need to be standardized in the Enterprise based GIS.

Wireless network visualization is important in ITS asset management systems. Based on the wireless communication case study, the ITS asset management systems were tested and evaluated to observe whether they can support this capability. NexusWorx supports wireless network visualization completely but Enterprise based GIS again will require modifications and customized codes to support this requirement. For Enterprise based systems existing in the public agencies it was assumed that these modifications will be performed effortlessly utilizing existing GIS expertise. Microsoft Access doesn’t have any means to support fiber trace, connectivity of fibers, ITS customized symbology or wireless network visualization.

9.5.1.2 *Data Management and Applicability*

Data recovery and retrieval is important in an asset management system. In case of system failure or lost data, recovery is paramount. A centralized database system is vital in such a case where all the users share the same database and it is stored centrally so that every user does not need to back up the data. NexusWorx and Enterprise Based GIS support this function; Microsoft Access will require some additional improvement to utilize this function completely.

Another important issue with multiple users accessing the same database is that there is a possibility that the data will be overwritten. Due to this issue the system has to have an administrator to validate the data before it gets updated. This protocol will enable data validation so the probability of having errors in the database will be minimized. All systems need to modify the database updating principle to address this requirement.

9.5.1.3 *User Interface*

NexusWorx being customized as an ITS focused system, is definitely more user friendly than other systems. However, enterprise based GIS systems can be made more user-friendly with some customization. Microsoft Access was found to be comparatively less user friendly as compared to the above two systems.

The learning curve is a very important issue because if the system requires a lot of time and effort to be proficient with it then eventually it will be hard to implement. NexusWorx is a simple ITS asset focused system so the average personnel with a little exposure to this system will be able to efficiently use the system. In general GIS is a complex system and more training is needed than NexusWorx to develop an expertise. In an Enterprise based GIS system the time requirement for training could be minimized if it is customized for an ITS asset management system. However, depending on the current use of enterprise based system, users may already be familiar with tools and layout. Microsoft access is a relatively easy system regarding the time requirement to be proficient to use the system compared to NexusWorx and Enterprise based GIS but will not perform as many functions.

This MOE was further divided into two categories; existing system straight out of the box and the other one that will support the user defined customization. Customized import functionality for straight out of the box will allow the system to use that data in a variety of formats because often the input data is in various formats rather than one single type. This capability is essential when the system is required to import the database from other sources and create a whole new database. It is much more efficient to use existing data formats used by an agency. NexusWorx and Enterprise based GIS supports a variety of import file/data types but Microsoft Access does not have this capability. NexusWorx and Enterprise based GIS both support all the required variety of import file types that are required for the applications. Enterprise based GIS supports user defined customization whereas NexusWorx would require adding this functionality on top of the existing system.

9.5.1.4 *Remote Access*

Most agencies prefer a web based system because it requires less software components and easy access from anywhere with a simple internet connection. NexusWorx is a web based system and Enterprise based GIS might require the system administrator to put the software into the central network to allow a web based accessible system.

Field updating is important during maintenance work or while upgrading ITS assets. NexusWorx and Enterprise based GIS both support this criteria however Microsoft Access was not capable of meeting this requirement.

Both NexusWorx, and Enterprise based GIS with some modification of the system, were able to support the privilege based hierarchical database access. However Microsoft Access was not able to support this.

9.5.1.5 *Enterprise Capability*

In many instances, multiple users may access the system simultaneously. NexusWorx being a enterprise based system, will support this feature along with the Enterprise based GIS. Microsoft Access fails to meet this requirement.

9.5.2 Cost Evaluation

The cost evaluation was performed by converting the estimated cost of the systems into relative rating values to be used in the multi-attribute utility models. The costs of the systems are summarized in Table 25 and 26. NexusWorx cost components were obtained from the vendor of NexusWorx. The cost of Microsoft Access was not considered as this system was base line and only studied for the system capabilities. Cost for SDEGIS came from ESRI. The personnel and operation and maintenance costs were obtained by consulting SCDOT. In Table 26 the personnel, licensing and operations and maintenance costs were presented as capital costs and annual costs. The cost components were then converted to annual costs as presented in Table 27.

Table 26 Annual and Capital Costs for Different Options

Cost ($ 1,000s)	**NexusWorx**		**Enterprise Based GIS**		**Microsoft Access**
	(Vendor Hosting)	(Client Server set up)	(New Setup)	(Add-on to Existing Setup)	
Personnel	0	0	60 to 80 (A)	0	NA
Software Licensing	60 to 80 (A)	180 to 200 (C)	40 to 60 (C) 10 to 15 (A)	100 to 300 (A)	NA
O&M	0	25 to 35 (A)	40 to 60 (A)	0	NA

(A) Annual cost
(C) Capital Cost

Table 27 Annual Costs for Different Options

Cost (5 year period) ($1,000s)	**NexusWorx**		**Enterprise Based GIS**		**Microsoft Access**
	(Vendor Hosting)	(Client Server set up)	(New Setup)	(Add-on to Existing Setup)	
Personnel	0	0	60 to 80[1]	0	NA
Software Licensing	60 to 80[2]	39 to 44[3]	18 to 28[4]	100 to 300[5]	NA
O&M	0	25 to 35[6]	40 to 60[7]	0	NA

[1] yearly salary of $60,000-$80,000

[2] 20 users each $3,000-$4,000

[3] an inflation rate of 3% for a 5 year period with a capital cost of $180,000-$200,000

[4] an inflation rate of 3% for a 5 year period with a capital cost of $40,000-$60,000 and an annual cost of $10,000-$15,000

[5] an inflation rate of 3% for a5 year period with a capital cost of $100,000-$300,000

[6] it is 20% of license cost for software licensing fee

[7] yearly salary of $40,000-$60,000

In Table 26, different system deployment options with their standard price are presented. Price may vary with factors such as time of purchase and type of contract agreements. For deploying NexusWorx, there were two options; vendor hosting and client server setup. In the vendor hosting setup, the database and server are provided and maintained by the vendor and the client only needs to purchase the license to use the system for an annual fee. The client server setup option has an initial setup cost where the agency will own their server and database system and will be responsible to maintain the servers.

In the vendor hosting option, there are two versions: The Editor and Viewer. The Editor user has access to all functionality and can be used to edit or modify all features and connectivity. The Viewer can be used to perform some attribute editing that allows a user to effectively modify device information, such as model number, serial number, and installed date. Each editor version costs $3,000-$4,000 per year for vendor hosting and each viewer version costs $1,600 per year. In the client server setup system each editor costs $10,000 (up to 10 users) and $7,000 (up to 20 users). Each viewer costs $3,500 (up to 10 users) and $2,700 (up to 20 users). In this evaluation, it was assumed that 20 users were needed with the editor version. Additionally, for the client server setup 20% of the total licensing fee will be charged as the annual fee for maintenance. For the yearly cost estimation, an inflation rate of 3% was used to convert them to present worth values. Detailed cost information for NexusWorx is attached in Appendix D.

For the Enterprise based GIS system, there are two options: First, a scenario where an agency does not own its Enterprise based GIS system and has to purchase an Enterprise based GIS system and needs to hire personnel to operate, maintain and use the GIS based system. This option is expensive and an inflation rate of 3% was considered for the personnel, and operation and maintenance costs. The cost for the software licensing was obtained from the ESRI and the system costs $40,000-$60,000 for the first year and $10,000-$15,000 per year every year after.

The second scenario is when the agency already owns a GIS server. In this scenario, the DOT is using the system for other asset management purposes and keen to adopt a centralized database system, with the ITS AM system as an additional layer on their existing Enterprise based GIS system. Intergraph Corporation was contacted for the standard pricing because many public agencies rely on this company for their utility management purposes and the pricing will reflect integrateable components with the existing SCDOT system. Additional resources might be required beyond the cost estimate so internal personnel can customize Enterprise based GIS for managing ITS assets. From the Intergraph Corporation, the price for software licensing was $5,000-$15,000 for each annual license. The authors considered 20 users for 5 years for the analysis.

Based on the cost, a linear approach was used to translate these costs into relative ratings for each system. This was done to transfer cost values into the same scale as that of the system capabilities so these cost components can feed into the multi-attribute utility analysis. Table 28 presents the basis for converting the cost components into relative ratings and Table 29 shows the calculated relative ratings for each system regarding costs.

Table 28 Cost and Relative Ratings

Cost (2009 US $)	Relative Rating
<10,000	5
10,000-29,999	4
30,000-49,999	3
50,000-69,999	2
>70,000	1

Table 29 Relative Rating for Costs of Alternative Software

Relative Rating	NexusWorx		Enterprise Based GIS		Microsoft Access
	(Vendor Hosting)	(Client Server set up)	(New Setup)	(Add-on to Existing Setup)	
Personnel	5	5	1.5	5	NA
Software Licensing	2	3	4	1	NA
O&M	5	3.5	3.5	5	NA

9.5.3 Performance Rating for the MOEs

Illustrated in Table 30, the performance ratings (defined as PR in the utility equations) for the case study are presented. For multi-attribute utility analysis two components were required: one is the performance rating for the attributes and the other is the utility value of each attribute. The performance ratings were derived from the case study analyzed by field experts and the utility values came from survey responses of public agency personnel.

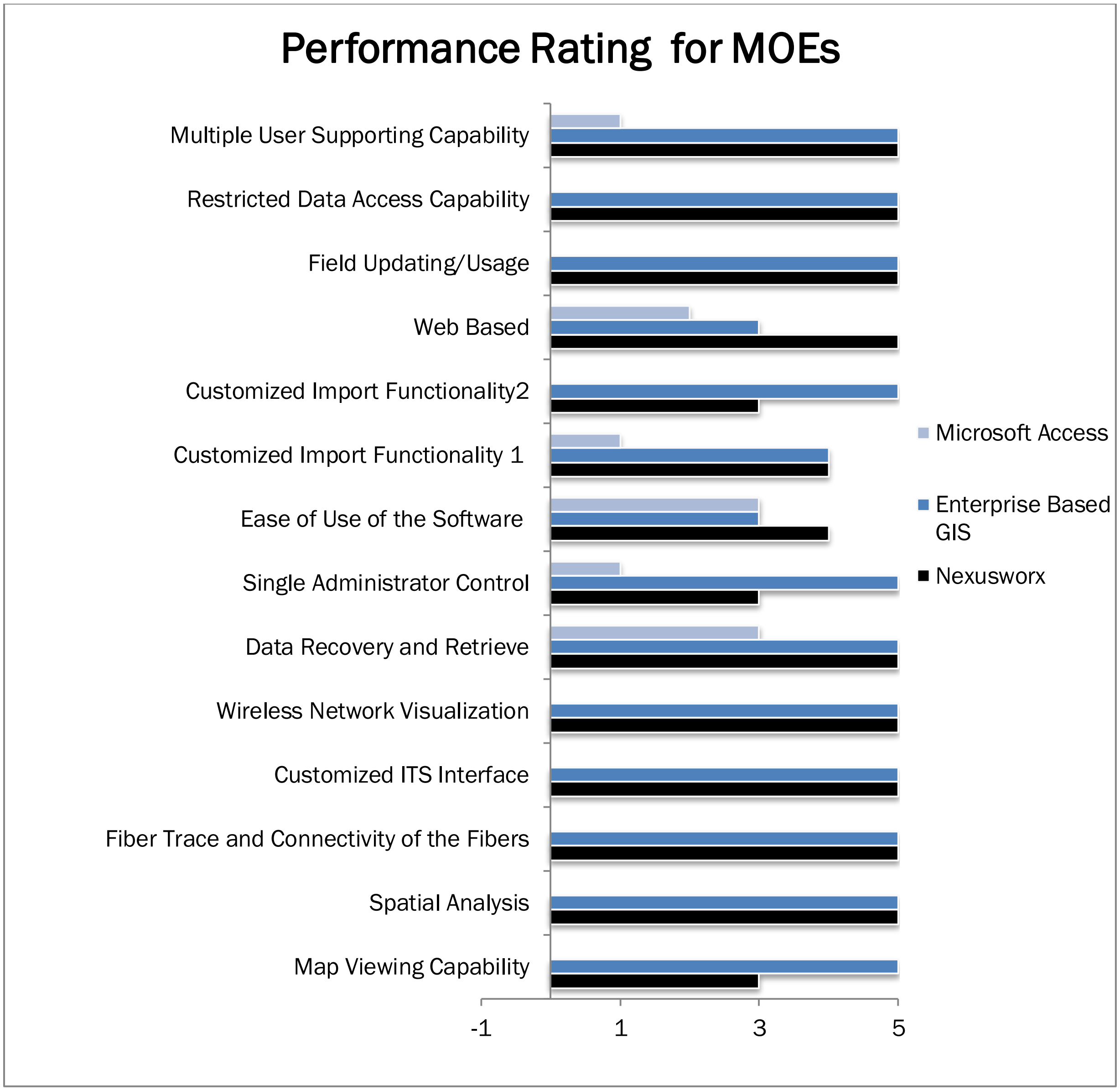
Table 30 Performance Rating for MOE's for Wireless Communications

MOE		Performance Rating (PR)		
		NexusWorx	Enterprise based GIS	Microsoft Access
Visualization	Map Viewing Capability	3	5	0
	Spatial Query	5	5	0
	Fiber Trace and Connectivity of the Fibers	5	5	0
	Customized ITS Symbology	5	5	0
	Wireless Network Visualization	5	5	0
Data Management and Applicability	Data Recovery and Retrieve	5	5	3
	Single Administrator Control	3	5	1
User Interface	Ease of Use of the Software	4	3	3
	Customized Import Functionality[1]	4	4	1
	Customized Import Functionality[2]	3	5	0
Remote Access	Web Based	5	3	2
	Field Updating/Usage	5	5	0
	Restricted Data Access Capability	5	5	0
Enterprise Capability	Multiple User Supporting Capability	5	5	1

[1](Straight out of the box)

[2](Supporting user specific customization)

In Figure 60, the performance ratings for the MOEs are presented. The performance rating was set on a scale of zero to five. In this rating five represents the maximum performance of the system that will fully satisfy the MOE, and zero represents the lowest performance.



1=Straight out of the box
2= Supporting user specific customization

Figure 61: Performance Rating (PR) for the MOEs

9.5.4 The Utilities of MOE’s

The utilities of the MOE’s are based on the rating from survey responses. A nationwide survey was conducted and responses from VDOT, TDOT, MnDOT, NCDOT, SCDOT and WsDOT were received. Two scenarios were considered while performing the analysis and the utilities were assigned accordingly. In one scenario, only system capabilities were considered and cost was ignored. In another scenario, both system capabilities and cost was considered.

9.5.4.1 *Evaluation on System Capabilities*

This scenario evaluated only system capabilities of selected ITS asset management systems and did not include costs. The utilities related to system capabilities of related MOEs add up to 1 under this scenario, shown in Table 31. Note that these utilities correspond to those previously presented in equation 9.1 and the values represent how important each characteristic was to survey respondents, where a higher value indicated more importance.

Table 31 The Utilities for the MOE Considering System Capabilities

MOE	Utility (U)
U_1 Map Viewing	0.0714
U_2 Spatial Query Visualization	0.0714
U_3 Fiber Trace and Connectivity	0.0769
U_4 Customized ITS Symbology	0.0678
U_5 Wireless Network Visualization	0.0549
U_6 Data Recovery and Retrieval	0.0733
U_7 Single Administrator Control	0.0678
U_8 Ease of Use	0.0788
U_9 Customized Import Functionality[1]	0.0733
U_{10} Customized Import Functionality[2]	0.0549
U_{11} Web Based System	0.0806
U_{12} Field Update and Usage	0.0751
U_{13} Restricted Data Access Capabilities	0.0751
U_{14} Multi-User Accessibility Simultaneously	0.0788
Total	**1.0000**

[1](Straight out of the box)

[2](Supporting user specific customization)

9.5.4.2 *Comprehensive Evaluation*

This scenario evaluated system capabilities along with the cost of license, operation and maintenance of selected ITS asset management systems. The utility related to the system capabilities along with cost components related MOEs add up to 1 under this scenario, shown in Table 32. Refer to equation 9.2 for the utility equation using these measures of effectiveness.

Table 32 Utilities for the MOE (Considering Costs)

MOE	Utility (U)
U_1 Map Viewing	0.0457
U_2 Spatial Query Visualization	0.0457
U_3 Fiber Trace and Connectivity	0.0492
U_4 Customized ITS Symbology	0.0434
U_5 Wireless Network Visualization	0.0352
U_6 Data Recovery and Retrieval	0.0469
U_7 Single Administrator Control	0.0434
U_8 Ease of Use	0.0504
U_9 Customized Import Functionality[1]	0.0469
U_{10} Customized Import Functionality[2]	0.0352
U_{11} Web Based System	0.0516
U_{12} Field Update and Usage	0.0481
U_{13} Restricted Data Access Capabilities	0.0481
U_{14} Multi-User Accessibility Simultaneously	0.0504
U_{15} Cost of Personnel	0.1000
U_{16} Cost of Software Licensing	0.1600
U_{17} Cost of Operation of Maintenance of the System	0.1000
Total	**1.0000**

[1](Straight out of the box)

[2](Supporting user specific customization)

9.5.5 Total Utility

Total utility for a system is estimated by multiplying each performance rating (PR_i) with respective utility (U_i) and then summing them up. The following subsections present the multi-attribute utility analysis based on system capability evaluation and comprehensive evaluation.

9.5.5.1 *Multi-Utility Analysis for Alternatives (Considering Only System Capabilities)*

The multi-attribute utility value determined by considering system performance is presented in Table 33. Highlighted values represent the maximum value of utility (U) and performance rating (PR) for each MOE among the systems. Refer to equation 9.3 when reviewing calculations. In these calculations, a higher utility indicates a more-preferable alternative.

Table 33 Multi-Attribute Utility Analysis (Considering System Capabilities)

MOE	**Utility (U)**	**NexusWorx**		**Enterprise based GIS**		**Microsoft Access**	
		PR*	U*PR	PR	U*PR	PR	U*PR
Map Viewing Capability	0.07	3	0.21	5	0.36	0	0.00
Spatial Query	0.07	5	0.36	5	0.36	0	0.00
Fiber Trace and Connectivity of the Fibers	0.08	5	0.38	5	0.38	0	0.00
Customized ITS Symbology	0.07	5	0.34	5	0.34	0	0.00
Wireless Network Visualization	0.05	5	0.27	5	0.27	0	0.00
Data Recovery and Retrieve	0.07	5	0.37	5	0.37	3	0.22
Single Administrator Control	0.07	3	0.20	5	0.34	1	0.07
Ease of Use of the Software	0.08	4	0.32	3	0.24	3	0.24
Customized Import Functionality	0.07	4	0.29	4	0.29	1	0.07
Customized Import Functionality	0.05	3	0.16	5	0.27	4	0.22
Web Based	0.08	5	0.40	3	0.24	2	0.16
Field Updating/Usage	0.08	5	0.38	5	0.38	0	0.00
Restricted Data Access Capability	0.08	5	0.38	5	0.38	0	0.00
Enterprise Capability	0.08	5	0.39	5	0.39	1	0.08
Total	1.00	-	**4.46**	-	**4.61**	-	**1.06**

*PR stands for performance rating

Sample Calculations

$MU_{NexusWorx}$= 0.071*3+0.071*5+0.077*5+0.068*5+0.055*5+0.073*5+0.068*3

+0.079*4+0.073*4+0.055*3+0.081*5+0.075*5+0.075*5+0.079*5

$MU_{NexusWorx}$=4.46 Total Utility (for Vendor hosting and Client Server Setup)

MU_{SDEGIS}= 0.071*5+0.071*5+0.077*5+0.068*5+0.055*5+0.073*5+0.068*5

+0.079*3+0.073*4+0.055*5+0.081*3+0.075*5+0.075*5+0.079*5

MU_{SDEGIS}=4.61 Total Utility (for New Setup and In Addition to Existing Setup)

$MU_{MicrosoftAccess}$= 0.071*0+0.071*0+0.077*0+0.068*0+0.055*0+0.073*3+0.068*1

+0.079*3+0.073*1+0.081*2+0.075*0+0.075*0+0.079*4+0.055*1

$MU_{Microsoft\ Access}$ =1.06 Total Utility

9.5.5.2 *Multi-Utility Analysis for Alternatives (Considering Comprehensive Evaluation)*

Both system capabilities and costs were considered in this analysis. The total multi utility for each alternative was calculated based on equation 4. Table 34 shows the multi-utility analysis findings from this scenario. See equation 9.4 for details about the calculations provided in the textbox. Note that Microsoft Access was not included in this analysis because it performed poorly in the previous analysis and the researchers considered it infeasible.

Table 34 Multi-Attribute Utility Analysis (Considering Comprehensive Evaluation)

MOE	Utility (U)	NexusWorx				Enterprise based GIS			
		Vendor Hosting		Client Server		New System		Existing System	
		PR	U*PR	PR	U*PR	PR	U*PR	PR	U*PR
Map Viewing Capability	0.046	3	0.137	3	0.137	5	0.229	5	0.229
Spatial Query	0.046	5	0.229	5	0.229	5	0.229	5	0.229
Fiber Trace and Connectivity of Fibers	0.049	5	0.246	5	0.246	5	0.246	5	0.246
Customized ITS Symbology	0.043	5	0.217	5	0.217	5	0.217	5	0.217
Wireless Network Visualization	0.035	5	0.176	5	0.176	5	0.176	5	0.176
Data Recovery and Retrieve	0.047	5	0.234	5	0.234	5	0.234	5	0.234
Single Administrator Control	0.043	3	0.130	3	0.130	5	0.217	5	0.217
Ease of Use of the Software	0.050	4	0.202	4	0.202	3	0.151	3	0.151
Customized ITS Interface[1]	0.047	4	0.188	4	0.188	4	0.188	4	0.188
Customized ITS Interface[2]	0.035	3	0.105	3	0.105	5	0.176	5	0.176
Web Based	0.052	5	0.258	5	0.258	3	0.155	3	0.155
Field Updating/Usage	0.048	5	0.240	5	0.240	5	0.240	5	0.240
Restricted Data Access Capability	0.048	5	0.240	5	0.240	5	0.240	5	0.240
Enterprise Capability	0.050	5	0.252	5	0.252	5	0.252	5	0.252
Cost of Personnel	0.1	5	0.500	5	0.5	1.5	0.15	5	0.500
Cost of Software Licensing	0.16	2	0.320	3	0.48	4	0.64	1	0.160
Cost of Operation and Maintenance of the System	0.1	5	0.500	3.5	0.35	3.5	0.35	5	0.500
Total	1	-	**4.174**	-	**4.184**	-	**4.089**	-	**4.109**

Sample Calculations

$MU_{NexusWorx}$= 0.046*3+0.046*5+0.049*5+0.043*5+0.035*5+0.047*5+0.043*3+0.050*4 +0.047*4+0.050*3+0.052*5+0.048*5+0.048*5+0.035*5+0.1*5+0.16*2+0.1*5

$MU_{NexusWorx}$=4.174 Total Utility (Vendor Hosting System)

$MU_{NexusWorx}$= 0.046*3+0.046*5+0.049*5+0.043*5+0.035*5+0.047*5+0.043*3+0.050*4 +0.047*4+0.050*3+0.052*5+0.048*5+0.048*5+0.035*5+0.1*5+0.16*3+0.1*3.5

$MU_{NexusWorx}$=4.184 Total Utility (Client Server Setup)

MU_{SDEGIS}=0.046*5+0.046*5+0.049*5+0.043*5+0.035*5+0.047*5+0.043*5+0.050*3+0.047*4 +0.050*5+0.052*3+0.048*5+0.048*5+0.035*5+0.1*1.5+0.16*4+0.1*3.5

MU_{SDEGIS}=4.089 Total Utility (New Setup)

MU_{SDEGIS}=0.046*5+0.046*5+0.049*5+0.043*5+0.035*5+0.047*5+0.043*5+0.050*3+0.047*4 +0.050*5+0.052*3+0.048*5+0.048*5+0.035*5+0.1*5+0.16*1+0.1*5

MU_{SDEGIS}=4.109 Total Utility (In addition to Existing Setup)

9.6 SUMMARY OF MULTI-UTILITY ANALYSIS FOR ALTERNATIVES

1. From the capability analysis it was clear that Enterprise based GIS outperformed the other alternatives in satisfying the selected measures of effectiveness for an ITS asset management system. NexusWorx was the next best system, also performing well yet rated lower. Microsoft Access performed poorly in the evaluation because it only reflected the base line condition.
2. For the comprehensive analysis, both NexusWorx and Enterprise based GIS had utility values very close to each other. Comparing the cost and system capabilities, it was evident that if any agency has an Enterprise based GIS system deployed for managing other assets, adding a layer on top of an existing system might be a preferred choice. This would also allow the agency to maximize the utility of existing base maps and data currently residing in the existing system. However, if any agency does not have an Enterprise based GIS system, then they might either choose a customized ITS asset management tool such as Nexusworx or initiate an Enterprise based GIS system.

The multi-attribute analysis is summarized in Table 35 and the summary is graphically presented in Figure 61.

Table 35 Summary of the MUA for the Alternatives

	Considering System Capabilities Evaluation (Total Utility)	Considering Comprehensive Evaluation (Total Utility)
NexusWorx (Vendor Hosting)	4.46	4.174
NexusWorx (Client Server System)	4.46	4.184
Enterprise Based GIS (New Setup)	4.61	4.089
Enterprise Based GIS (In Extension to Existing Setup)	4.61	4.109
Microsoft Access	1.06	NA

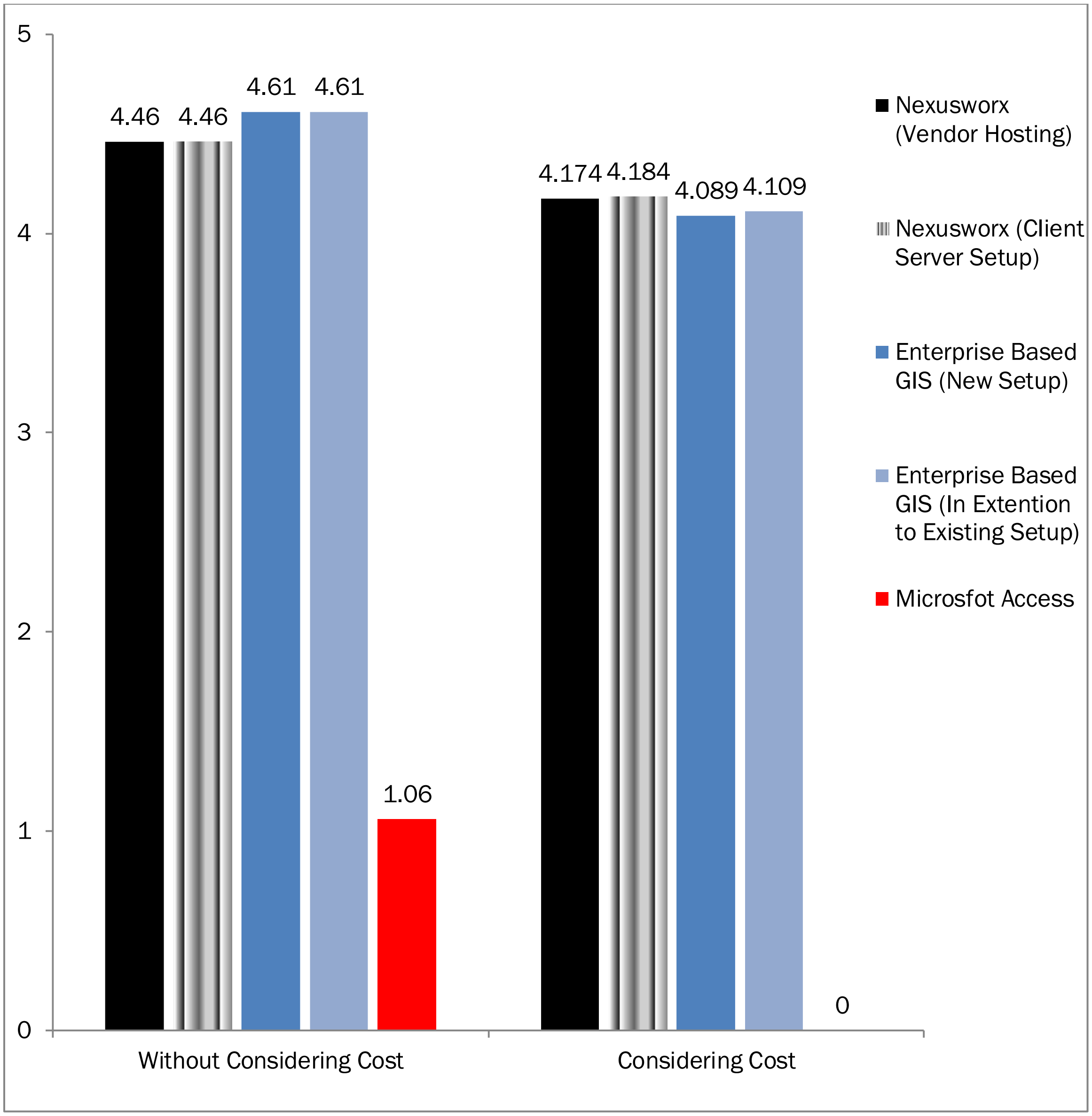


Figure 62 Summary of Multi-Attribute Utility Analysis

10 IMPLEMENTATION STRATEGY

The goal of this implementation strategy, presented in Appendix E, is to summarize the most important characteristics in selecting the technology alternatives, the major steps used in designing the wireless sensor networks, the key factors that need to be considered connecting sensors in the field or the field to the TMC, and to identify possible sources of opportunities and concerns within the implementation process.

11 CONCLUSIONS AND RECOMMENDATIONS

The Section first presents conclusions developed based upon the study results. The second part of this Section presents recommendations for utilizing the research results and future research need to be done in this area.

11.1 Conclusions

The authors conducted a systematic study and analysis of the performance, reliability and cost-effectiveness of three wireless technologies: Wi-Fi, WiMAX and DSRC. These three technologies are all closely related to on-line traffic surveillance and were evaluate through literature review, survey of public agencies, field study and simulation analysis. The focus of this study was on the communication between roadside traffic control devices, and between devices and TMCs.

Survey responses revealed that public agencies are using Wi-Fi, cellular services provided by commercial carriers, state owned and operated microwave systems and even WiMAX. The responses also illustrated an interest among public agencies concerning the use of WiMAX for providing communication between ITS devices and centers. However, these agencies reported a need for reliability and performance assessment of the available options in relation to requirements. Moreover, the interview responses revealed that these agencies have had positive experiences and strong interest in future expansion with wireless technologies, such as Wi-Fi and WiMAX. This interest is because of the broadband capabilities and potential cost-effectiveness of such technologies. Respondents expressed interest in exploring the feasibility and possible costs of building state- owned wireless infrastructures for traffic surveillance and monitoring.

A case study conducted based on the existing traffic surveillance networks in seven metropolitan cities in South Carolina provided an excellent opportunity to study the process of designing a wireless network. The study interfaced cameras and traffic sensors with one another and with the existing ITS backbone. This case study also addressed the use of Wi-Fi and WiMAX technologies to cover the region adequately and support the required surveillance performance. It also allowed for the comparison between Wi-Fi and WiMAX architectures when dealing with a relatively sparse camera density.

11.1.1 Wi-Fi Field Tests

The authors selected saturated throughput, successful delivery ratio, received signal strength and signal-noise-ratio as parameters for evaluating performance and reliability of a wireless traffic sensor network.

A Wi-Fi (802.11g/b) field study revealed that when the wireless system operating at certain modulation rate, throughput first stays constant until a certain distance between a wireless transmitter and a receiver, and then starts to decrease. For most modulation rates, the drop occurs between 300 ft to 400 ft between a transmitter and a receiver. Beyond this distance, the noise over the communication link significantly increases so the communication performance significantly degrades and becomes very unreliable as most packets are dropped.

These findings imply that when traffic agencies implement wireless sensor networks in the field, traffic sensors nodes should be deployed within a distance that can be supported at a specific chosen modulation rate to ensure reliable effective data transmission for traffic management. Field tests are needed for each deployment location to identify this distance threshold. Moreover, higher modulation rates provide higher throughput, however less tolerance to the background noise and interference, which results in a less successful delivery ratio. Setting modulation rates as automatic in practice does not necessarily provide the best balance between system throughput and delivery ratio.

Traffic agencies need to conduct similar field tests before implementation to identify which modulation rate and transmission power the system should be operating at to meet the performance requirements for specific applications.

11.1.2 WiMAX Field Tests

Two types of WiMAX field experiments, fixed and nomadic applications, revealed that achievable throughput were within ranges from1.414 Mbits/sec to 5.489 Mbits/sec in a typical highway environment. This means that it can support typical traffic sensor data requirements between 64 and 384 Kbits/sec.

The nomadic experiments related to the coverage suggested that LOS greatly affects the connectivity level. Moreover, as an emerging technology, the capabilities and the performance of WiMAX network sometimes are affected by the characteristics of the client radio. Traffic agencies need to test the performance of different radio products before implementation to ensure the minimum communication requirements per unit could be satisfied.

A solar power configuration was also presented for WiMAX wireless supported traffic surveillance system examples. Given the power requirements of the traffic cameras and client radios, engineers can estimate the solar battery array requirements. The solar module, battery rating, regional sun rate and the available installation space for each unit affects the configuration design.

11.1.3 Video Quality and Wireless Communications

Besides the communication between field devices, this study also assessed the quality requirements of real-time traffic video data transmission over 802.11g wireless network as video is the most widely used tool for traffic monitoring. As an application of interactive video streaming, jitter and average packet rate were identified as important indicators of quality of real-time traffic monitoring over a wireless Internet connection, as reported in the literature.

Based on the experimental results, the authors found that jitter is highly correlated with the live video quality for a real-time traffic monitoring system. Higher jitter indicated greater chances of the video image being missed or the video link being disconnected. The study identified the tolerated jitter value to be one second. These threshold values ensure an acceptable video quality, which means smooth surveillance video with no frames skipped. Higher values will cause a video image being skipped, which affects the surveillance quality. A jitter value between 0.5 to 1 second will likely slow down the video transmitting. However, the value will not likely contribute to the skip of the frame, while higher values will cause skipped frames and discontinuous video.

To avoid jitter challenges, the value should be controlled within 1 second through applying a one second buffer size to minimize the discontinuity of surveillance video. Packet rate, another key factor of video quality, is suggested to be at least above the average value of 23 packets/ sec to ensure smooth video continuity for traffic surveillance. The field experiment related to video quality demonstrated that a 802.11g network is able to support one receiving computer with an average packet rate of 26 per second, providing an acceptable smooth traffic monitoring function. However, due to the limit of the overall link bandwidth and congestion in TCP, the network cannot support two receiving computers simultaneously with an acceptable video quality

11.1.4 Simulation Study

Other than field study, ns-2 simulation was utilized to analyze the performance of large scale wireless sensor networks appropriate for on-line traffic management, under differing expected error rates that may result from adverse conditions. The wireless sensor based traffic monitoring system is simulated and analyzed based upon two metrics: maximum achievable throughput and successful delivery ratio.

By setting the error rate to each communication link, the analysis showed that the communication network capacity decreases when the error rate increases and more packets begin to drop. This simulation analysis also found that within a wireless network, the numbers of relays required for data transmission affects performance of the network. At certain data rates, the achievable throughput of the furthest sensor is less than others due to the increased probability of more packets being dropped during transmission. Therefore, the number of relays needed for certain traffic control application needed to be carefully selected to ensure both the wireless connection and reliable performance. The implication of lesser relays is an increased number of required controllers that must have direct Internet connection.

While a major benefit of adopting wireless sensor networks is the reduction in the amount of wired connections needed for a system, this poses a trade-off between the cost of the system and the required bandwidth of a system. The saturating throughput for each sensor (camera) need not be maximized, especially the furthest one. Instead, it needs only to meet its specific throughput requirement. However, for key traffic infrastructure such as tunnels and bridges, traffic agencies might need to have a camera directly connected to TMC with a dedicated link to ensure the surveillance quality in adverse conditions. Moreover, simulation results indicates that with a 5% error rate, the saturating throughput dropped below 64 Kbps, which is far lower than the typical used traffic camera rate. The system will not support all cameras when any adverse condition causes more than 5% communication link error rate. This fact suggests that even for existing traffic cameras requiring very low data rates, traffic agencies must keep the error rates of the communication link within a certain threshold to ensure that every camera in the system is working properly.

11.1.5 Performance-Cost Analysis

For decision makers to select the best communication methods for a given location and application, the results of an economic analysis should accompany technical results. Performance-cost analysis indicated that the Wi-Fi infrastructure and mesh network had the same throughput to cost ratio. Considering the number of fiber drops needed, a Wi-Fi mesh solution has highest throughput-cost ratio for the Greenville traffic camera system, while the WiMAX mesh is the next best option. Without considering the cost of fiber connection, the WiMAX mesh was found to have higher throughput to cost ratio than WiMAX infrastructure. However, compared to infrastructure option, the mesh option has less expandability for future ITS devices deployment.

According to typical data rates of traffic cameras, both of the infrastructure-based network architectures provide a significant amount of excess bandwidth for use in supplying connectivity to future ITS components. The WiMAX infrastructure provides the greatest amount of excess bandwidth, which benefits any future expansion of the system. When several ITS devices located on a same location sending information simultaneously and sharing the bandwidth, WiMAX infrastructure can provide the most bandwidth upgrade space.

11.2 Recommendations

The recommendations are organized in three subsections: recommendations for use of this research and recommendations for future research and general recommendations.

11.2.1 Recommendations for Use of This Research

The following recommendations are made regarding the use of this research for wireless based on-line traffic management:

- The summary of key technical characteristics and factors of the three selected technologies could be utilized by state agencies and transportation engineers with a basic understanding of the opportunities and limitation regarding wireless network design, as well as the benefits and drawbacks of each of the three technologies.
- The procedure that was used in the field study can be utilized by practitioners to identify the achievable performance, such as throughput and delivery ratio in the field. At certain locations, the distance interval to locate traffic sensor, operational modulation rate and transmission power need to be identified to ensure effective traffic control and management prior to deployment. Furthermore, this study recommends important parameters to quantify the wireless communication performance and reliability.
- The results of the study on traffic video quality requirements could help transportation agencies in developing the specifications or design of a wireless-based video surveillance system. A threshold buffer size was recommended for an Internet-based real time traffic surveillance that would provide video smoothness without any significant delay for real-time use. Traffic agencies can minimize the jitter using the threshold buffer size proposed in this study to ensure effective traffic surveillance.
- The simulation study proposed a process that could be used by traffic agencies to measure throughput degradation for on-line traffic management operations. The quantitative measures of throughput degradation are essential for bandwidth planning of a wireless roadway traffic surveillance network designed for on-line traffic management as this signifies reliability of the network under different scenarios, such as different network topologies or adverse conditions. This issue must be resolved in the network deployment to ensure that each single communication link has the capability to support traffic data transmissions, especially when large bandwidths are required for large scale video surveillance.
- Performance-cost analysis provides a foundation for further investigation of the benefit-cost analysis of Wi-Fi and WiMAX wireless technologies under different network topologies. Findings from this research will benefit transportation agencies and other stakeholders in evaluating and selecting wireless

communication options and network topologies for various traffic control and management applications.

11.2.2 Recommendations for Future Research

The following recommendations are made for further research on the areas covered in this study:

- Future field studies should be conducted to quantify the effects of modulation rate and transmission power on received signal power in the field. This can provide a reference for traffic agencies to predict the possible performance in the field prior to the future ITS implementation.
- Future field test should also be conducted to look into the effects of the traffic volume on wireless communication performance in the field. This issue is very critical for the highly congested roadway area, where the traffic control devices are most likely to be deployed.
- Field studies should also be conducted to quantify the error rate caused by adverse environmental conditions, interference and topology. The error rate collected by field experiments can be input into simulations, as presented in this paper, to study the performance of a large scale wireless traffic sensor network.
- For the communication between field devices to the TMCs, future work should involve testing different jitter control mechanisms and acceptable buffer sizes that can guarantee smooth surveillance video transmission and effective on-line traffic management. Research should also evaluate important parameters related to the surveillance video quality of images received from multiple video sources through a wireless network and the Internet.
- Future simulation study needs to be conducted to assess both the traffic operation and communication performance of a wireless traffic sensor network. An integrated simulator platform should be developed for this purpose. Possible MOEs could be detection rate, false alarm rate and communication matrices. Communication matrices could include communication latency under different traffic conditions, such as during an incident or other emergency conditions. A vehicular traffic network could be created as a number of network files that define all aspects of a transportation system, including its roadway simulation network, geometrics, traffic control methods, ITS components, driver characteristics, and traffic volumes. Microscopic traffic data, such as flow, speed and occupancy could be collected and stored into individual sensor log files to compose advanced traffic management strategies for real time incident detection and clearance decisions. On the other side, a communication simulator could be used as a single executable file modeling individual network protocols and events occurring in each network protocol at each node. This would allow users to extend procedures into any protocol by inserting a code into the corresponding protocol source files

and recompiling the core. In the vehicular traffic simulator, each traffic sensor, detector or controller defined could be modeled as a node at a specified location in the communication simulator. In other words, the communication simulator is a logical extension of the vehicular traffic detector responsible for performing network-based operations. To model traffic sensor/controller network, such as incident detection and traffic control procedures, relevant algorithms could be inserted into one of communication simulator’s application layer module. On the other hand, data processing algorithms can be inserted either in vehicular traffic simulator or communication simulator, or both can model node-specific real-time procedures for a node. Nodes in communication simulator could achieve network consensus on detection and control decisions, which are to be conveyed back to the matching vehicular traffic detector through node-specific channel files. Locked-step execution of two simulators could be enforced to enable synchronized simulation

11.2.3 General Recommendations

- Multiple options are available to supplement SCDOT funding for ITS deployments. Researchers recommend that the SCDOT become more active in USDOT field operational tests and other demonstration projects. Although some of the tools deployed through these programs are not fully tested, such projects can provide the SCDOT with core infrastructure to leverage future expansions.
- Many ITS systems fight congestion problems and can thus contribute to mitigating transportation related emission issues. It is recommended that air quality improvement funds, such as Congestion Mitigation Air Quality, should be explored as potential funding sources for funding ITS projects.
- ITS systems can often serve additional roles in transportation security. Hence funding can be explored through the US Department of Homeland Security. This option is particularly attractive for surveillance systems such as those used to detect and verify traffic incidents.
- Researchers recommend that the SCDOT explore public-private partnerships such as resource sharing initiatives. Although these partnerships have traditionally focused on fiber optic and cellular communication, creativity could bring additional funding for ITS projects.
- To accelerate the deployment and benefits of ITS systems, many states have chosen to participate in pooled fund studies such as the IntelliDrive initiative, formerly known as vehicle-infrastructure-integration, or VII. The SCDOT should seriously consider becoming more actively involved in such programs, federal studies, and private-public partnerships; to increase the amount of non-traditional funding for ITS projects. These programs offer great opportunities to increase ITS infrastructure and capability at virtually no cost to the state.

12 REFERENCES

Aguayo, D., J. Bicket, S. Biswas, G. Judd, and R. Morris. (2004). Link-level Measurements from An 802.11b Mesh Network. ACM SIGCOMM Computer Communication Review, 34(4).

Ammana A. (2008). Assessment of current and emerging broadband wireless technologies for VDOT operations program. Center for Technology Development, Virginia Tech Transportation Institute.

Bai, F., and H. Krishana. (2006) Reliability Analysis of DSRC Wireless Communication for Vehicle Safety Applications. Proceedings of 2006 IEEE Intelligent Transportation Systems Conference. Vol. 1, Toronto, Ontario, Canada, pp. 355-362.

Baskaran, V.M. Tiong, S.K. Jamaludin, M.Z. (2005)Analysis of Real-Time Multiple Source Video Streaming via Wireless 5.8 GHz for Intelligent Traffic Management System, Proceedings of 13th IEEE International Conference, Nov, 2005, pp. 5-12.

Bartin, B., Ozbay, K., Mudiganda, S., Yanmaz-Tuzel, O., and List, G. (2006). Modeling and simulation of unconventional traffic circles. Transportation Research Record, 1965, 201-209.

Berkeley Highway Lab (BHL). (2006). <www.calccit.org/news/slides/JD%20Margulici,%20CCIT.ppt> Accessed July 10, 2009.

BP SX 40 & 50. BP Solar. http://www.solartech.com.au/pdfs/products/solar_panels/bp_sx_40_50.pdf, Accessed on August 1, 2008.

Broadcom Corporation (2006). 802.11n: Next-Generation Wireless LAN Technology (White Paper). <http://www.broadcom.com/collateral/wp/802_11n-WP100-R.pdf>

Brydia R.E., Raback L.G., Rajbhardari R., Johnson J.D., and Brackin E. (2008). Communication Trends and Their Impacts on TXDOT ITS Deployments. FHWA/TX-08/0-5586-1, Texas Department of Transportation.

Bultitude, R. J. C., De Jong, Y. L. C., Pugh, J. A., Salous, S., Khokhar, K. (2007) Measurement and Modeling of Emergency Vehicle-to-Indoor 4.9 GHz Radio Channels and Prediction of IEEE 802.16 Performance for Public Safety Applications. Proceedings of Vehicular Technology Conference. pp. 397-401.

Broadcom Corporation (2006). 802.11n: Next-Generation Wireless LAN Technology (White Paper). <http://www.broadcom.com/collateral/wp/802_11n-WP100-R.pdf>

Broadband Wireless Exchange Magazine. (2006). Mobile WiMAX Wireless Internet Access. <http://www.bbwexchange.com/WiMAX/> Accessed on Apr 15, 2009.

Cai, H., Lin, Y. (2005). Design of a Roadside Aeamless Wireless Communication System for Intelligent Highway. Proceedings IEEE Networking, Sensing and Control, Tucson, AZ, 342-347.

Chan, C. Y., and Bu, F. P. (2006). Vehicle-Infrastructure integrated approach for pedestrian detection: feasibility study based on experimental transit vehicle platforms." Proceedings of Transportation Research Board 85th Annual Meeting (CD-ROM), Transportation Research Board, Washington D.C.

Chen, Y. (2007). Enhance Emergency Services by Use of Novel Road Management System in Wireless City. Proceedings of Intelligent Transportation Systems Conference, 2007, pp. 748-753.

Cheung, S.Y., and Varaiya, P. (2007) Traffic Surveillance by Wireless Sensor Networks: Final Report. California PATH Research Report, <www.path.berkeley.edu/PATH/Publications/PDF/PRR/2007/PRR-2007-04.pdf> , accessed July 20, 2008.

Chowdhury, M., Wang, K., Kim, Y., and Ma, Y. (2007) Integrated Simulation Platform for Evaluating Wireless Traffic Sensor Network for Traffic Safety and Security Response - Final Report. South Carolina State University.

Chowdhury, M., and Sadek, A. (2004). Fundamental of Intelligent Transportation System Planning, Artech House Publishers.

Cisco Systems. (2009). Capacity, Coverage, and Deployment Considerations for IEEE 802.11g. Cisco Systems, <http://www.cisco.com/application/pdf/en/us/guest/products/ps430/c1244/ccmigration_09186a00801d61a3.pdf>, accessed on Apr 15, 2009.

Cisco Systems[1]. (2009) <http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5279/ps5285/product_data_sheet09186a008018495c.html>

Cisco Systems[2]. (2008) <http://www.waveform.ie/_fileupload/Image/Cisco%201520%20Data%20Sheet.pdf>

City of Cape Town, South Africa. (2005). Traffic signal services. http://www.capetown.gov.za/atrams.

Coifman, B. and Ramachandran, M. (2004). Distributed surveillance on freeways with an emphasis on incident detection. Conference on IEEE Intelligent Transportation Systems, Washington, WA, 773-778.

Crunch, T. (2006). Phoenix PD Keeps the City Safe With Firetide Wireless Mesh. Firetide, Inc., <http://www.firetide.com/innerContent.aspx?id=1106>, accessed on Apr 15, 2009.

Debeasi, P. (2008). Mobile Technologies and Trends: WiMAX Performance. <http://searchmobilecomputing.techtarget.com/tip/0,289483,sid40_gci1315881,00.html>, accessed on November 2, 2009.

DD-WRT, <http://www.dd-wrt.com/dd-wrtv3/index.php>, accessed on January 20, 2009

Doucet, K. (2006). WiMAX moving from Fixed to Mobility. Redline Communications Inc. <http://www.memobilitysummit.com/2006/speakers/redline.pdf> , accessed on Apr 15, 2009.

Duke Energy, South Carolina, <http://www.duke-energy.com/south-carolina.asp>, accessed on July 30, 2009.

Dusit N., and Hossain, E. (2007). Integration of WiMAX and Wi-Fi Optical Pricing for Bandwidth Sharing. IEEE Communications Magazine, 45(5), 140-146.

Endoh, K., Yoshida, K., and Yakoh, T. (2008). Low Delay Live Video Streaming System, Proceedings of conference on 6th IEEE International Industrial Informatics (INDIN), 1481-1486.

Ferries, D. (1990). Client Requirements for Real-time Communication Services, Journal of IEEE Communications, 28(11), pp. 65-72.

Filis, K. G., Theodoropoulou, E. D., and Lyberopoulos, G. L. (2007). The effect of a Rapidly Changing Urban Environment on Nomadic WiMAX Performance. Proceedings of Mobile and Wireless Communications Summit 16th IST, 1-5.

Fries, R., Chowdhury, C. and Brummond, B. (2008), Transportation Infrastructure Security Utilizing Intelligent Transportation Systems, John Wiley and Sons.

Gallagher, B.; H. Suzuki, and H. Akatsuka. Wireless Communications for Vehicle Safety: Radio Link Performance and Wireless Connectivity Methods. IEEE Vehicular Technology Magazine. Vol. 4, No.4, 2006, pp. 4-16.

Gordon, R., R.A. Reiss, W.M. Dunn, and D.R. Morehead. (1993). Communications handbook for traffic control systems. FHWA-SA-93-052, Federal Highway Administration, U.S Department of Transportation.

Gordon, R., and Tighe, W. (2005). Traffic Control Systems Handbook. FHWA-HOP-06-006, Federal Highway Administration, U.S Department of Transportation.

Gray, D. (2007). A Comparative Analysis of Mobile WiMAX Deployment Alternatives in the Access Network. WiMAX Forum.

Heidemann, J., F. Silva and Wang, X. (2004). Sensors for Unplanned Roadway Events--Simulation and Evaluation: Draft Final Report. METRAN Project Report 04-08. METRANS Transportation Center, University of South California.

Hancock, J. (2004). Jitter: Understanding it, Measuring it and Eliminating it. Agilent Technologies. <http://www.highfrequencyelectronics.com/Archives/Apr04/HFE0404_Hancock.pdf. >, Accessed July 10, 2009.

Hideo, T. (1996). Intelligent Transportation Systems in Japan. <http://www.tfhrc.gov/pubrds/fall96/p96au41.htm>, accessed on November 2, 2009.

HiperMAX-micro Base Station. (2008). *Airspan Networks Inc*. www.airspan.com/pdfs/HiperMAX_Micro1.pdf. Accessed on August 1, 2008.

H'mimy, H. (2005). Advanced Topics in Wireless Communications. <http://www.engr.smu.edu/EETS/8315/EE8315_Lecture12_WiMAX_2005_PA1.ppt>, accessed on November 2, 2009.

Horsley, J. (2007), Policy for Cooperative ITS. Presented at 14th ITS World Congress Executive Session 06, Beijing, China. <http://www.transportation.org/sites/aashto/docs/Horsely-2007-10-02.pdf>, accessed on November 2, 2009.

Hunsucker, D. Q. (2002). Evaluation of 220 MHz Frequencies for ITS Experimentation. Kentucky Transportation Center. <http://www.e-archives.ky.gov/Pubs/transportation/TC_Rpt/KTC_02_03_SPR_235_00_1F.pdf>, accessed on April 15, 2009.

Hwang, M., Kemp, J., Lerner, L. E., Neuerburg, N., Okuneieff, P. (2006). Advanced Public Transportation System: State of the Art Updated 2006. FTA-NJ-26-7062-06.1, Federal Transit Administration, U.S. Department of Transportation.

Inflation Data dot com, <http://www.inflationdata.com/inflation/inflation_rate/historicalinflation.aspx>, accessed on July 30, 2009.

Iperf, University of Central Florida, <http://www.noc.ucf.edu/Tools/Iperf/default.htm>, accessed on July 10, 2009.

ITS Standard Advisory (2003). Dedicated short range communication (DSRC). Advisory No.3, U.S. Department of Transportation, <http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm> , assessed on April 15, 2009.

Joe, I. (1996). Packet Loss and Jitter Control for Real-time MPEG Video Communications, Journal of Computer Communications, 19, 901-914.

Jones, W. S. (2002). Broadband Wireless: Is it an option for your ITS. U.S. Department of Transportation.

Kanafani, A., Benouar, H., Chiou, B., Ygnace, J., Yamada, K., and Dankberg, A. (2006). California Train Connected. California Research Report. UCB-ITS-PRR-2006-4. California Path Program. <http://www.path.berkeley.edu/PATH/Publications/PDF/PRR/2006/PRR-2006-04.pdf> , accessed on April 15, 2009.

Kim, H.; Shin, M.; Nam, B. and Lovell, D. (2007). An Integrated Transportation and Communication Simulation Framework for Vehicular Ad Hoc Network Applications. Proceedings of TRB 87th Annual Meeting. Transportation Research Board, Washington, D.C.

Kiyotaka, S., Kawasaki, K. and K. Nakamura. (2006). Application of Ad-hoc Network Technology to Railway Systems. Journal of Railway Technical Research Institute, Quarterly Reports. 47(2). 83-88.

Klein, A. L., Mills, K.M. and Gibson, R.P.D. (2006). Traffic Detector Handbook: Version 3. U.S. Department of Transportation, Washington D.C.

Koul, M.S. (2007). Analysis of Effects of Packet Loss and Delay Jitter on MPEG-4 Video Quality, <http://students.uta.edu/ms/msk3794/docs/mskoul-mpeg4%20loss%20paper.pdf>, accessed July 10, 2009.

Krunz, M., Mugattash, A., and Lee, S.J. (2004). Transmission Power Control in Wireless Ad hoc networks: Challenges, Solutions and Open Issues. Journal of IEEE Network, 18(5), 8-14.

Law, A. M. and Kelton, W. D. (2000). Simulation Modeling and Analysis (3th edition), New York, McGraw-Hill.

Leader, S. (2004). Telecommunications handbook for transportation professionals: The basics of telecommunications. FHWA-HOP-04-034, U.S. Department of Transportation, Washington D.C.

Lu, L., and Lu, X.Y. (2007). Quality Accessing Over a Packet Network, Second Workshop on Digital Media and its Application in Museum & Heritage. <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04414582>, accessed July 10, 2009.

Ma, Y. (2008). Distributed Intelligent Vehicle-Infrastructure Integration System for Real-Time Traffic Surveillance. Ph.D. study, Clemson University, Clemson, SC, 2008.

Ma, Y.C., Zhou, Y., Chowdhury, M., Wang, K.C. and Fries, R. (2009). A Framework for Performance Evaluation of Communication Alternatives for Intelligent Transportation Systems. Journal of Intelligent Transportation Systems, 13(3), 111-126.

Martin, J., W. Pressly, and M. Westall. (2008). WiMAX Performance at 4.9 GHz. <https://mgridhost.clemson.edu/WiMAX/default.aspx>, accessed on November 2, 2009.

Martin, P., Perrin, J., Hansen, B. (2001). Incident Detection Algorithm Evaluation", Report prepared for Utah Department of Transportation. http://www.mountain-plains.org/pubs/pdf/MPC01-122.pdf, Accessed on October 31, 2009.

Martin, J., W. Pressly, and M. Westall. (2008) WiMAX Performance at 4.9 GHz. https://mgridhost.clemson.edu/WiMAX/default.aspx.

Mirchandani, P. and Head, L. (1998). RHODES: a real-time traffic signal control system: architecture, algorithms, and analysis. http://www.sie.arizona.edu/ATLAS/docs/TRISTANIII.pdf.

MOXA, http://www.captec.co.uk/data/products/pdfs/moxa_soft_dvr.pdf, Accessed July 10, 2009.

Nation Oceanic and Atmospheric Administration, (NOAA). (2006). "Hurricane Katrina, August 21-23 2005", U.S. Department of Commerce, <http://www.weather.gov/os/assessments/pdfs/Katrina.pdf> (April 15, 2009)

Ngatman, M.F., Ngadi, M.A., and Sharif, J.M. (2008). Comprehensive study of transmission techniques for reducing packet loss and delay in multimedia over IP, Journal of Computer Science and Network Security, Vol..8 No.3, 292-299. <http://paper.ijcsns.org/07_book/200803/20080342.pdf>, accessed July 10, 2009.

Niyato, D., and Hossain, E. (2007). Integration of WiMAX and Wi-Fi: Optimal Pricing for Bandwidth Sharing. IEEE Communication Magazine, May 2007, pp. 140-145.

Nuaymi, L. (2007). WiMAX Technology for Broadband Wireless Access. John Wiley & Sons, Ltd. England.

Quadstone. Paramics Traffic Simulation Model. Quadstone Limited. Retrieved from http://www.Paramics-online.com, January, 2009.

Osafune, T., Monden, K., Fukuzawa, S., and Matsui, S. (2004). Performance Measurement of Mobile Ad Hoc Network for Application to Internet-ITS. 2004 International Symposium on Applications and the Internet. Tokyo, Japan, 25-30.

Ozbay, K., Yasar, I., and Kachroo, P. (2004). Modeling and PARAMICS Based Evaluation of New Local Freeway Ramp Metering Strategy that Takes into Account Ramp Queues. Transportation Research Record, 1867, 89-97.

Park, S.J., and Sivakumar, R. (2002). Load-sensitive Transmission Power Control in Wireless Ad-hoc Networks. Proceedings of IEEE Global Telecommunications Conference, 1, Taipei, Taiwan, 42-46.

Peterson, L.L., and Davie, B.S., (2003). Computer Networks: A System Approach, 3rd Ed, Morgan Kaufmann, California.

Pourahmadit, V., Jamalit, H., and Naieeni, R.S. (2005). Saturated Throughput Analysis of the IEEE 802.11b DCF Mode in a Slow Rayleigh Fading Channel, Proceedings of the 13th IEEE International Conference on Networks, 1, 46-50, Kuala Lumpur, Malaysia.

Ramachandra, K., and Ali., H.H. (2004). Evaluating the Performance of Various Architectures for Wireless Ad Hoc Networks. Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 37, Big Island, HI, 4721-4729.

Road and Traffic Authority, New South Wales, Australia. (2006). Sydney coordinated adaptive traffic system (SCATS). http://www.rta.nsw.gov.au/trafficinformation/trafficfacilities/scats/.

Roadway Sensors. ITERIS. (2008). <http://www.oceanstatesignal.com/PDF/Detection/Iteris/VersiCam.pdf>, accessed on August 1, 2008.

Siemens. (2006). Principles of SCOOT. http://www.itssiemens.com/en/t_nav224.html.

Smith, B.L., Zhang, H., Fontaine, M.D., and Green, M.W. (2004). Wireless Location Technology-Based Traffic Monitoring: Critical Assessment and Evaluation of An Early Generation System. Journal of Transportation Engineering, 577-584.

Schnacke, D. (2004). Proposed applications for 5.9 GHz DSRC in North America.” Presented at ITS World Congress, Japan, <http://www.itsforum.gr.jp/Public/E4Meetings/P03/schnackeSS27.pdf>, accessed on April 15, 2009.

Schwartz, M., (2005). Mobile Wireless Communications, Cambridge University Press, 25.

Solar Panel Store. Colorado Solar Inc. <http://www.solarpanelstore.com/>, accessed on August 1, 2008.

Sun rate. MRSOLAR 2008. Mrsolar.com. <http://www.mrsolar.com/content/solar-insolation-maps/>, accessed on August 1, 2009.

Stephanedes, Y.J., Douligeris, C., Takaba, S. (1996). Communications for the intelligent transportation system. IEEE Communications Magazine, 34(10), 24-30.

The Network Simulator - ns-2. (2006). Information Sciences Institute. The University of Southern California. <www.isi.edu/nsnam/ns>, accessed on July 20, 2008.

Tokuyama, H. (1996). Intelligent transportation systems in Japan. http://www.tfhrc.gov/pubrds/fall96/p96au41.htm.

Tse, D., and Viswanath, P. (2005) Fundamentals of Wireless Communication. Cambridge University Press, 1st Edition.

Tyco Integrated Systems. (2006).Traffic management – SCATS. http://www.traffic-tech.com/pdf/scatsbrochure.pdf.

University of California at Berkeley. (2005). Vehicle-Infrastructure Integration (VII) and safety: rubber and radio meets the road in California. Intellimotion, 11(2).

University of California, Berkeley. (2006). VII California demonstrates success: Finalist in ITSA "Best of" research and innovation. Intellimotion, 12(1).

University of California, Berkeley. (2006). VII California demonstrates success: Finalist in ITSA "Best of" research and innovation. Intellimotion, 12(1).

U.S. Department of Transportation. (2006). Intelligent transport systems: technology overview. http://itsdeployment.ornl.gov/technology_overview/.

U.S. Department of Transportation (2007). National ITS Architecture Version 6.0, < http://www.iteris.com/itsarch/>, accessed on November 3, 2009.

U.S. Department of Transportation (2003). ITS Deployment Analysis System (IDAS), <http://idas.camsys.com/>, accessed on November 3, 2009.

U.S. Department of Transportation (2007). National ITS Architecture Version 6.0, < http://www.iteris.com/itsarch/>, accessed on November 3, 2009.

U.S. Department of Transporation ITS Costs Database. (2006). Referenced September 30, 2006 at <http://www.itscosts.its.dot.gov/its/ benecost.nsf/AdjustedUnitCosts >

US Department of Transportation. (2001). Intelligent Transportation Systems Benefits: 2001 Update. USDOT, prepared by Mitretek.

Vassilopoulos, A., and Subirana, B. (2007). Wireless Boardband 2007: WiMAX & CO. e-business Center PricewaterhouseCoopers & IESE.

Wang, B. B, Sen, I., and Matolak, D. W. (2007). Performance Evaluation of 802.16e in Vehicle to Vehicle Channels. Proceedings of Vehicular Technology Conference, 1406-1410.

Wang, K.C., Chowdhury, M.A., and Fries, R. (2005). Real-time Traffic Monitoring and Automated Response with Wireless Sensor Networks. Proceedings of 12th World Congress on Intelligent Transport Systems. CD-ROM. San Francisco, CA.

Wi-Fi Finder. jiwire.com. Retrieved on 2008-04-20.

Wireshark, <http://www.wireshark.org/about.html>, accessed July 10, 2009.

Wireless Ad Hoc Sensor Network. National Institute of Standard and Technology. http://w3.antd.nist.gov/wahn_ssn.shtml. Accessed on August 1, 2008.

Wu, D. P., Hou, Y.W., Zhu, W.W., and Zhang, Y.Q. (2001), Streaming Video over Internet: Directions and Approaches, Journal of IEEE Transactions on Circuits and Systems for Video Technology, 11 (3), 282-300.

Xu, Q., Mak, T., Ko, J., and Senqupta, R. (2004). Vehicle-to-Vehicle Safety Messaging in DSRC. Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks. New York, N.Y., 19-28.

Yang, Q.Y., Sisiopiku,V., Arnold, J.A., Pisano, P., and Nelson, G.G. (2000). Assessment of Rural Intelligent Transportation System Wireless Communications Solutions." Transportation Research Record, 1739, 51-58.

Zhou[1], Y., Chowdhury, M., and Wang, K.C. (2009). A Synthesis of Wireless Communication Alternatives for Traffic Control and Management Applications. Proceedings of 2009 Technical Conference and Exhibit, Institute of Transportation Engineers, Phoenix, AZ.

Zhou[2], Y., Chowdhury, M., Wang, K.C., and Ma, Y.C., (2009). Wireless Traffic Sensor Network Performance due to Environmental Disturbances and Relay Network Topology. Proceedings of 88th Transportation Research Board Annual Meeting, Washington. D.C.

Zhou[3], Y., Chowdhury, M., Martin, J., Wang, K.C., Westall, J., and Kang, X.Y. (2009) Field Performance Study of a Regional WiMAX Network for Intelligent Transportation System Applications. Journal of Transportation Research Board, Transportation Research Board, (in press).

Zhao, J., and Govindan, R. (2003). Understanding Packet Delivery Performance in Dense Wireless Sensor Networks. Proceedings of ACM Conference on Embedded Networked Sensor Systems, Los Angeles, CA, 1-13.

13 APPENDICES

Appendix A Communication Infrastructure for ITS Survey

Objective:

This survey will provide researchers with information pertaining to the scope and the level of implementation and experience of communication infrastructure alternatives for intelligent transportation systems within your jurisdiction, specifically in regard to on-line traffic management.

1. What type of communication infrastructure do you have (please choose from following choices) and what are the applications (such as traffic cameras, traffic sensors, dynamic message signs, etc.)?

Medium	Applications	Miles of Coverage and/or No. of Connected Devices
Wired *(Check all that apply)*		
_____T1	______________________	______________________
_____ISDN	______________________	______________________
_____DSL	______________________	______________________
_____Others *(please specify)*		
____________________	______________________	______________________
Wireless *(Check all that apply)*		
_____Cellular	____________________	____________________

(Please specify type/bandwidth: ______ e.g. GPRS/32kbps, EDGE/236kbps, etc)

_____Wi-Fi ____________________ ____________________

_____WiMAX ____________________ ____________________

_____Others *(please specify)*
_____Others (*please specify* technology/bandwidth)

____________________ ____________________ ____________________

Feature Descriptions for Your Current Communication Infrastructure. Please provide an overview description of your infrastructure, e.g., "The system covers primarily metropolitan highways (x miles), secondary roads (y miles) and/or rural roads (z miles), p percent of them are monitored by TMC in real time, and the rest are stand-alone devices or regional clusters."

____

____

2. Previous Communication Evaluation Experience
Have you evaluated the communication system in terms of performance, cost and reliability?

Yes ☐☐☐No ☐
If yes, please summarize the major findings. *Please use additional sheets if necessary.*

____

____

____

____

Please e-mail a copy of the report at mac@clemson.edu, or mail to the address shown in the cover letter.

Emailed ☐☐☐Mailed☐

3. Do you know of any evaluation report on communication system evaluation for traffic management?

Yes ☐☐☐No ☐

If yes, please write down the source.

____

____

____

Have any one of the above publications been most influential to the choice/design of your current communication infrastructure?

Yes ☐☐☐No ☐

If yes, please write down the source.

____

4. Do you have any plan (or already planned) to use any new wireless alternative (other than what you have today) to support traffic management applications (or other related applications)?

What types of technology are you considering and why?

Type 1: ________________________

Reason: ____

Type 2: ________________________

Reason: ____

Type 3: ________________________

Reason: ____

5. Do you have any plan to expand your traffic management infrastructure?

Yes ☐☐☐No ☐

If yes, how do you plan to support the expansion with its need of communication infrastructure (for example, to satisfy increased bandwidth and coverage requirement, etc.)

____

____

____

____

6. Could you share with us of your experience in the following areas with your communications infrastructure for traffic management? *Please use additional sheet if necessary.*

   Maintenance (e.g., scope, frequency, man-hour, periodical costs) _______________

   ____

   ____

   Performance & Reliability (Please fill out the following item from your experience of your wireless communication infrastructure for traffic management.)

Wireless System	Reliability (e.g. failure during adverse weather condition or in foliage area)	Performance (e.g. throughput (kbps) and delivery ratio (%): percentage of received data rate divided by sent out data rate)
___Cellular	__________________________	________________________
___Wi-Fi	__________________________	________________________

___WiMAX ____________________________ __________________________

_____Others ____________________________ __________________________
(please specify)

Others____

____

Appendix B Communication System Survey Follow-Up Questionnaire

1. What is (are) the typical data rate(s) of your video surveillance system?
(*The answer can be provided as one or a range of bits-per-second data rate estimate, or in terms of the video standard, e.g., Motion JPEG, MPEG3, etc., with the chosen frame rate, frame size, and color depth.*)

2. What is the minimum and maximum required data rate you would expect your current and future video surveillance system or other similar devices to have?
(*The answer can be based on the current and planned usage of your system. For example, for incident detection, a 28 kbps or 56 kbps connection may suffice, while it may not be sufficient for some advanced applications you have in mind.*)

3. What is your average camera density in metro areas and average distance interval between two cameras on your monitored roadways?

4. How much do you own, and how much do you pay for leasing your current communication infrastructure? An example list of infrastructure may include.

Infrastructure	**Covered miles or square miles**	**Owned or leased**	**One-time and/or recurring costs**
Fiber/copper land line network			
Cellular wireless service			

Other infrastructure ___________			
Other infrastructure ___________			

5. Current and/or planned applications on emerging wireless technologies:

Wireless Technology	**Current or Planned Applications and Scope**	**Technology specific Specifications***	**Unit Cost ($/mile or any other)**
Wi-Fi			
WiMAX			
DSRC			
Other ___________			
Other ___________			

* Wireless channels used, frequency range, bandwidth, line-of-sight requirements, etc.

6. What are the current and planned network topologies you use to connect your video surveillance and other traffic devices?

(*For example, are all cameras required to send their data directly to a manned traffic management center, or are they processed by automated servers at several regional locations. If you know your current network architecture, such as point-to-point, star, or hierarchical, please also indicate.*)

7. Licensing Issues

Are you using any licensed* wireless communication technology? For your planned future expansions, do you have a preference for licensed or unlicensed technology? (Following is the explanation of licensing relate to wireless technologies)

(**The frequency that is used by a wireless technology can be either licensed or unlicensed as defined by the Federal Communications Commission (FCC). Unlicensed bands, such as the 915 MHz, 2.45 GHz, and 5.8 GHz ISM bands, are used by the Wi-Fi and Bluetooth technologies. These are relatively smaller bands that allow use by any compliant devices without licensing fees; unlicensed bands are, however, share by many technologies and must tolerate occasional interferences. Licensed frequencies, such as those used by the cellular, satellite, WiMAX, and DSRC technologies, must be acquired at cost by network service providers and then leased to users. Licensed frequencies assure mostly interference free operations but at a recurring leasing costs. It is expected that any ITS deployments will have to weigh the choice between licensed and unlicensed technologies based on their costs, performance, and reliability tradeoffs.*)

Appendix C Additional Case Studies

The case studies of other five cities are presented as follows, including Charleston, Spartanburg, Myrtle Beach, Gaffney, and Rock Hill.

Charleston

The section of traffic surveillance system in Charleston, SC consists of 42 traffic cameras, 36 Radar detectors and 3 dynamic message signs to be wireless connected. All these devices are located on I-26 and I-526, showed in the Figure C-1.

Distance between each node is calculated to form sub-networks (also called clusters) that each device is with radio range and also to minimize the numbers of fiber optic connections. Detailed calculation of distance is available in the attachments.

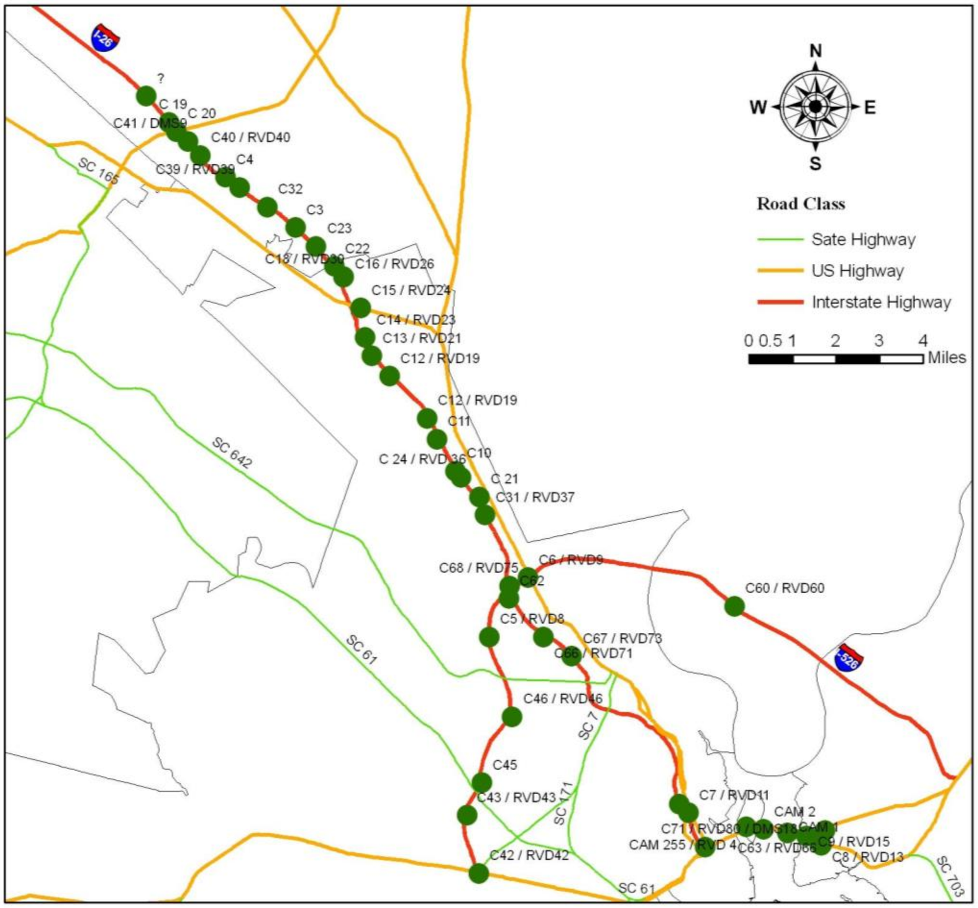


Figure C-1 Traffic Surveillance Devices in Columbia, South Carolina

WiMAX Infrastructure Models

The traffic surveillance devices in Charleston, SC were divided into 13 sub-networks, each containing at a maximum six nodes within 2 miles, showed in Figure C-2.

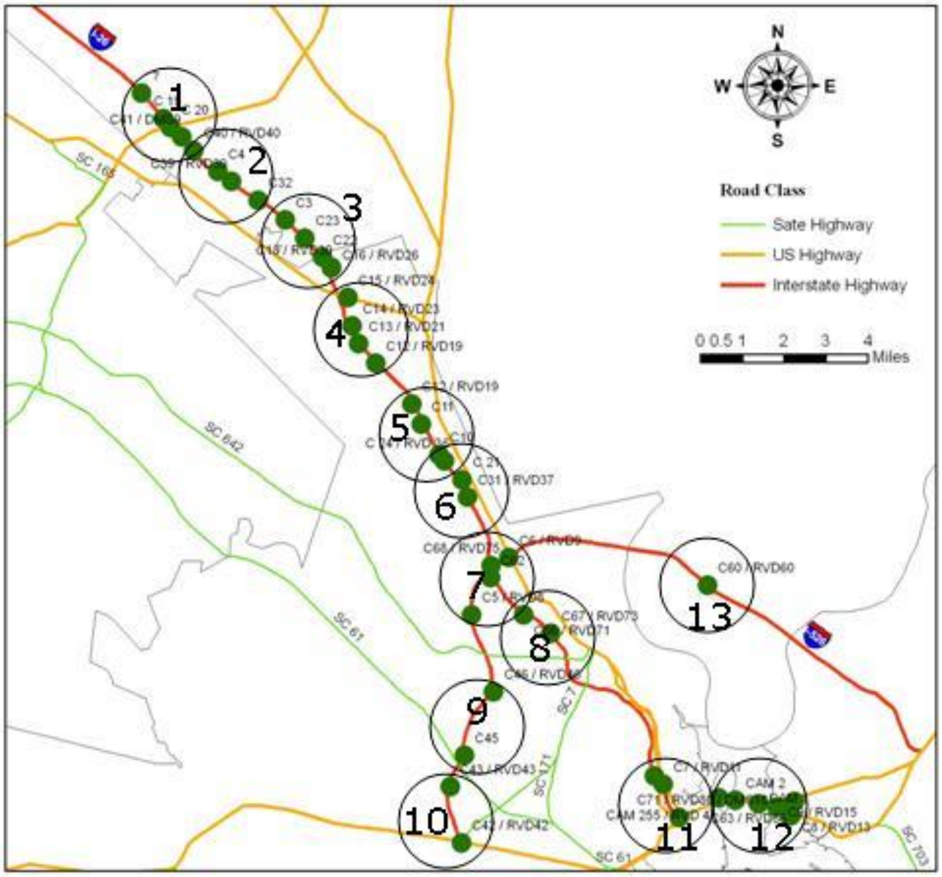


Figure C-2 Traffic Surveillance Devices in Columbia, South Carolina

In this scenario, there would be a total of thirteen fiber optic Internet connections required, and forty-two WiMAX radio.

Wi-Fi Infrastructure Network

The Wi-Fi infrastructure model shown in Figure C-3 divides the forty-two nodes into twenty-two clusters. Each cluster would have its own fiber optic access.

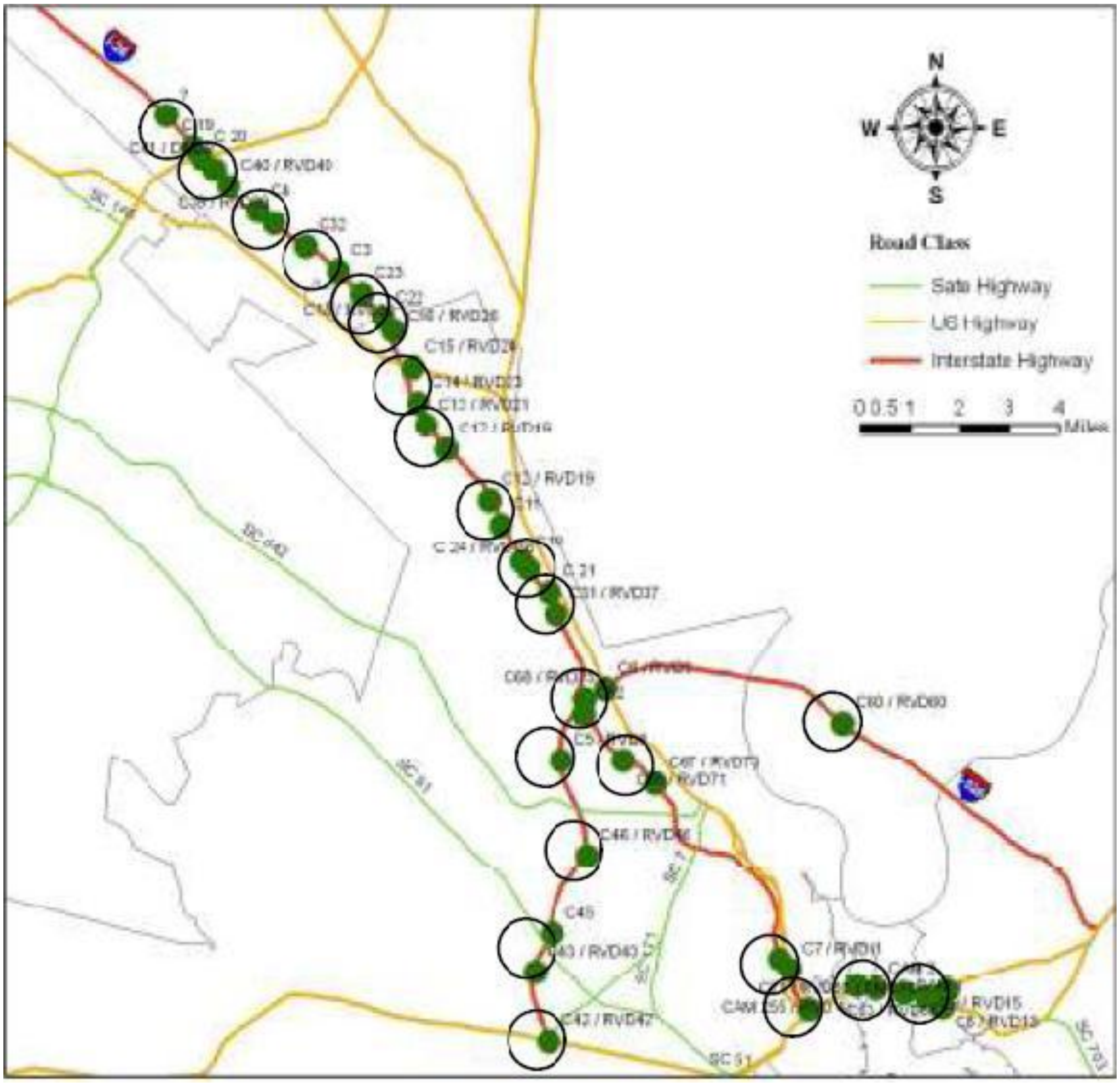


Figure C-3 Wi-Fi Infrastructure Model of Columbia Site

Wi-Fi Mesh Network

The Wi-Fi mesh model shown in Figure C-4 divides the twenty-two clusters into five mesh clusters, a group of seven clusters, two groups of five, a group of four and one satellite node. In this scenario, there would be a total of five fiber optic Internet connections required, and forty-two Cisco 1310 access points.

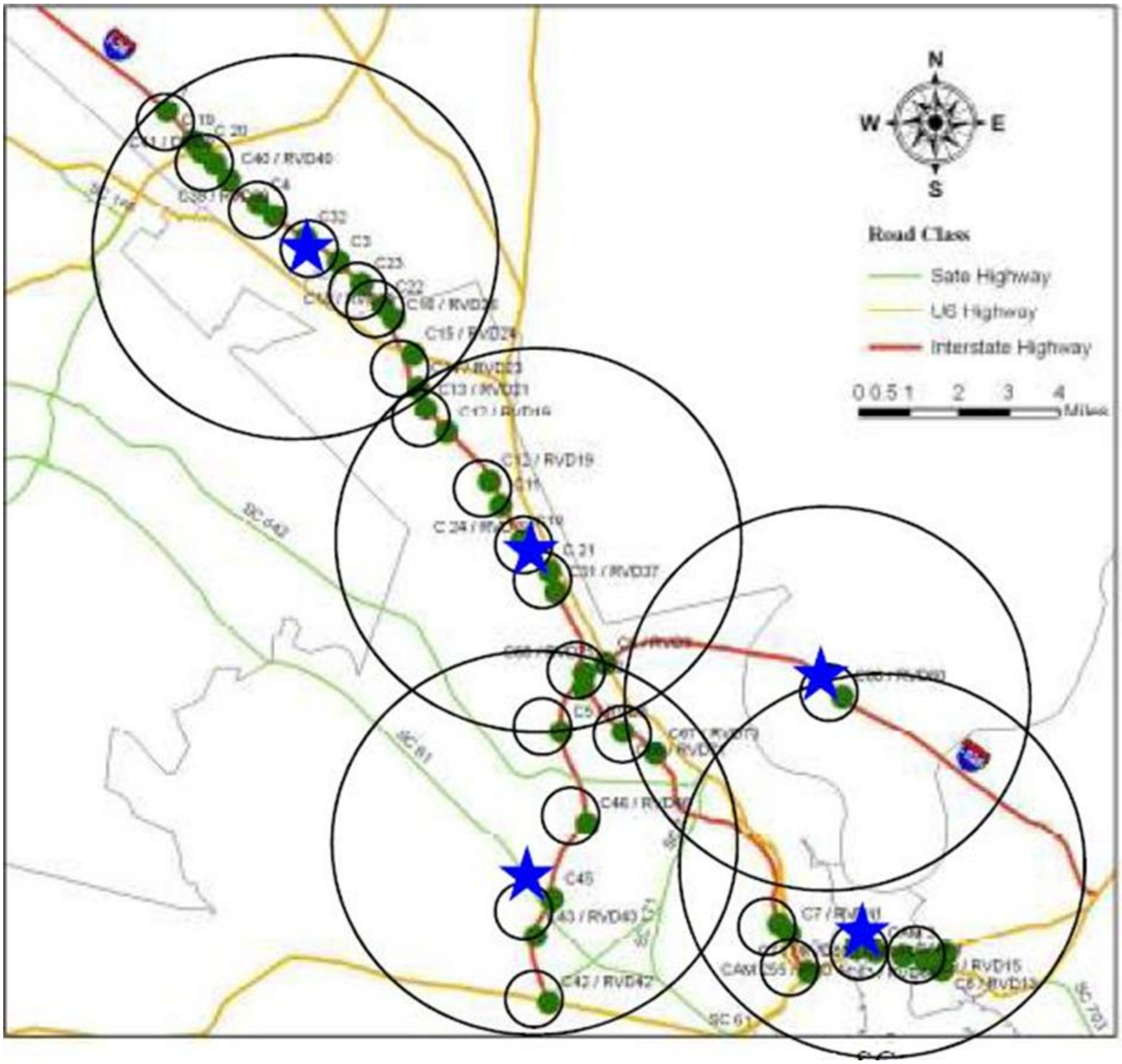


Figure C-4 Wi-Fi Mesh Network for Charleston, SC

WiMAX Mesh Network

The WiMAX mesh model shown in Figure C-5 divides the twenty-two clusters in the same manner as the Wi-Fi mesh model; with into four mesh clusters. Each node would have its own Motorola WiMAX base station, with each node in the clusters forwarding data from the other nodes. For this case study the access point locations with Internet access were chosen to minimize this maximum hop-count. In this scenario, there would be a total of four fiber optic Internet connections required, and forty-two Motorola WiMAX base stations.

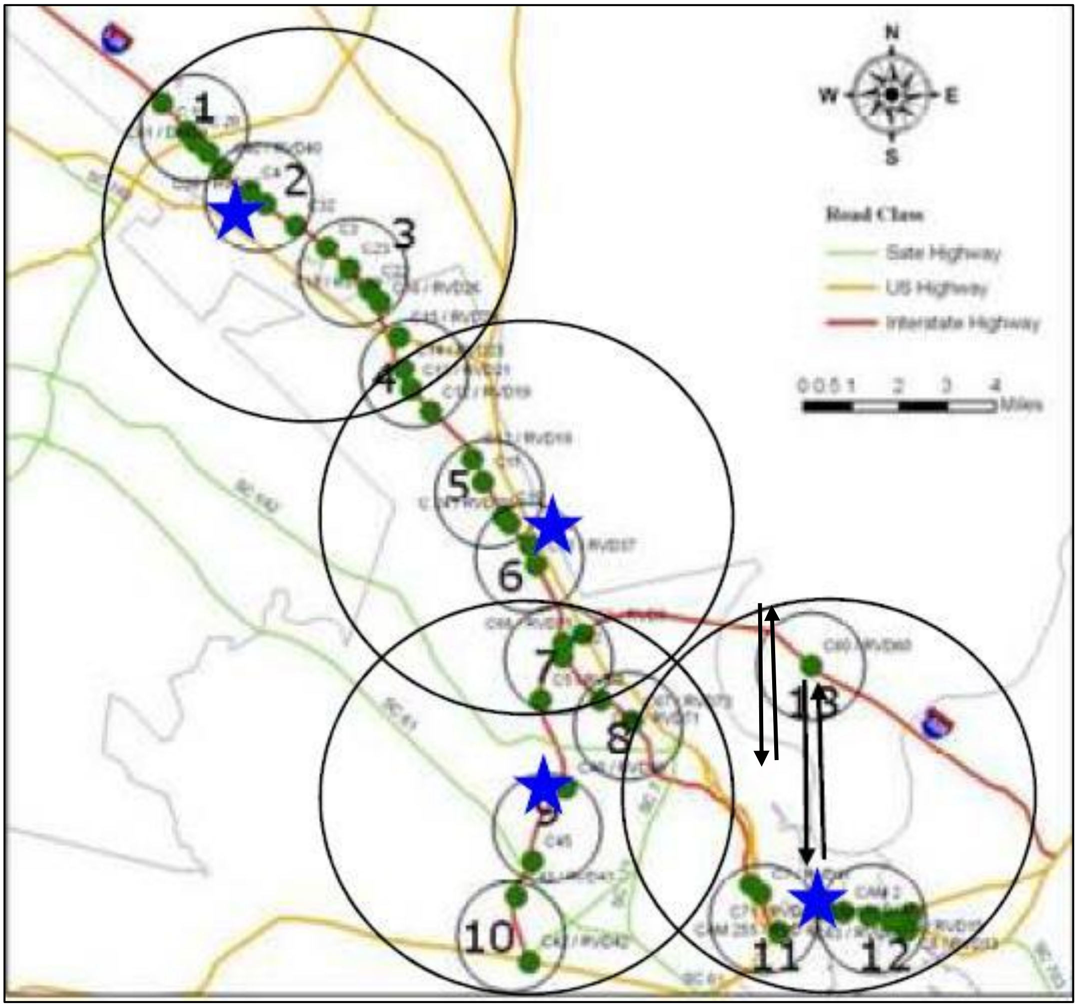


Figure C-5 WiMAX Mesh Network for Charleston, SC

Spartanburg

The section of traffic surveillance system in Spartanburg, SC consists of 18 traffic cameras to be wireless connected. All these devices are located on I-85, showed in the Figure C-6. Distance between each node is calculated to form sub-networks (also called clusters) that each device is with radio range and also to minimize the numbers of fiber optic connections. Detailed calculation of distance is available in the attachments.

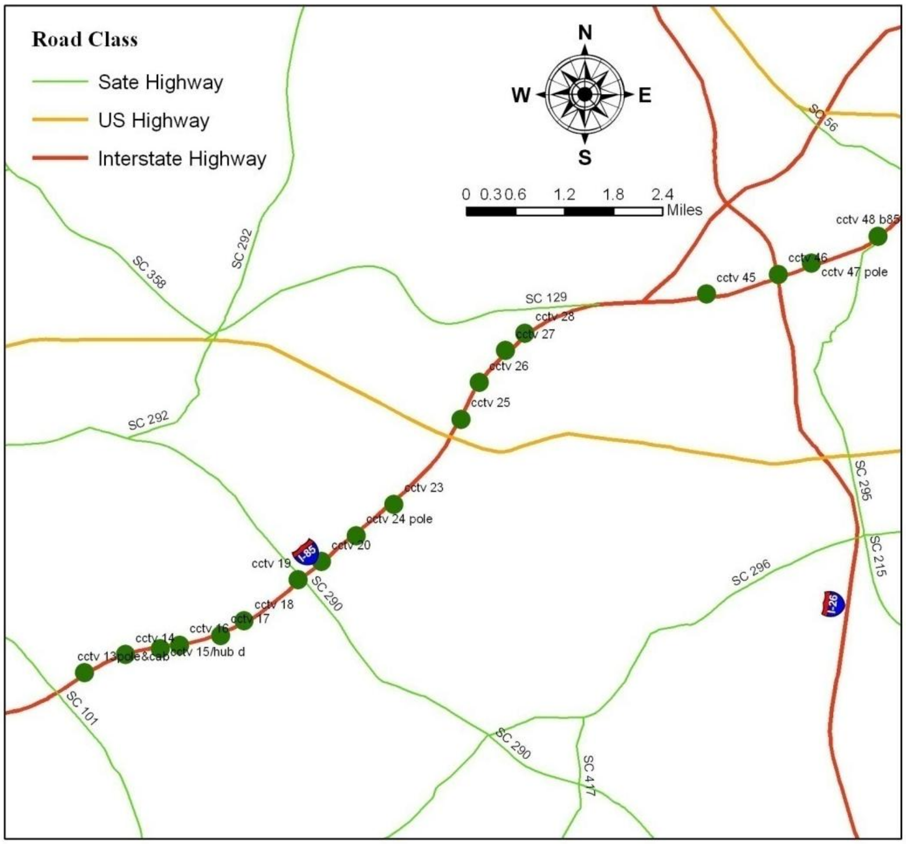


Figure C-6 Traffic Surveillance Devices in Spartanburg, South Carolina

WiMAX Infrastructure Models

The traffic surveillance devices in Spartanburg, SC were divided into four sub-networks, each containing at a maximum five nodes within 2 miles, showed in Figure C-7. In this scenario, there would be a total of four fiber optic Internet connections required, and eighteen WiMAX radio.

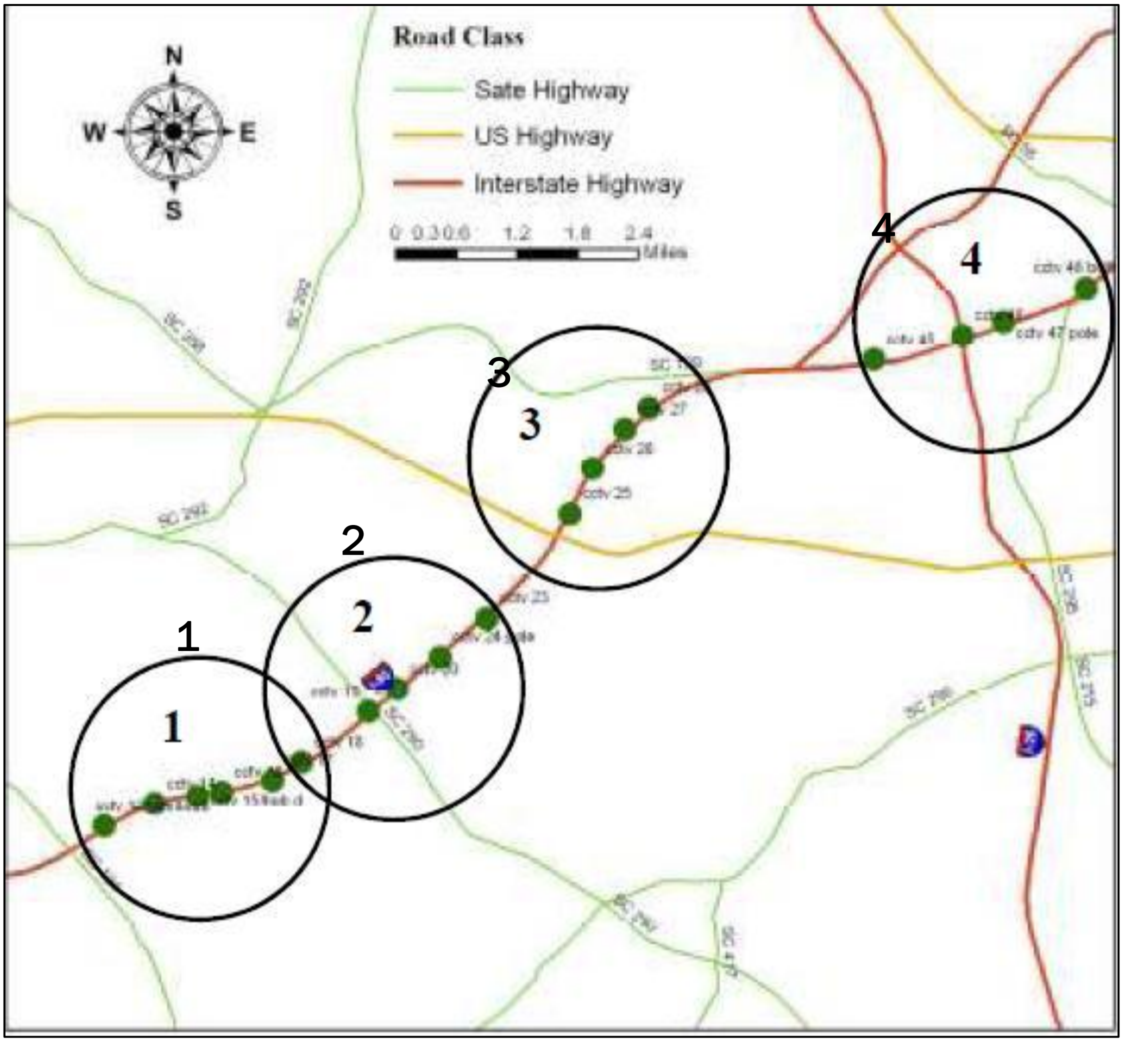


Figure C-7 WiMAX Infrastructure Network for Spartanburg, SC

Wi-Fi Infrastructure Network

The Wi-Fi infrastructure model shown in Figure C-8 divides the eighteen nodes into ten clusters. Each cluster would have its own fiber optic access.

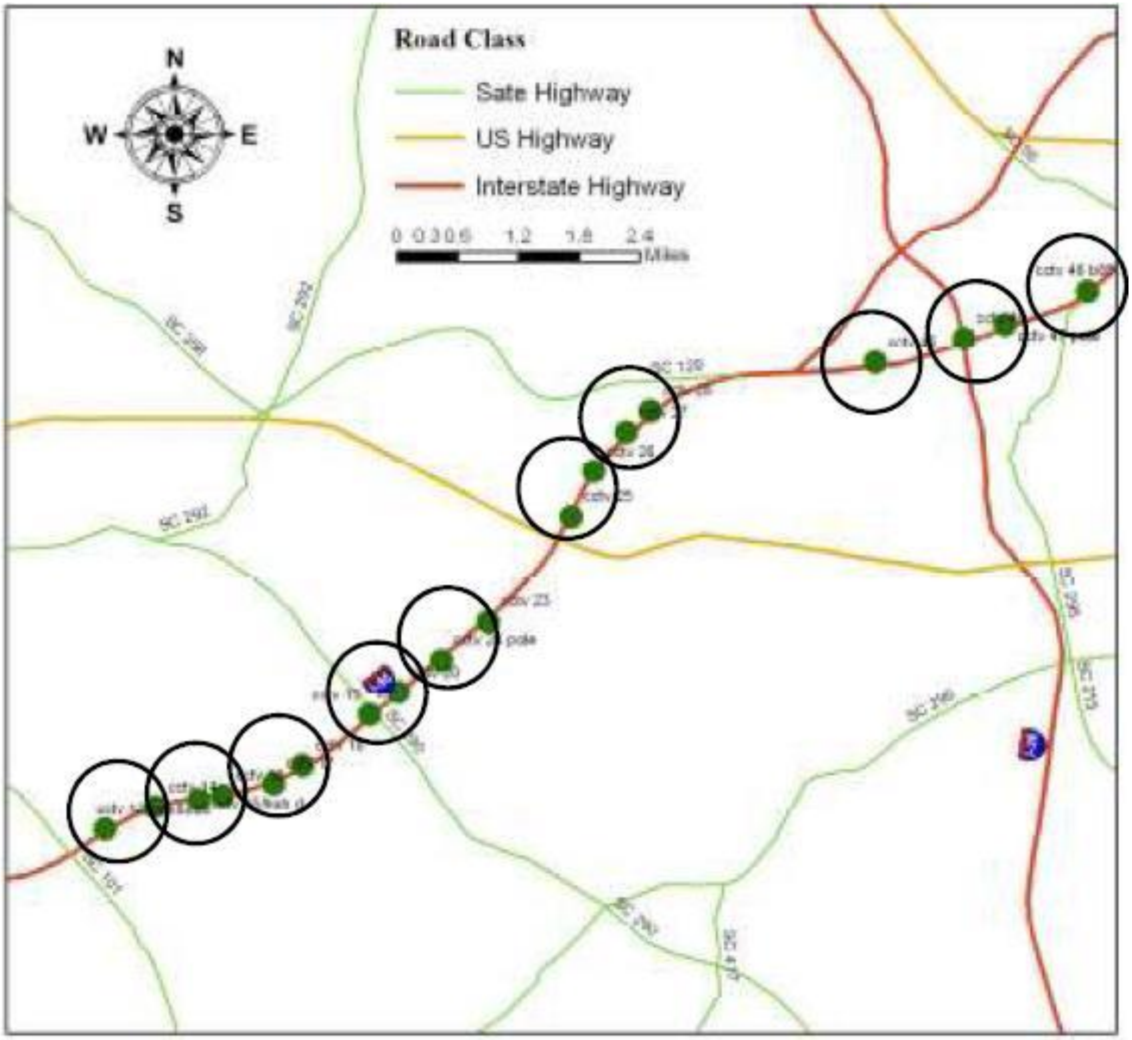


Figure C-8 Wi-Fi Infrastructure Network for Spartanburg, SC

Wi-Fi Mesh Network

The Wi-Fi mesh model shown in Figure C-9 divides the twenty-two clusters into three mesh clusters, a group of four clusters and two groups of three clusters. In this scenario, there would be a total of three fiber optic Internet connections required, and eighteen Cisco 1310 access points.

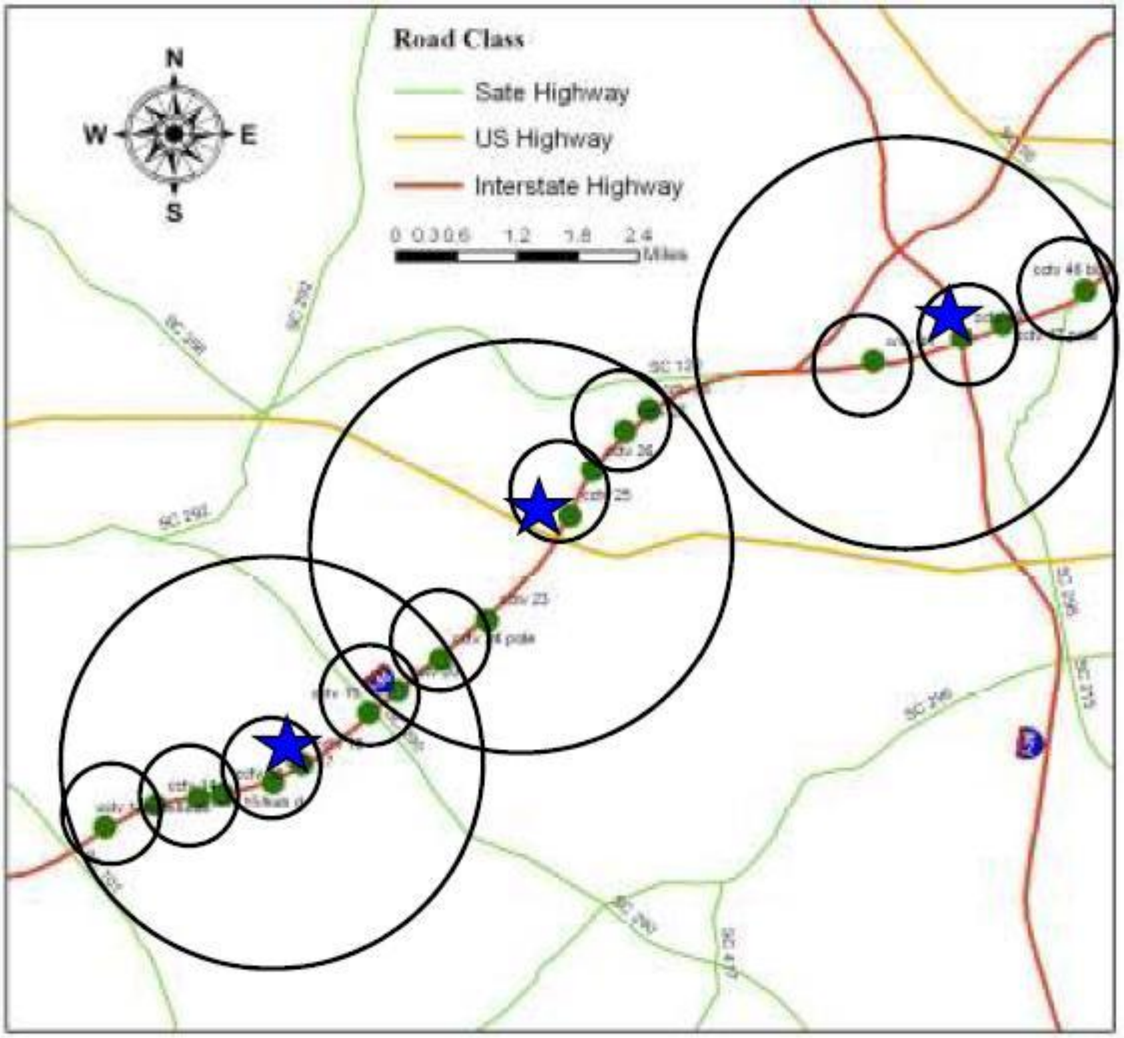


Figure C-9 Wi-Fi Mesh Network for Spartanburg, SC

<u>WiMAX Mesh Network</u>

The WiMAX mesh model shown in Figure C-10 divides the ten clusters in the same manner as the Wi-Fi mesh model; with into three mesh clusters. Each node would have its own Motorola WiMAX base station, with each node in the clusters forwarding data from the other nodes. For this case study the access point locations with Internet access were chosen to minimize this maximum hop-count. In this scenario, there would be a total of three fiber optic Internet connections required, and eighteen Motorola WiMAX base stations.

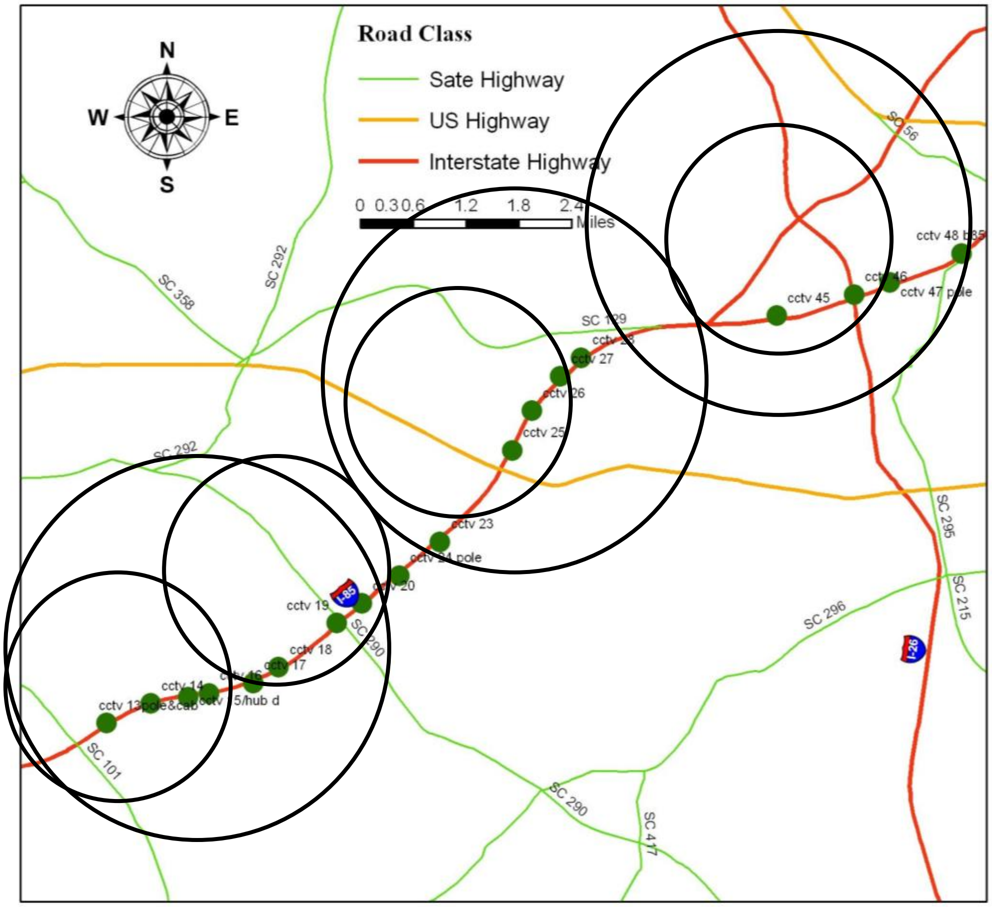


Figure C-10 WiMAX Mesh Network for Spartanburg, SC

Myrtle Beach

The section of traffic surveillance system in Myrtle Beach, SC consists of 20 traffic cameras and 4 radars to be wireless connected. All these devices are located on US-17 and US 501, showed in the Figure C-11. Distance between each node is calculated to form sub-networks (also called clusters) that each device is with radio range and also to minimize the numbers of fiber optic connections. Detailed calculation of distance is available in the attachments.

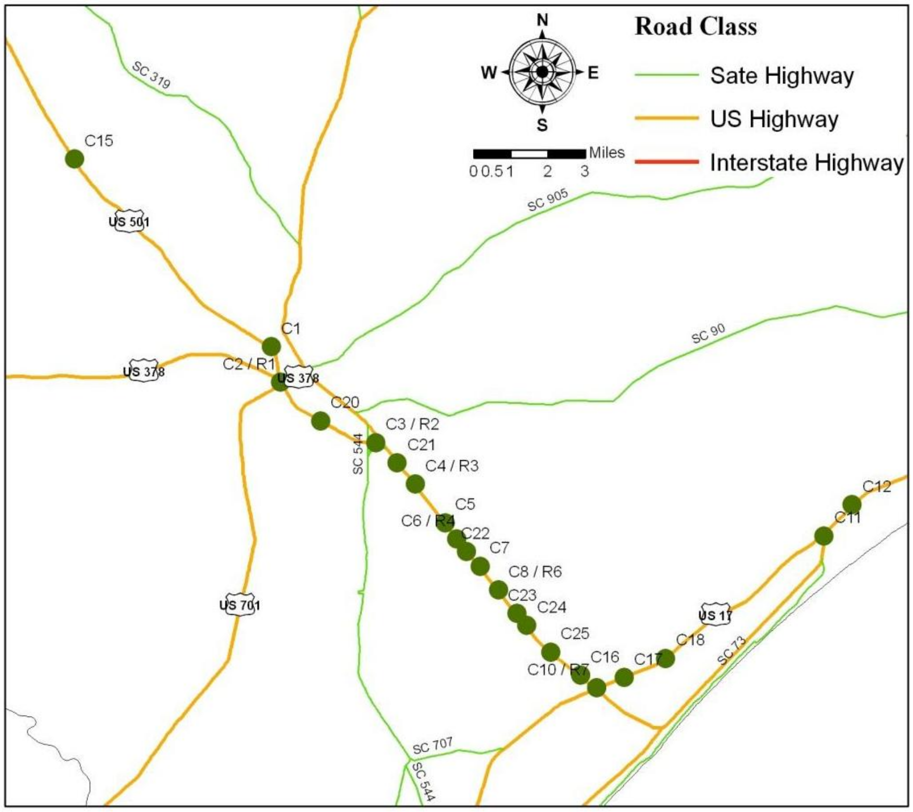


Figure C-11 Traffic Surveillance Devices in Myrtle Beach, South Carolina

WiMAX Infrastructure Models

The traffic surveillance devices in Spartanburg, SC were divided into seven sub-networks, each containing at a maximum four nodes within 2 miles, showed in Figure C-12. In this scenario, there would be a total of seven fiber optic Internet connections required, and 20 WiMAX radio.

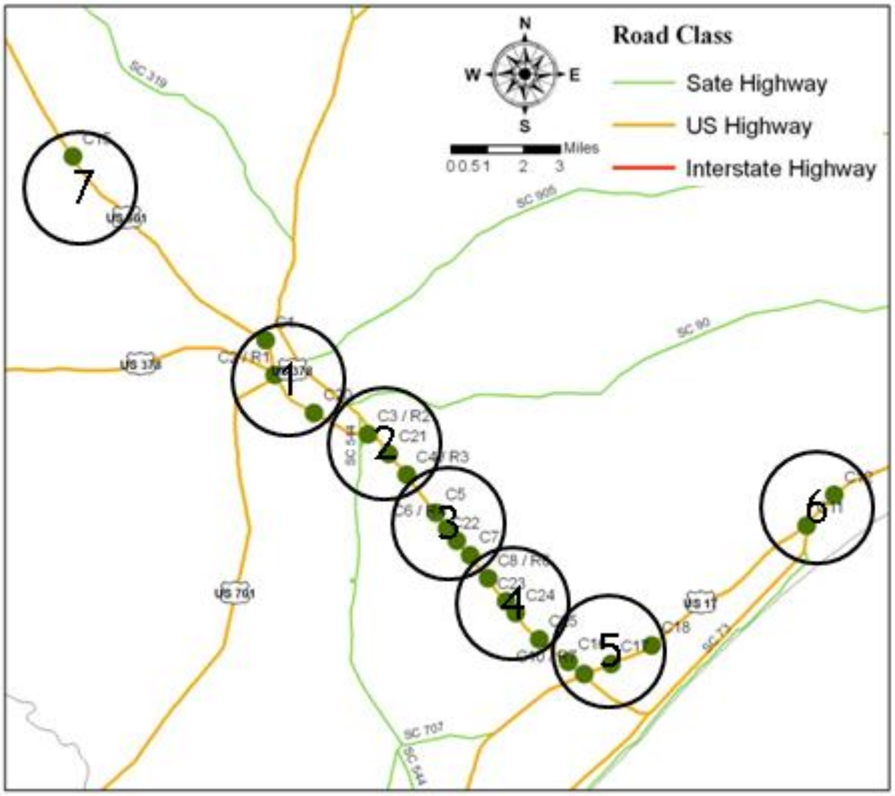


Figure C-12 WiMAX Infrastructure Model for Myrtle Beach, SC

Wi-Fi Infrastructure Network

The Wi-Fi infrastructure model shown in Figure C-13 divides the 20 nodes into twelve clusters. Each cluster would have its own fiber optic access.

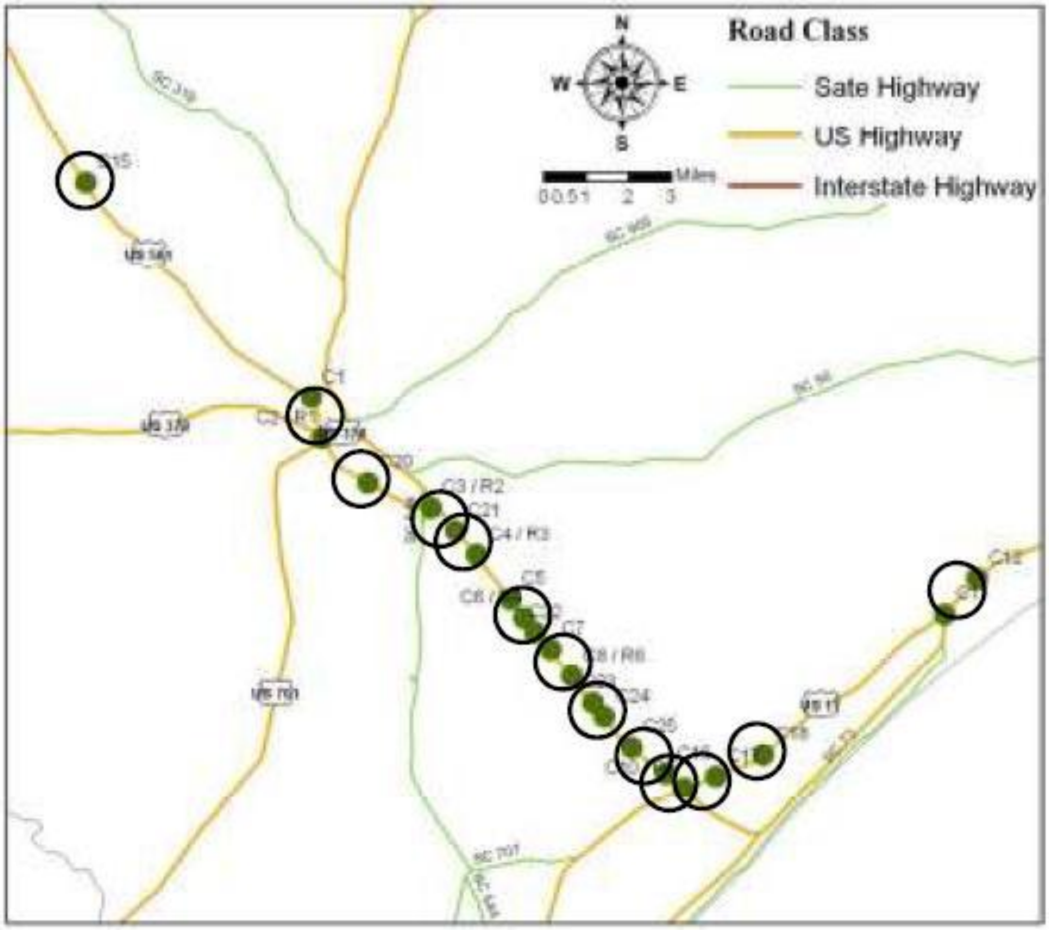


Figure C-13 Wi-Fi Infrastructure Model for Myrtle Beach, SC

Wi-Fi Mesh Network

The Wi-Fi mesh model shown in Figure C-14 divides the thirteen clusters into three mesh clusters, a group of five clusters, a group of six clusters and a satellite node. In this scenario, there would be a total of three fiber optic Internet connections required, and 20 Cisco 1310 access points.

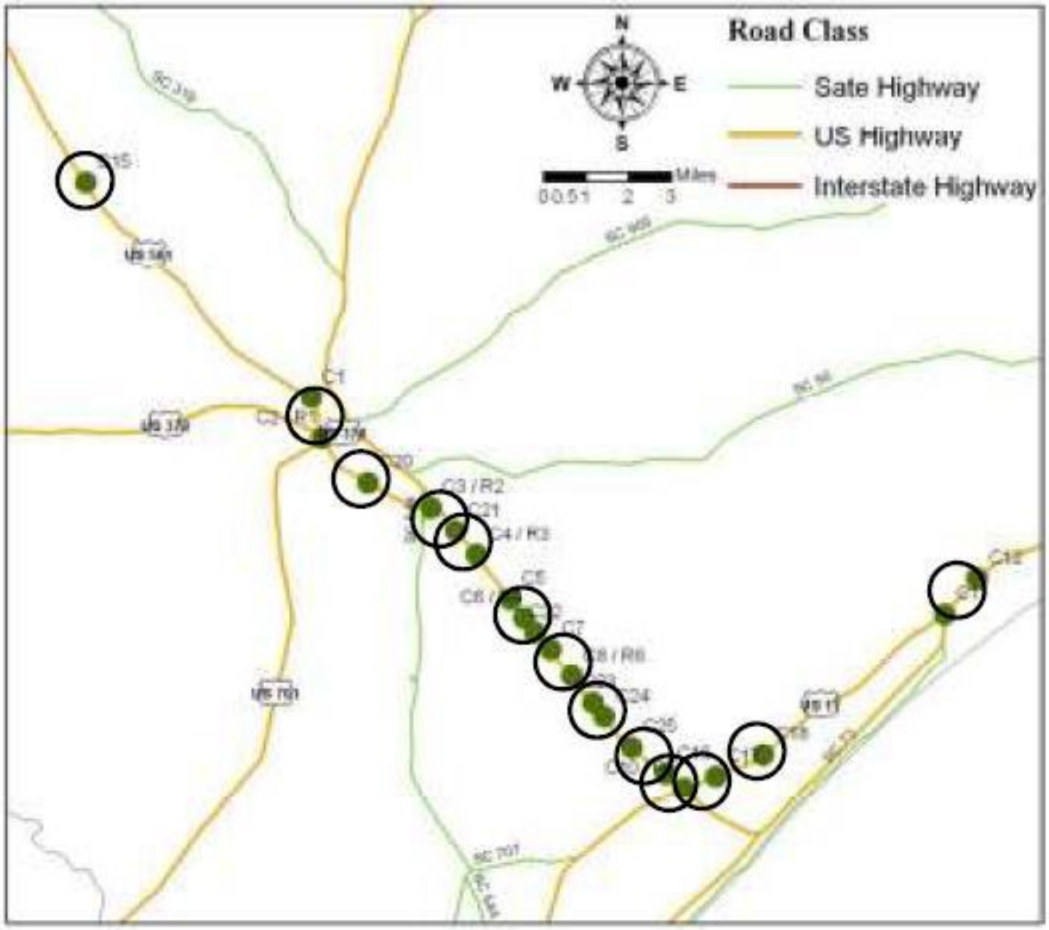


Figure C-14 Wi-Fi Mesh Network Model for Myrtle Beach, SC

WiMAX Mesh Network

The WiMAX mesh model shown in Figure C-15 divides the six clusters in the same manner as the Wi-Fi mesh model; with into three mesh clusters. Each node would have its own Motorola WiMAX base station, with each node in the clusters forwarding data from the other nodes. For this case study the access point locations with Internet access were chosen to minimize this maximum hop-count. In this scenario, there would be a total of three fiber optic Internet connections required, and 20 Motorola WiMAX base stations.

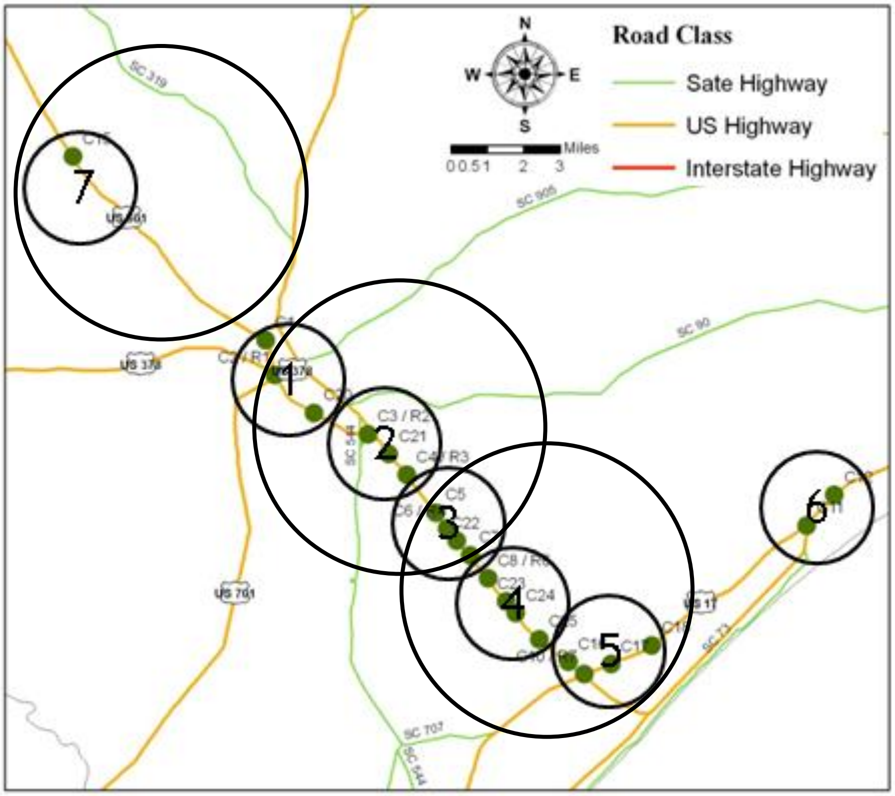


Figure C-15 WiMAX Mesh Network Model for Myrtle Beach, SC

Rock Hill

The section of traffic surveillance system in Rock Hill, SC consists of 26 traffic cameras and 25 radars to be wireless connected. All these devices are located on I-77, showed in the Figure C-16. Distance between each node is calculated to form sub-networks (also called clusters) that each device is with radio range and also to minimize the numbers of fiber optic connections. Detailed calculation of distance is available in the attachments.

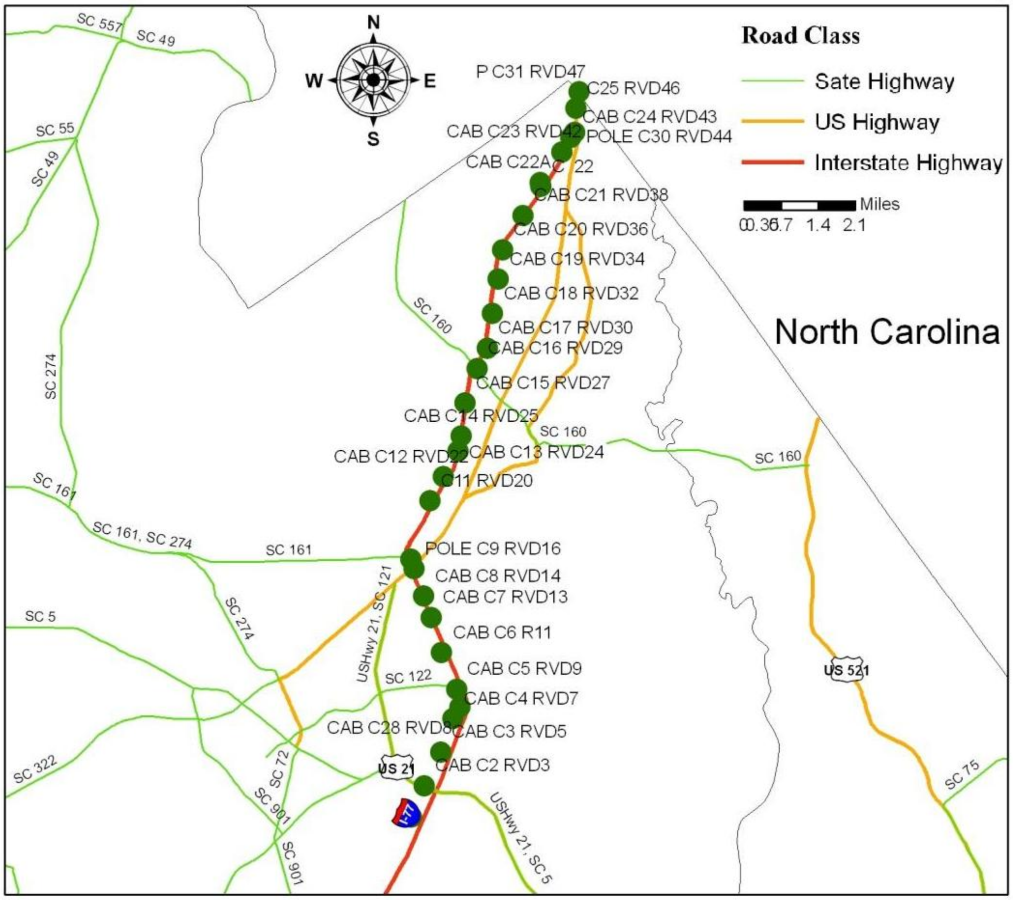


Figure C-16 Traffic Surveillance Devices in Rock Hill, SC

WiMAX Infrastructure Models

The traffic surveillance devices in Spartanburg, SC were divided into six sub-networks, each containing at a maximum five nodes within 2 miles, showed in Figure C-17. In this scenario, there would be a total of six fiber optic Internet connections required, and twenty-six WiMAX radio.

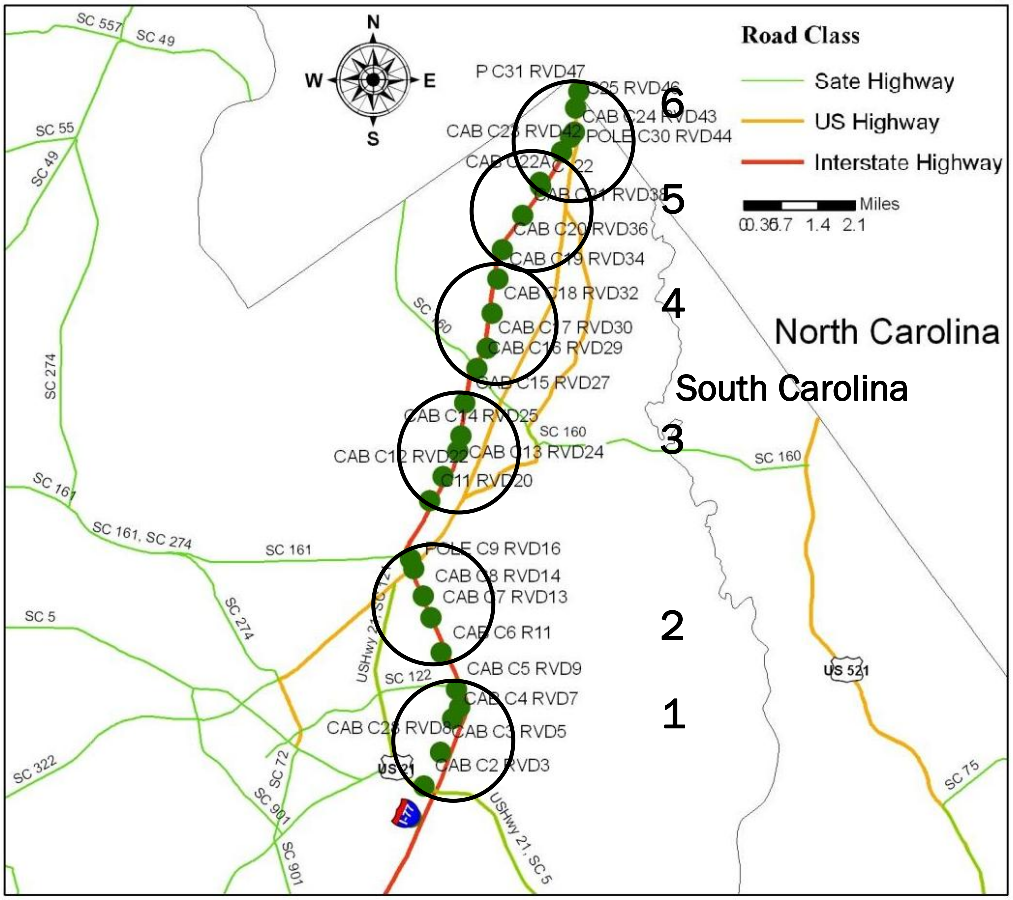


Figure C-17 WiMAX Infrastructure Network Model for Rock Hill, SC

Wi-Fi Infrastructure Network

The Wi-Fi infrastructure model shown in Figure C-18 divides the twenty-six nodes into twelve clusters. Each cluster would have its own fiber optic access.

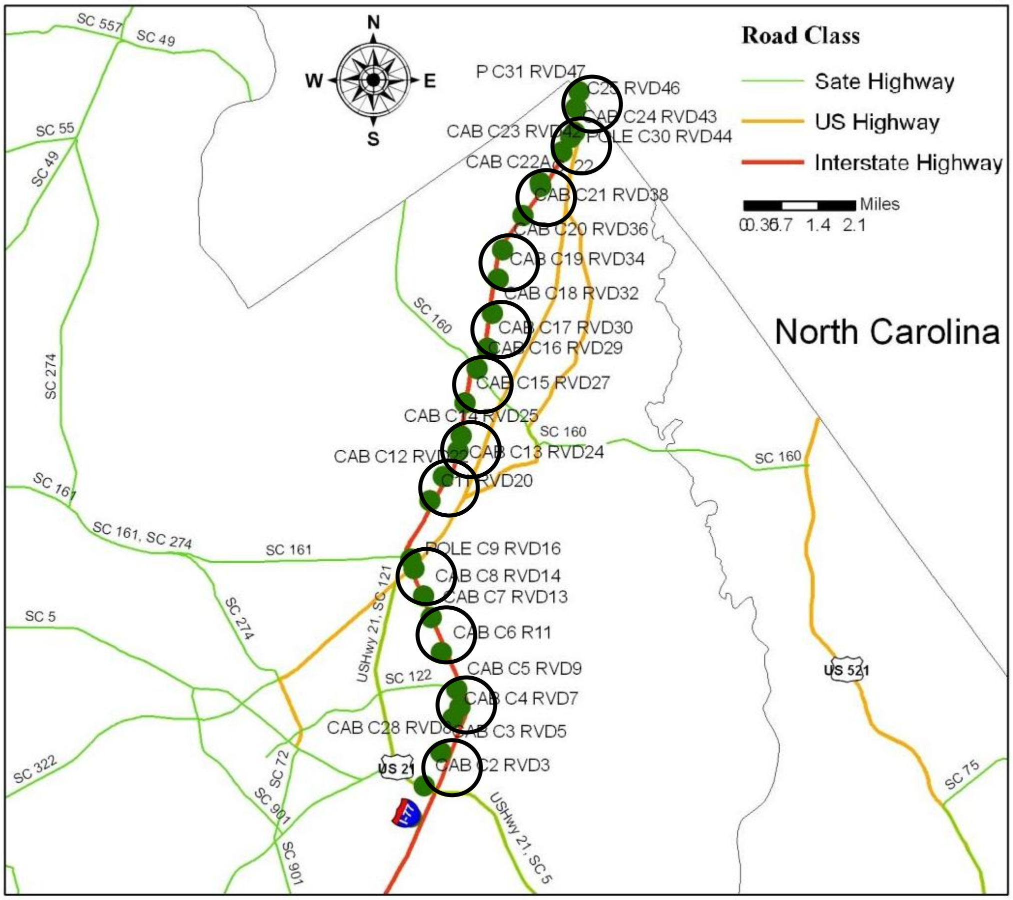


Figure C-18 Wi-Fi Infrastructure Network Model for Rock Hill, SC

Wi-Fi Mesh Network

The Wi-Fi mesh model shown in Figure C-19 divides the twelve clusters into two mesh clusters, each one contains six clusters. In this scenario, there would be a total of two fiber optic Internet connections required, and twenty-six Cisco 1310 access points.

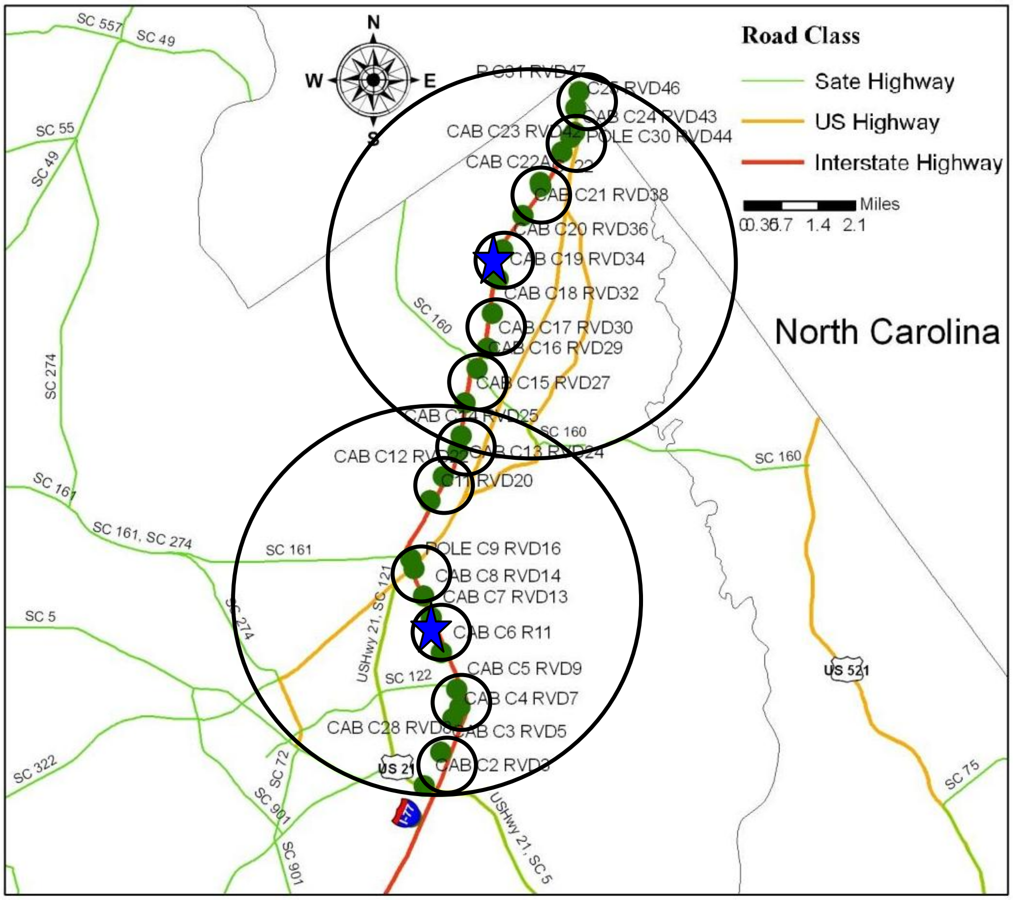


Figure C-19 Wi-Fi Mesh Network Model for Rock Hill, SC

<u>WiMAX Mesh Network</u>

The WiMAX mesh model shown in Figure C-20 divides the six clusters in the same manner as the Wi-Fi mesh model; with into two mesh clusters. Each node would have its own Motorola WiMAX base station, with each node in the clusters forwarding data from the other nodes. For this case study the access point locations with Internet access were chosen to minimize this maximum hop-count. In this scenario, there would be a total of two fiber optic Internet connections required, and twenty-six Motorola WiMAX base stations.

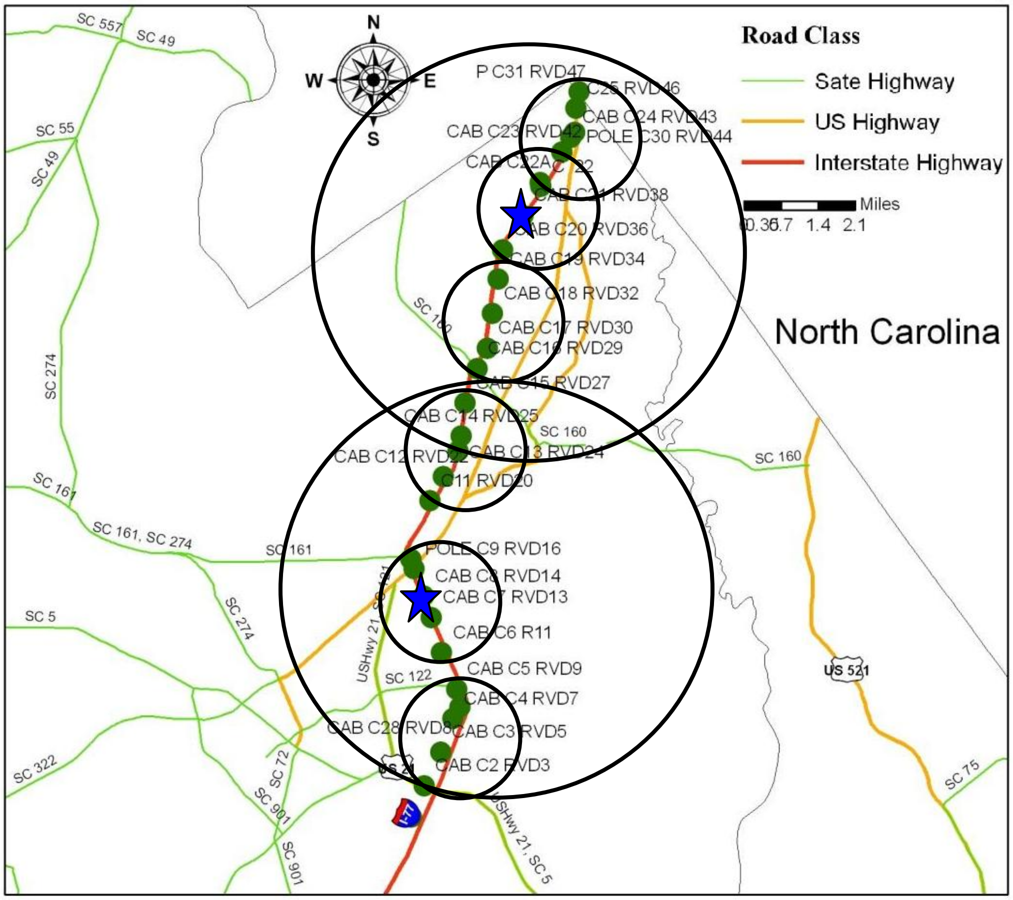


Figure C-20 WiMAX Mesh Network Model for Rock Hill, SC

Gaffney

The section of traffic surveillance system in Gaffney, SC consists of 28 traffic cameras and 20 radars to be wireless connected. All these devices are located on I-85, showed in the Figure C-21. Distance between each node is calculated to form sub-networks (also called clusters) that each device is with radio range and also to minimize the numbers of fiber optic connections. Detailed calculation of distance is available in the attachments.

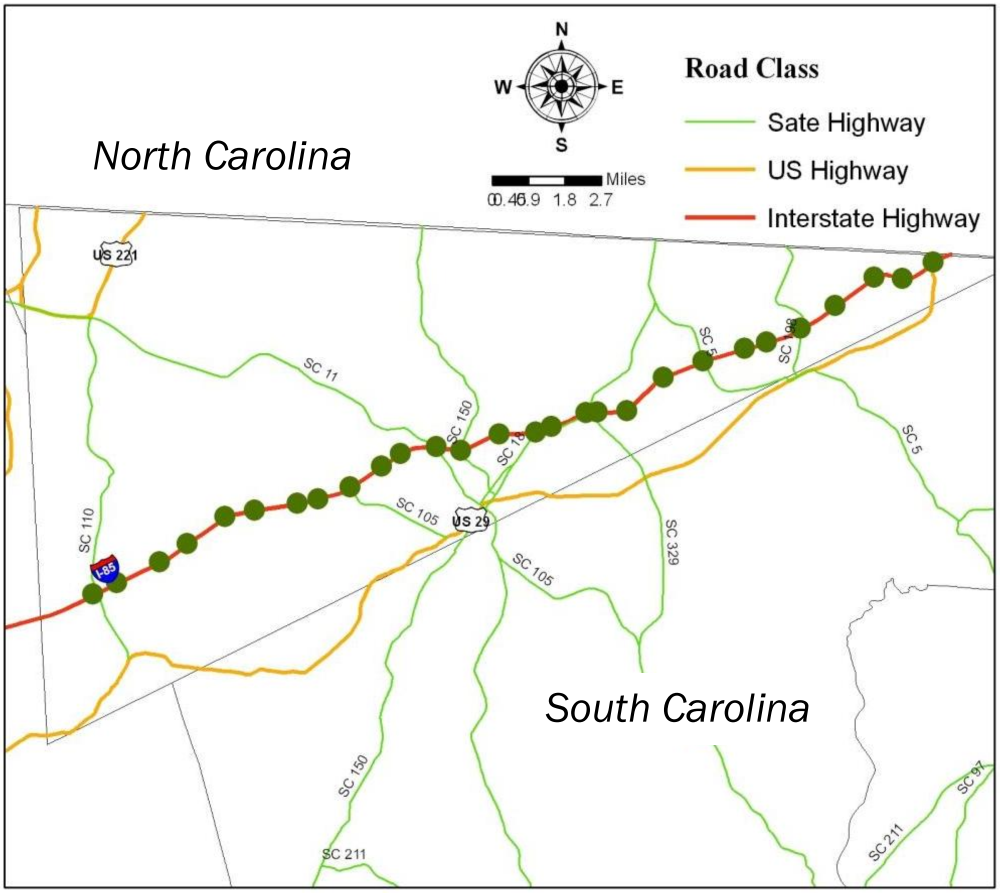


Figure C-21 Traffic Surveillance Devices in Gaffney, SC

WiMAX Infrastructure Models

The traffic surveillance devices in Spartanburg, SC were divided into ten sub-networks, each containing at a maximum four nodes within 2 miles, showed in Figure C-22. In this scenario, there would be a total of ten fiber optic Internet connections required, and 28 WiMAX radio.

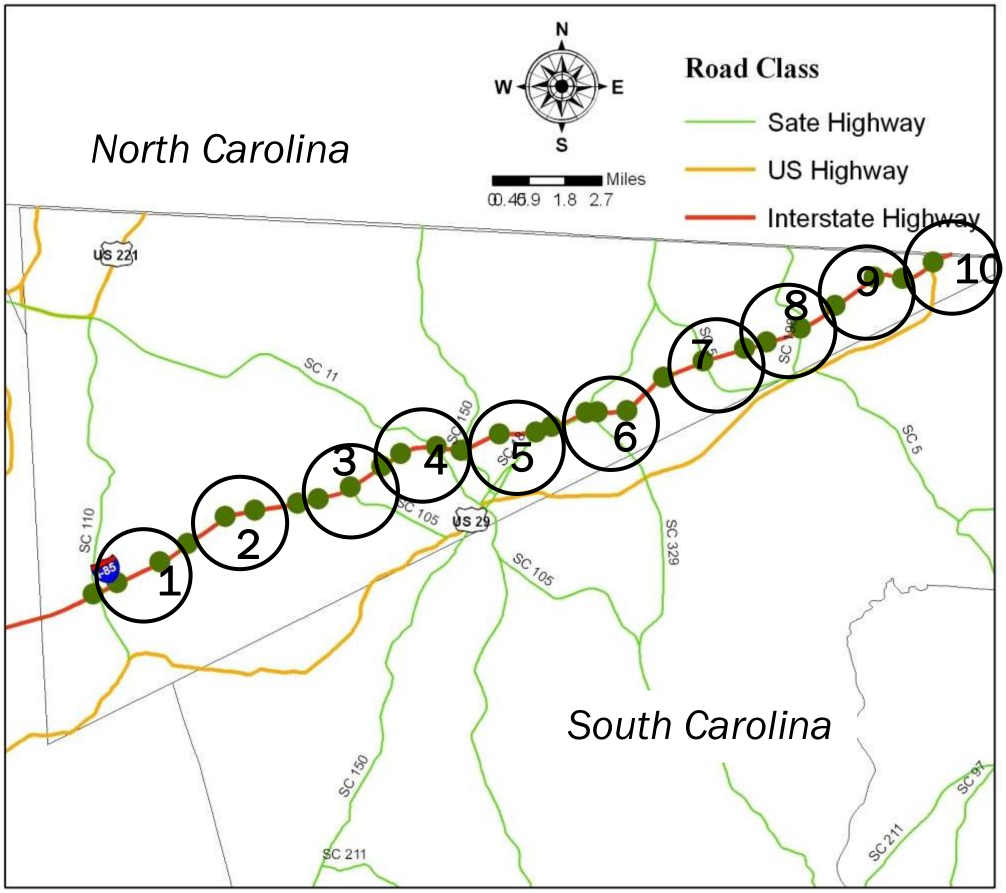


Figure C-22 WiMAX Infrastructure Model for Gaffney, SC

Wi-Fi Infrastructure Network

The Wi-Fi infrastructure model shown in Figure C-23 divides the 28 nodes into eighteen clusters. Each cluster would have its own fiber optic access.

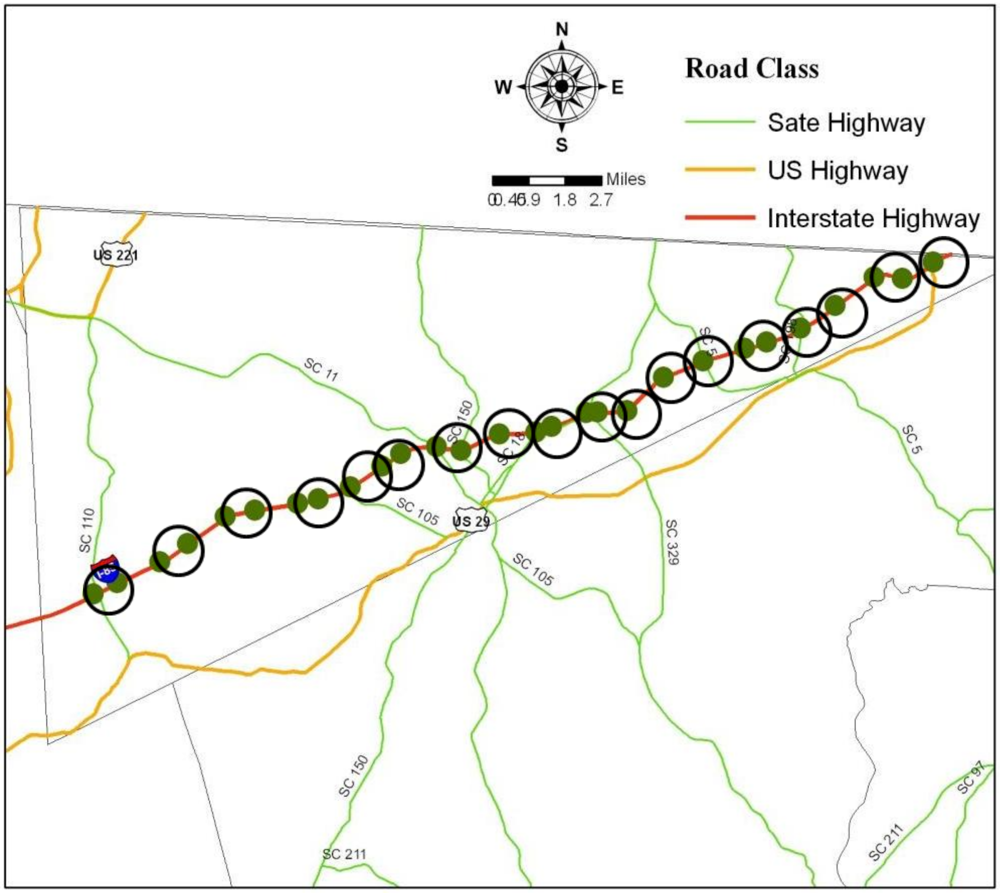


Figure C-23 Wi-Fi Infrastructure Model for Gaffney, SC

Wi-Fi Mesh Network

The Wi-Fi mesh model shown in Figure C-24 divides the 18 clusters into 3 mesh clusters, each one contains six clusters. In this scenario, there would be a total 3 of fiber optic Internet connections required, and 28 Cisco 1310 access points.

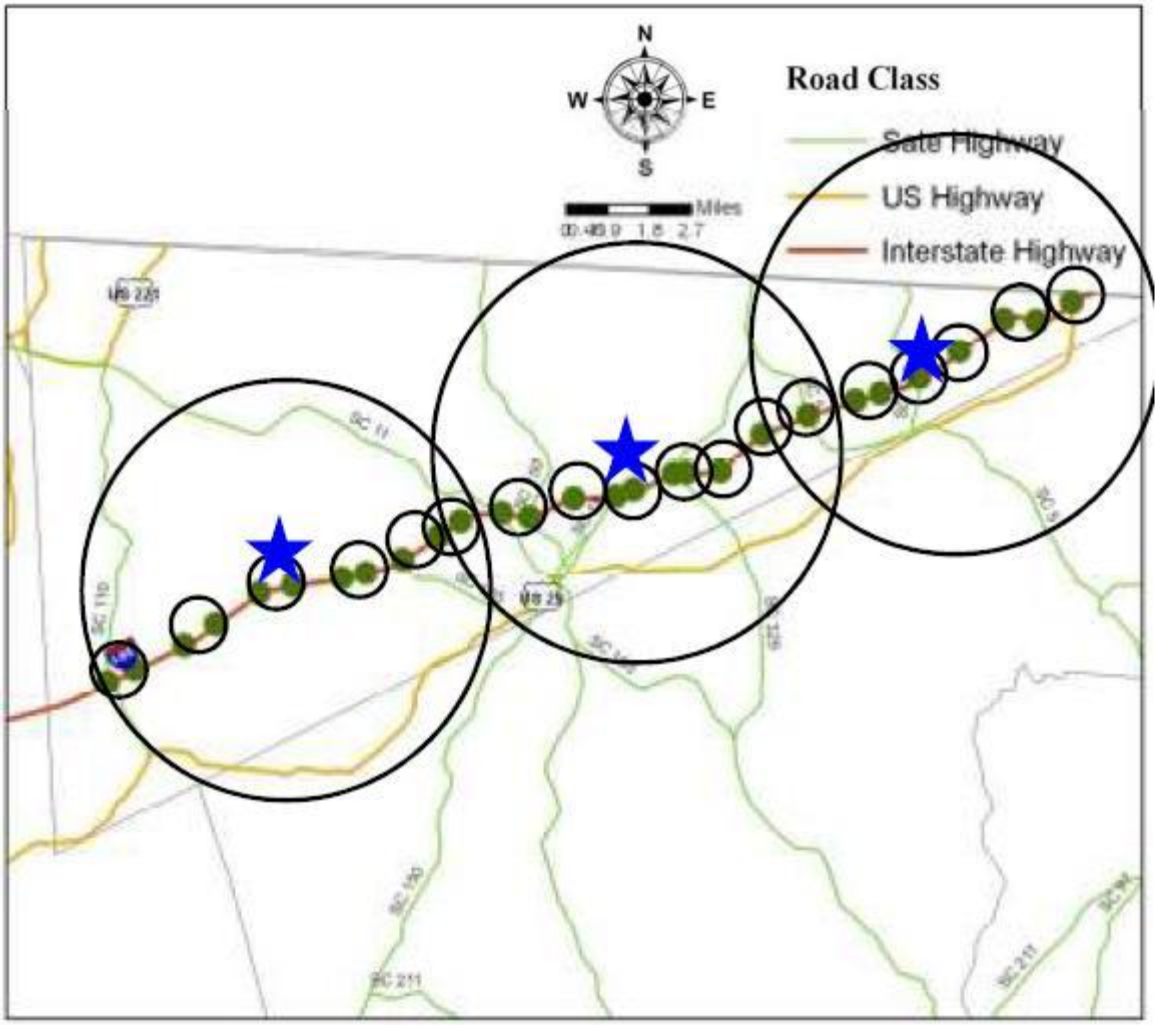


Figure C-24 Wi-Fi Mesh Model for Gaffney, SC

WiMAX Mesh Network

The WiMAX mesh model shown in Figure C-25 divides the ten clusters in the same manner as the Wi-Fi mesh model; with into three mesh clusters. Each node would have its own Motorola WiMAX base station, with each node in the clusters forwarding data from the other nodes. For this case study the access point locations with Internet access were chosen to minimize this maximum hop-count. In this scenario, there would be a total of three fiber optic Internet connections required, and 28 Motorola WiMAX base stations.

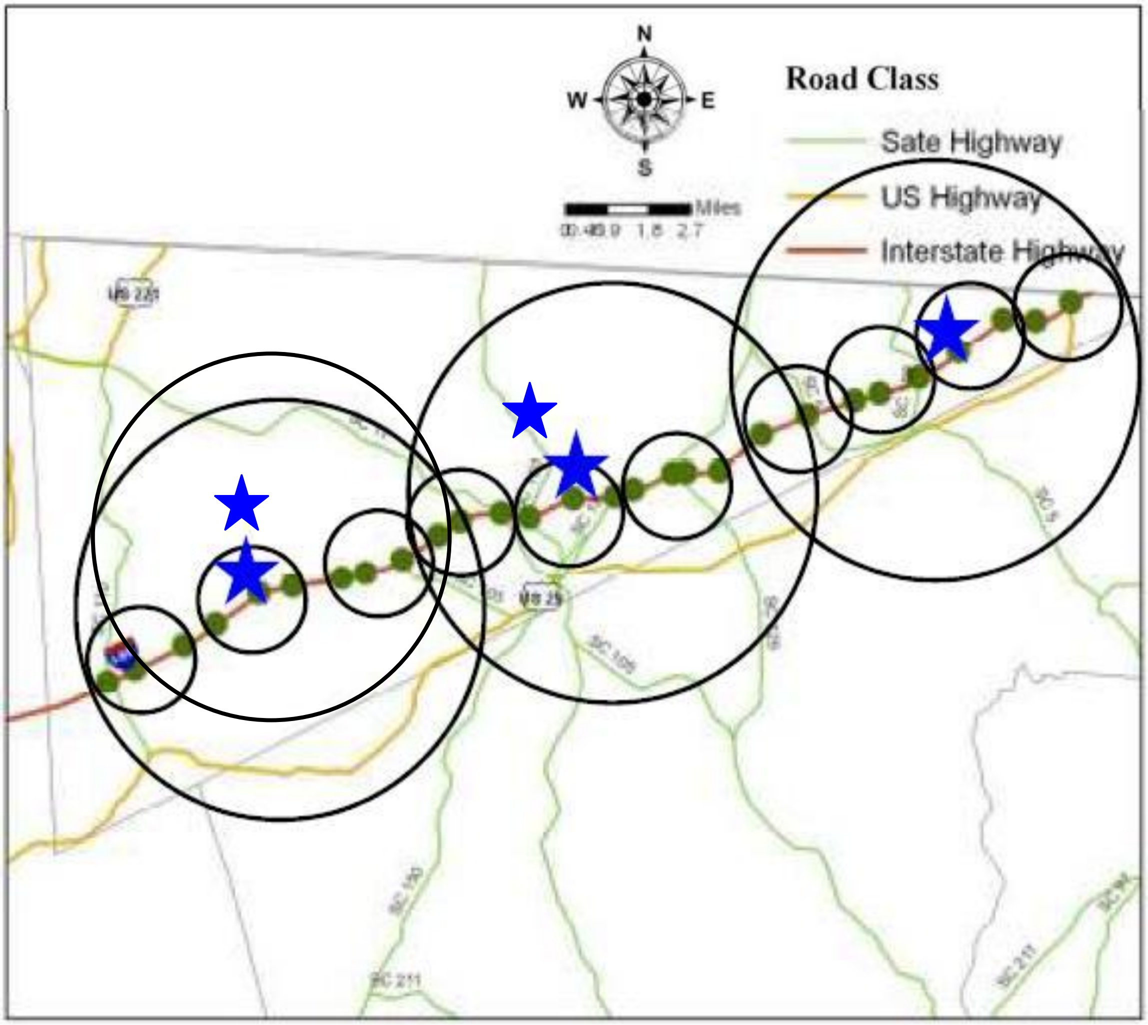


Figure C-25 WiMAX Mesh Model for Gaffney, SC

Appendix D Cost Estimation Details for NexusWorx

Deploying NexusWorx Software Licenses

For deploying Nexus*Worx* on your servers, Byers recommends two physical servers—one as the application server and second for database. The required 3rd party software is Oracle-Enterprise with Spatial 10G (10.2.0.4) 64-bit and Sun micro systems Jboss 4.2.3 application server. Byers is an embedded reseller of Oracle Enterprise -Spatial and can provide licenses at an 80% discount off of the Oracle MSRP. The price breakdown for the software licenses is as follows:

Editor License (Named User):	$ 10,000 (each)
Viewer User (Concurrent User):	$ 3,500 (each)
Oracle-Enterprise 10g with/Spatial embedded use:	$ 6,500 (based on minimum of 25 named users)

Annual maintenance is 20% off the software license cost including Oracle, if purchased via Byers Oracle ESL agreement. To provide support, Byers requires that the customer provide a method for remote access to the servers with the minimum ability to conduct webcasts from the server to Byers technical support. Table D-1 summarizes the recommended detailed server requirements. Recommended Detailed Server Requirements

Application Server		Database Server	
Number	Description	Number	Description
1	Quad Core Processor	2	Quad Core Processor
8	Gig RAM	8	Gig RAM
1	320 Gig HD	2	320 Gig HD (RAID)
1	Gigbit Ethernet	1	Gigbit Ethernet
2	Redundant Power Supply	2	Redundant Power Supply
OS	Red Hat Linux v4.6 Enterprise 64bit or Win-2008 Server 64bit	OS	Red Hat Linux v4.6 Enterprise 64bit or Win-2008 Server 64bit
Software	Jboss 4.2.3	Software	Oracle-Enterprise w/Spatial 10.2.0.4 64-bit

Byers' Implementation Service

Software Setup and Configuration: $6,000 – The cost to set up and configure the initial custom application, including custom attributes, themes, locates and database scheme modifications, and testing the changes. This is higher than our hosted cost because additional considerations must be addressed for customer server deployment.

*Landbase Load: $1,200** – This estimated cost will vary based on the source and size of the digital landbase. Byers is not a reseller of digital landbase but can contact, on behalf of our customers, various providers to obtain quotes and work with them to assure that the landbase features that are configured in Nexus*Worx* are supported.

Onsite Software Deployment: $900 (per day + plus actual travel expenses) – This is a required item for the implementation on your servers. The cost will cover Byers' technical support being on site for database set up and import, application deployment, user setup and initializing, and system admin training. The timeframe will vary based on each customer's IT expertise and knowledge of Oracle Spatial and Jboss tunning.

End User training: $4,200 (3 day course + plus actual travel cost) – This covers the cost for our standard 3 day training course for both Editors and Viewers. The 1st day is for both types of users, with the remaining 2 days for Editors only. **Note: Administrator training is conducted as part of the Onsite Software Deployment.**

Estimated Cost

Table D-2 outlines the typical cost for deploying Nexus*Worx* on your server. Some costs are estimated. This scenario considers running Linux servers.

NexusWors Software Deployment Cost

Description	**Units**	**Type**	**Unit Cost**	**Cost**
*Servers**	2	Per	$ 7,500.00	$ 15,000.00
Oracel Enterprise/Spatial ESL License	25	Per	$ 260.00	$ 6,500.00
Jboss	1		$ -	$ -
*Red Hat Linux- Enterprise Subscription**	2	Per	$ 800.00	$ 1,600.00
				$ -
NexusWorx Editor	0	Per	$ 10,000.00	$ -
NexusWorx Viewer	0	Per	$ 3,500.00	$ -
Starter Package (2 editors, 4 viewers)	1		$ 29,000.00	$ 29,000.00
				$ -
Description	**Units**	**Type**	**Unit Cost**	**Cost**
*Landbase License**	1	Per	$ 1,000.00	$ 1,000.00
				$ -
*Byers Onsite Implementation**	*4*	Days	$ 900.00	$ 3,600.00
Software Setup and Configuration	1	Lump	$ 6,000.00	$ 6,000.00
*Landbase Load**	1	Lump	$	$

			1,200.00	1,200.00
				$ -
NexusWorx Training	1	Per	$ 4,200.00	$ 4,200.00
				$ -
*Travel per day**	1	Lump	$ 2,200.00	$ 2,200.00
				$ -
NexusWorx Maintenance & Support	0.2	%	$ 6,500.00	$ 1,300.00
				$ -
				$ -

Provided By Byers

** Estimated*

Total Cost	$ 71,600.00

Appendix E Implementation Strategy

One of the objectives of this project is to set up guidelines which traffic personnel can use for deployment of wireless communication technologies in the field of ITS. This section presents an implementation strategy to aid the SCDOT with the design, deployment and implementation of wireless communication infrastructure for ITS.

As shown in the Figure E-1, the implementation process starts by reviewing literature, and conducting interviews/survey. Then network design should begin including technology, topology and protocol selection. The next step is to evaluate the performance and reliability of the designed network. The technology, topology and communication protocol supports different ITS applications with respect to performance and reliability requirements.

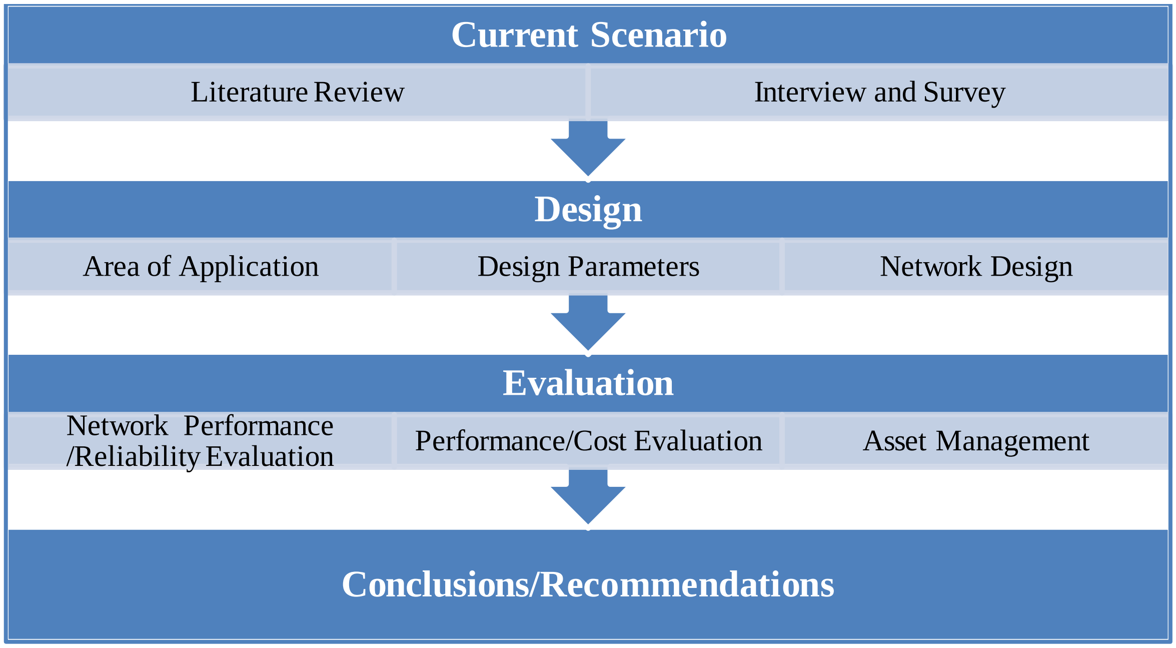


Figure E-1 High Level Implementation Process

E.1 Current Scenario

In Section two and four the literature review, interview and survey aspects of the Implementation Process were presented. As newer wireless technologies enter the marketplace, the SCDOT will need to reevaluate its selection methods to include those choices. Following the steps outlined in those chapters can guide researchers or practitioners to include additional alternatives into the selection process. More information regarding either current literature or interview/survey methods could be found using some of the references mentioned in the report.

***E.2** Design*

Figure E-2 demonstrates the recommended design process to be employed in future implementations of communication systems for ITS. This figure expands on Figure E-1, specifically providing more details on the design part of the implementation process.

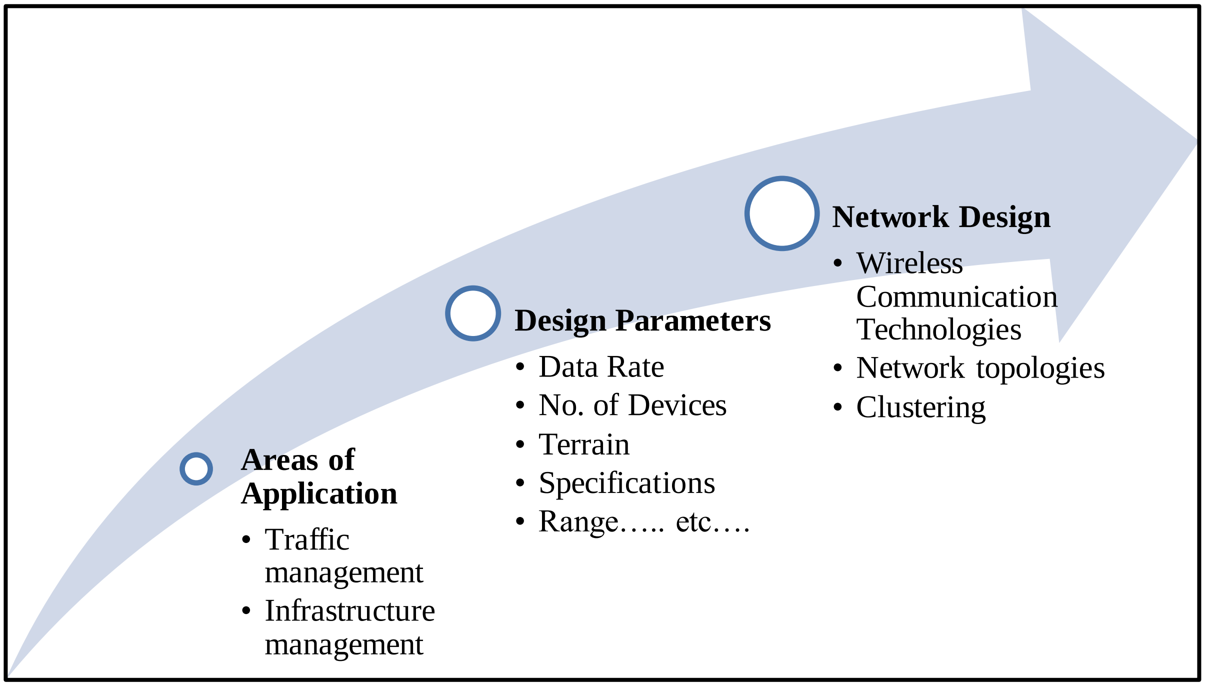


Figure E-2 Design Process

E.2.1. Areas of Application:

Wireless sensor networks have a wide range of applications. While common wireless sensor applications in the transportation field include traffic management and operation, wireless sensor networks can also be used in transportation infrastructure monitoring, structural health monitoring, pavement monitoring, etc. Significant opportunities exist for public agencies to collaborate with each other and share the same wireless network for different needs.

The first step in the design process is to identify the application areas, as shown in both Figures E-1and E-2. The National ITS architecture provides extensive resources for this stage of the design process. For instance, if the SCDOT wants to deploy wireless traffic network surveillance, that Natinoal ITS architecture specifies a market package, ATMS01 (Figure E-3), defining the communication and data flow needed between various subsystems and terminators. After identifying the appropriate market packages, engineers can modify the standard market package based on the project data flow requirements, performance and reliability needs.

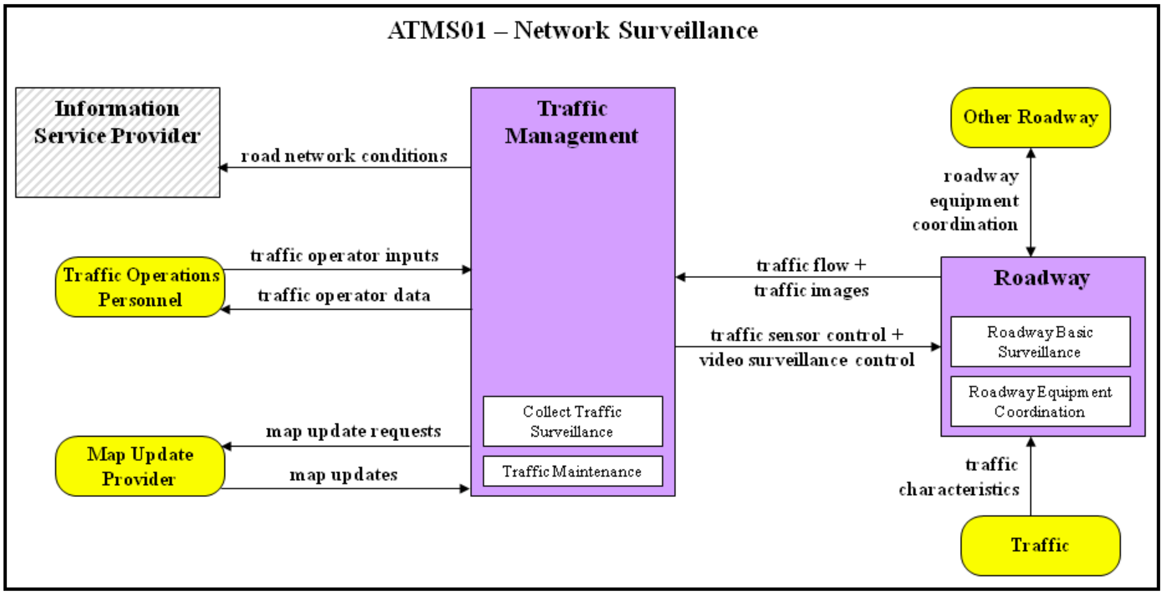


Figure E-3 Network Surveillance Market Package (USDOT 2009)

E.2.2. Design Parameters

The second step of the wireless system design process, as shown in Figure E-2, is identifying appropriate design parameters. These factors can includ data rate, the expected number of ITS devices, the local terrain specifications unique to the project, and desired transmission range. Since each element of an ITS system has a different role and performance environment, the following text presents common parameters for each: 1. Field devices 2. The environment and 3. Wireless communications.

1. ITS Field Device Parameters

When designing the wireless system for ITS application, it is necessary to be aware of specifications of various field devices. The report targeted online traffic monitoring as the ITS application. For this application we considered field devices such as cameras, radars and DMS. Their locations and spacing were key factors while deciding various communication parameters. Camera data rates had a significant impact on deciding the required bandwidth for the communication link. Designers should be particularly cognizant of the required data rates when designing such systems.

2. **Environmental and Exposure Parameters:**

   These environmental factors play a significant role in the performance of a wireless implementation. The following should be considered in this context.

   - Geographical terrain
   - Line of Sight obstructions
     - Natural obstructions like foliage
     - Man-made obstructions like buildings or towers
   - Exposure to Electromagnetic and Radio Frequency Interference

3. **Wireless Communication Parameters:**

   These are the most important design parameters which basically decide the wireless technology to be used and the suitable topology for implementation**.**

   - Practical bandwidth requirements can be calculated after knowing the specifications of the various ITS devices.
   - The frequency of operation can be decided after determining:
     - The acceptable amount of interference that can be tolerated
       - Can be due to other RF sources.
     - The use of a licensed or unlicensed band of operation
       - Unlicensed bands have a higher possibility of interference but are less costly.
   - Range required for the communication
     - Dependent on the location and placement of the field devices.

E.2.3. Network Design

Designing and planning an ITS network begins with determining the requirements that the various sensors, cameras, and other ITS components will necessitate. This part of the design process allows designers to discuss technology/topology/protocol selection, network design process, and equipment selection.

E.2.3.1. Wireless Communication Technologies

In Table E-1, every column contains pertinent characteristics for a network important for selecting wireless options to be used in an ITS environment. For additional details, Table 12 in Section 6 summarized certain technical specifications that determine what applications wireless technologies considered in this study, Wi-Fi, WiMAX and DSRC can reasonably support.

Table E-1 Major Characteristics of Wireless Communication Alternatives for ITS

Major Factors	Category	Others
Specification		Several IEEE Standards for one technology
Licensed	Licensed Frequency Unlicensed Frequency	Licensed has less interference but could be more costly
Frequency	200, 700, 900 MHz 2.4, 2.5, 3.5, 5.8, 5.9 GHz	The lower the transmitting frequency, the better the signal
Range		Depends on the antenna technology
Link Rate		Achievable rate is determined by many factors
Throughput		Normally less than the link rate
Architecture	Point-to-Point (P2P)	TMC to TMC
	Point-to-Multi-Points (P2M)	Cameras to TMC
	Mesh	Cameras to Cameras
EIRP		The maximum EIRP depends on the network architecture and frequency range

E.2.3.2. Wireless Network Topology

The network architecture, also known as topology, defines the network configuration. There are two commonly used network topologies, centralized and distributed, as shown in Figure E-4. Centralized, or infrastructure network, requires point-to-point connection from sensors to a controller or to a TMC. If the connection is cut-out, there is no alternative route available to relay the information from this particular sensor in the field to the controller or management center. On the right side of Figure E-4, in the mesh distributed network, sensors can still communicate with others even if one connection failed. This topology provides more flexibility to relay traffic information especially in emergency situations; however, it requires a more complex deployment. Detailed discussion about these two topologies can be found in Section 5 to assist practitioners in choosing the best topology for each application.

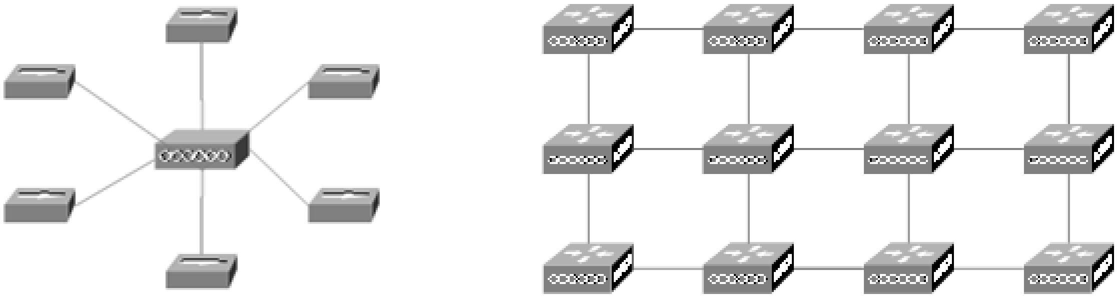


Figure E-4 Centralized (left) and Distributed (right) Network Topologies

When determining the network topology, it is also important to identify the communication protocols. There are many communication protocols available to be used for ITS applications. The National Transportation Communication for ITS Protocols (NTCIP) is a family of standards being jointly developed by AASHTO, ITE, and NEMA. These standards define the communication protocol between field devices, or between field devices to TMCs. Other common used IEEE protocols include TCP and UDP, which were used in this study. Each protocol has different performance characteristics. Traffic agencies need to select the one that can best serve their applications needs. Again, the National ITS Architecture provides resources to aid practitioners to selecting appropriate communication protocols for each application.

E.2.3.2. Network Clustering

After knowing the technology, topology and protocol, the designers can begin the clustering process as shown in Figure E-5. There are four main aspects to designing a wireless traffic monitoring network. First, it is important to know the number of traffic surveillance devices (eg. camera, radar detector) that will be connected to the network and the exact location of each. This is described as “device locations” in the flowchart. After the location and number of cameras is known, the bandwidth required to support all of the cameras in the network should be calculated. Next, the topology of the network, the distances between the cameras and their configuration, is calculated. Finally, an iterative process called “clustering” is conducted which allows the cameras to form groups that are within radio range and reduce the number of fiber optic connections required. If the clustering process leads to no solution, either additional access point can be added or the bandwidth requirements for each camera need reduction. Either of these choices leads to a restart of the clustering process. The process of clustering involves reducing the number of access points in the system until the number of access points required to support the cameras is at a minimum. The procedure begins with each camera as an access point, and then the access points are removed one-by-one and checked to ensure the system is still functional. After each iteration, the total bandwidth required at each access point is calculated and checked to ensure network stability. After repeating this process a solution will arise where each camera is connected to one access point and each access point serves multiple cameras; thus suggesting a cost-effective design. Examples of network design can be found in Section 6.

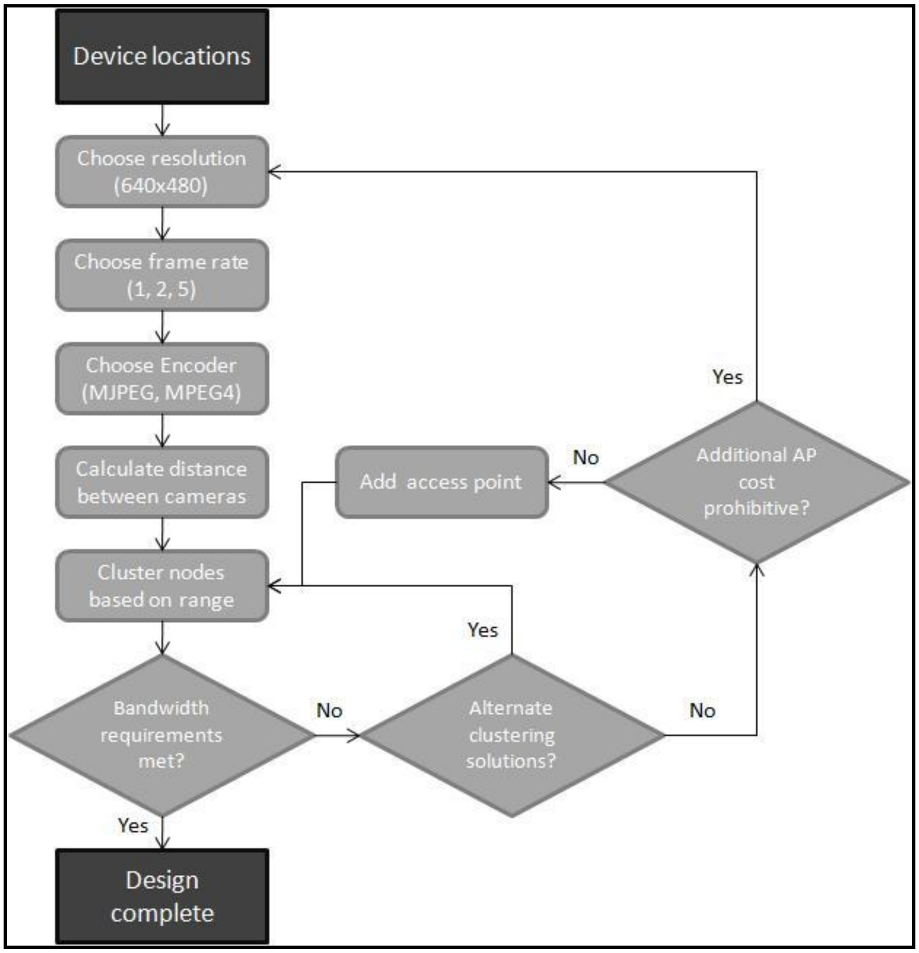


Figure E-5 Flowchart for preliminary network design

E.3 Evaluation

The next step in implementing an ITS communication system is to evaluate the merits of each alternative. Due to the ever-advancing array of technology, the best choices are not always clear and require quantitative analysis. This implementation plan recommends evaluating alternatives based on three factors: 1. network performance and reliability 2. Performance and cost and 3. Asset management.

E.3.1. Network Performance and Reliability Evaluation

This study analyzed the performance and reliability of the communication at two levels – subsystem level and system level. At the subsystem level the researchers conducted field tests in which they studied the desirable parameters of wireless communication. To analyze the overall system, a simulation setup using network simulator ns2 and the traffic simulator Paramics were used. The simulation setup provided a system level evaluation in which the effects of environmental parameters could be studied. The Figure E-6 demonstrates the hierarchy for evaluation.

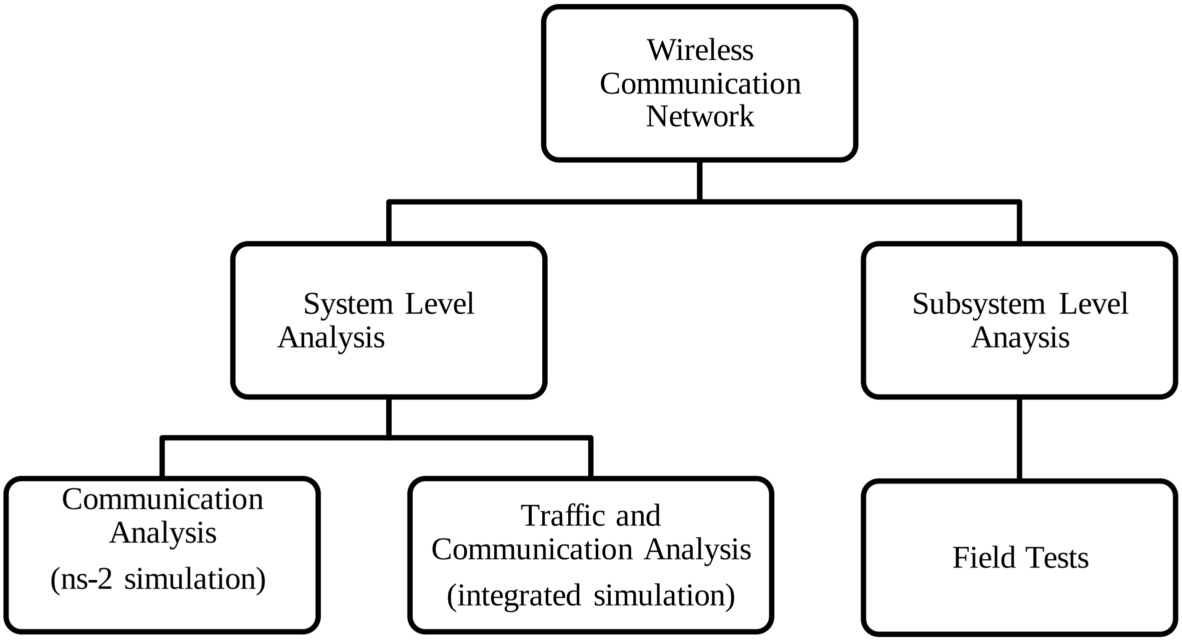


Figure E-6 Hierarchy of Evaluation

E.3.1.1.Sub-system level analysis: Field Tests

There are many factors that can affect the communication performance and reliability in the field. Three key factors that researchers recommend traffic agencies consider when planning for communication networks for transportation systems are: Distances, Environmental, and Technical.

1. Distances

The traffic sensors need to be placed within the wireless communication coverage range, which varies with technologies. If a longer distance is required, communication relays are needed to relay the traffic information from one sensor to the other. However, deployment costs increase when more relays are used. In addition, field test results indicate that an increase in the number of relays used increases the chance that data packets will get lost during transmissions. In a distributed network, the performance of the network is limited by the furthest sensor because it requires the most relays to transmit the information back to the local controller or TMC. Therefore, deploying relays at the maximum communication range in order to decrease the number needed will decrease the loss of reliability due to the use of relays. However, the field results also showed that throughput decreases when the distance between sensors (relays) increases. This creates a trade-off between performance and the deployment cost.

When using different communication technologies and topologies, the communication range is different. The performance-cost analysis from this study indicated that the Wi-Fi infrastructure and mesh network had the same throughput-cost ratio. Considering the number of fiber drops needed, a Wi-Fi mesh solution has the highest throughput-cost ratio, while the WiMAX mesh is the next best option. Since the WiMAX mesh was found to have higher throughput-cost ratio than WiMAX infrastructure, the case study showed that the total cost is always cheaper with a mesh solution. However, it has been stated previously in the report that the mesh topology does not provide the ease of expansion for future ITS devices compared to the infrastructure option.

This study did not compare the amount of excess bandwidth for each of the architectures, as it is extremely network specific. According to previously mentioned typical data rates of traffic cameras, both of the two infrastructure-based network architectures provide a significant amount of excess bandwidth for use in supplying connectivity to future ITS components. The WiMAX infrastructure provides the greatest amount of excess bandwidth which benefits the system’s future expansion. When several ITS devices are located on a single pole sending information simultaneously and sharing the bandwidth, WiMAX infrastructure can provide the most bandwidth upgrade space.

2. Environmental Factors

As mentioned previously, in the highway environment, many factors could impact the performance between two adjacent sensors. These factors include highway terrain, foliage coverage and weather. Field test results indicate that mountainous highway terrain significantly decreases the communication performance. Traffic agencies should either place the sensors closer to each other and over the highway terrain peaks or use the amplifier to amplify the signals.

For the highway segments that have intensive foliage coverage, amplifiers also can be used to increase the transmission distance of a signal. Amplifiers are normally installed on the sensor side and are categorized by how much they increase signal strength. The one used in this study is a HyperAmp 2401GI-500 amplifier that can increase the signal strength 500 mW (L-com 2009). Thus, if the sensor initially sends the information with 70 mW power, the total power with the amplifier is 570 mW.

3. Technical Factors

There are two key technical factors that need consideration when deploying a sensor network in the field, modulation rate and transmission power. Modulation rate is the speed at which data is transmitted in a carrier, which can be achieved through different modulation schemes. Higher modulation rates provide better throughput, so more data from the field can be transferred in real time. However, higher modulation rates are normally less robust to the background noise and interference, so more data packets get dropped. For each modulation rate, there is a threshold distance between the transmitting and receiving nodes, beyond which the performance is unreliable. For ITS applications, access points (or traffic sensors) should be deployed within the distance at a specific modulation rate to ensure effective data transmission for traffic management. For most modulation rates, the drop in performance occurs between 300 ft and 400 ft.

The second key technical factor is transmission power, which also limits the coverage range of the wireless communications between two sensors. It is ideal to keep transmission power to a minimum in order to keep traffic sensor costs low, yet higher power can support longer communication ranges where required.

There are many products available for either Wi-Fi or WiMAX network communications. The case study presented in Section 1 used the specifications of a Cisco product. It is important to note that each product has different performance specifications and costs and that these will change over time. Traffic agencies should choose them according to their specific needs and budgets. The field study results indicate that at the same location, the performance provided by different devices (WiMAX, Wi-Fi, and DSRC) is significantly different. Detailed information can be found in Section 5.

E.3.1.1.1 Field **Test Procedures**

Before deploying the wireless sensor network in the field, the SCDOT needs to conduct field tests to identify which modulation rate and transmission power the system should be operating at in order to meet the performance requirements for specific applications. Moreover, at certain locations, the effects of the foliage coverage and highway terrain need to be quantified. Table E-2 demonstrates the field test procedure used in this study which is recommended for future evaluation of ITS communication infrastructure by the SCDOT.

Table E-2 Field Test Procedure

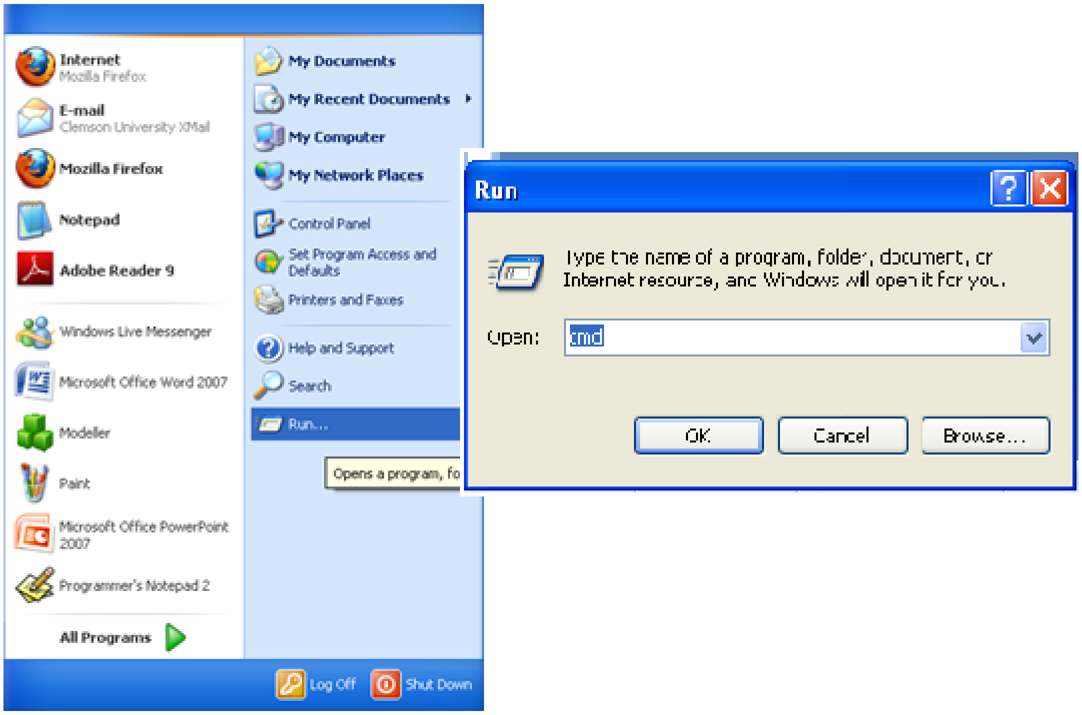
Steps	Details
1. Select the test location	Select the locations that the sensors will be placed. Select the locations will limit the highway terrain characteristics and foliage coverage effects.
2. Determine Distance	Start with a distance shorter than the maximum, eg. 200 ft
3. Place sensors (routers)	Routers can be used as sensors, and it is better to place them at a certain height above the ground. At least two routers are needed, one as a transmitter, the other as a receiver.
4. Determine Modulation Rates	Each technology can support several rates. Start with a lower rate. Set up the rate at the transmitter side.
5. Select Transmission Powers	Start with a higher power. Set up the power at the transmitter side.
6. Identify MOEs	Saturated throughput, packet delivery ratio, Receive Signal Strength Indicator (RSSI) and Signal-To-Noise Ratio (SNR)
7. Test the Performance	Set up the iperf server at the transmitter side Set up the iperf client at the receiver side Run iperf to start data transmission Run wireshark to record signal strength Change the distance, modulation rate or transmission power, then repeat step 1-6

Step 7 from table E-2 is particularly challenging and therefore described in detail next. The steps to setup Iperf are:

Step A: Download iperf.exe file from http://www.noc.ucf.edu/Tools/Iperf/

Step B: Install iperf on both the receiver and transmitter. Save the iperf folder under the C drive.

Step C: Click “Start- Run”, and type “cmd” in the pop-up window, and then click ‘OK’, as shown in Figure E-6.

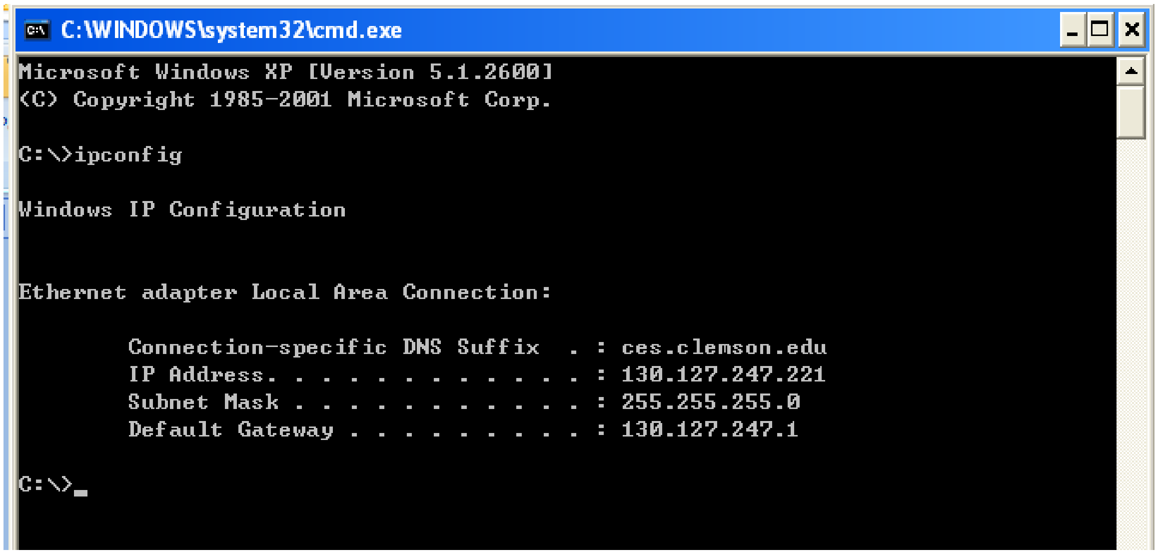


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

Figure E-6 Step 3

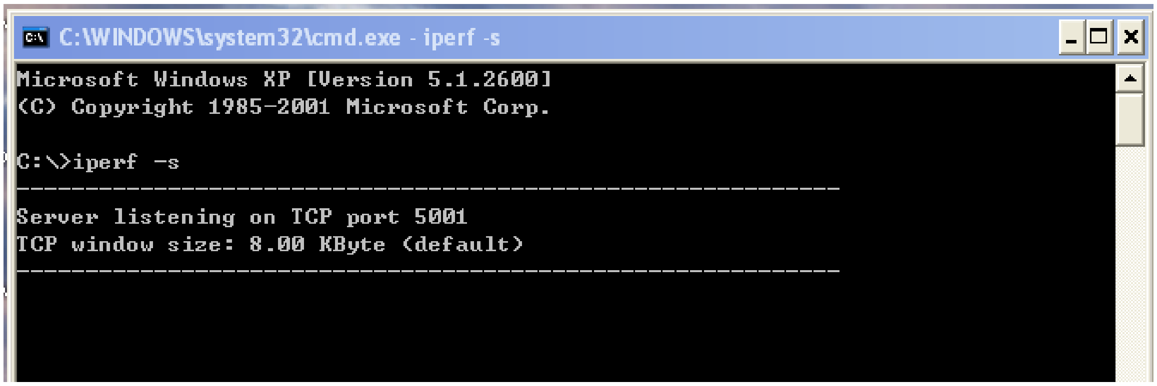
Step D: Get the ip address on the server side: Type “ipconfig” and then click “enter”, shown in Figure E-7



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : ces.clemson.edu
        IP Address. . . . . . . . . . . . : 130.127.247.221
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 130.127.247.1

C:\>_
```

Figure E-7: Get the Ip Address of the Server

Step E: Set-up server: type “iperf –s” and then click “enter”, shown in Figure E-8. Default protocol is TCP.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 8.00 KByte (default)
------------------------------------------------------------
```

Figure E-8: Set Up the Server

Step F: Set-up the client: type “iperf –c 130. 127.247.221 and then click “enter”. Now the server and client are connected.

Step G: If you want to test UDP protocol, type “iperf –u –s” on the server side.

If want to test different bandwidths, type “iperf -c 130.127.247.221 –b 2m”. This example sets up a bandwidth with a 2Mbps connection. To set up the test duration, type “iperf –c 130.127.247.221 –b 2m –t 60”. This example sets up one test duration as 60 seconds.

E.3.1.1.2 **From Field to TMC**

When connecting the field devices with the TMC wirelessly, there are certain factors that also require consideration. These factors include distance, foliage coverage, and highway terrain. Detailed impacts of these factors can be found in section 11.2.1. An amplifier is recommended to be used in certain locations to overcome the negative impacts on the signal strength.

Other than the factors in the field, there are three factors needed to be considered to ensure the performance of real-time video surveillance at a TMC: threshold buffer size, frame rates and number of users (monitors). Buffer is the computer memory that can temporally hold the video data. The video test results indicated that jitter values greater than 1 second will likely delay the video transmission so human eyes can observe a slow down or even disconnection. The value changes when using different wireless technologies. Evaluation tests are recommended to identify the threshold jitter value and set up the buffer size accordingly to ensure video smoothness.

Higher frame rates provide better video quality but require higher bandwidth. This study used a standard frame rate as an example. Pre-evaluation test is needed to identify the required bandwidth and buffer size. When more than one user are connecting to the same field device, such as several offices receiving video from the same traffic camera simultaneously, the performance could be significantly decreased compared to connections with one user. Sometimes, this performance can cause one user to receive smooth video while the others may suffer a slow-down or disconnection. A pre-evaluation test is needed to identify the number of users the system can support.

E.3.1.2. System Level analysis: Simulations

To obtain a comprehensive quantitative assessment of the dependency of a wireless traffic sensor network on the communication errors and topology decisions a simulation setup was used. Two types of simulations were carried out to analyze the system level performance: Communication Network Simulation using the software Network Simulator Version 2 (ns-2) and simultaneous simulation of communication network and roadway traffic and control simulation using an integrated simulator consisting of ns-2 and a microscopic traffic simulator PARAMICS. The traffic personnel can make use of similar simulations to evaluate some of the following Measures of Effectiveness (MOEs) from the system point of view:

- Communication MOEs
    - Throughput
    - Delivery Ratio
- Latency
    - Transportation MOEs
    - Incident Detection Rate
- Detection Time

Appendix F and Section 7 provide a better insight into the simulation procedure used. The following link can provide a better understanding of programming in ns2 (http://nile.wpi.edu/NS/). Appendix G contains the tcl file used in the ns2 simulation.

E.3.2. Performance/Cost Evaluation

While choosing a particular wireless technology, it is always necessary to evaluate the cost-benefit performance. Section 8 of this report deals with Performance/Cost analysis of the Greenville network. A similar strategy could be employed by the personnel before choosing a specific technology. In particular, it is important for future comparisons to include the anticipated costs of a communication system and the ability to provide the required throughput performance and allow needed future expandability. This study used a ratio of data bits per dollars, similar to a more-traditional benefit-cost ratio. The case example revealed that mesh networks provided better performance-cost ratios but they provided limited opportunity for future expansion. Thus, where costs were most important, mesh was best and where future expandability was most important, an infrastructure-based topology was best. Although these findings were specific to the study site, similar trends are likely throughout South Carolina.

E.3.3. Asset Management

The authors suggested the best options to adopt an asset management system for an efficient management of SCDOT ITS assets. The report also describes a multi-attribute methodology to evaluate performance of different asset management schemes. The findings of this study indicate that asset management of ITS systems would benefit most from using Enterprise-GIS systems. This type of system can leverage from current personnel experience in GIS and allow the management of multiple SCDOT assets, not just ITS, in one system.

The researchers recognize that implementing such systems take significant time and recommend that if immediate ITS asset management is sought, that a proprietary asset management system, Nexus Worx, be chosen. This software was rated only slightly less than Enterprise-GIS systems and still provides the functionality that the SCDOT requires for managing ITS assets.

If, ITS asset management is a long-term goal of the SCDOT, Enterprise-GIS can serve as an excellent management tool for keeping, organizing, and graphically-displaying all of the ITS devices owned and operated. For details on the analysis supporting these recommendations, see Section 9 of the research final report.

Appendix F Integrated Simulation

In the PARAMICS/ns-2 integrated simulator, each traffic sensor, detector or controller defined in PARAMICS is modeled as a node at a specified location in ns-2. In other words, the ns-2 node is a logical extension of the PARAMICS detector responsible for performing network-based operations.

To model traffic sensor/controller network, such as incident detection and traffic control procedures, algorithms are inserted into one of ns-2's application layer module, which is named as "***snet.cc***". On the other hand, data processing algorithms can be inserted either in PARAMICS' ***plugin.***c or ns-2's ***snet.cc***, or both can model node-specific real-time procedures for a node.

In this simulation, all incident detection algorithms are implemented in ns-2 module through ***snet.cc*** file, for which real-time data acquired by a PARAMICS detector is transmitted towards its matching nodes in ns-2 through the use of node-specific PARAMICS to ns-2 channel file.

The detection procedure in snet.cc can initiate communication on demand with other sensors and controllers using the ns-2 communication support. Moreover, nodes in ns-2 achieve network consensus on detection and control decisions, which are conveyed back to the matching PARAMICS detector through node-specific ns-2 to PARAMICS channel files.

The locked-step execution of ns-2 and PARAMICS is enforced to enable synchronized simulation. A synchronization file is defined to grant the execution permission for either PARAMICS or ns-2 at any time. The integrated simulator architecture is illustrated in Figure F.1.

Traffic detectors are normally placed in distance intervals longer than the typical communication range of wireless sensors, which depends on the technology. Each traffic sensor serves as the detector and communication relay both. This network deployment can be done straightforwardly in ns-2 by declaring additional nodes between the desired detector locations. Therefore, only a subset of simulated nodes in ns-2 is mapped to detectors in PARAMICS, while all nodes participate in the wireless ad hoc communication. In PARAMICS, users build, calibrate, and validate a traffic network. In ns-2, users define the wireless network protocol stack, the network topology, and the execution time and interval.

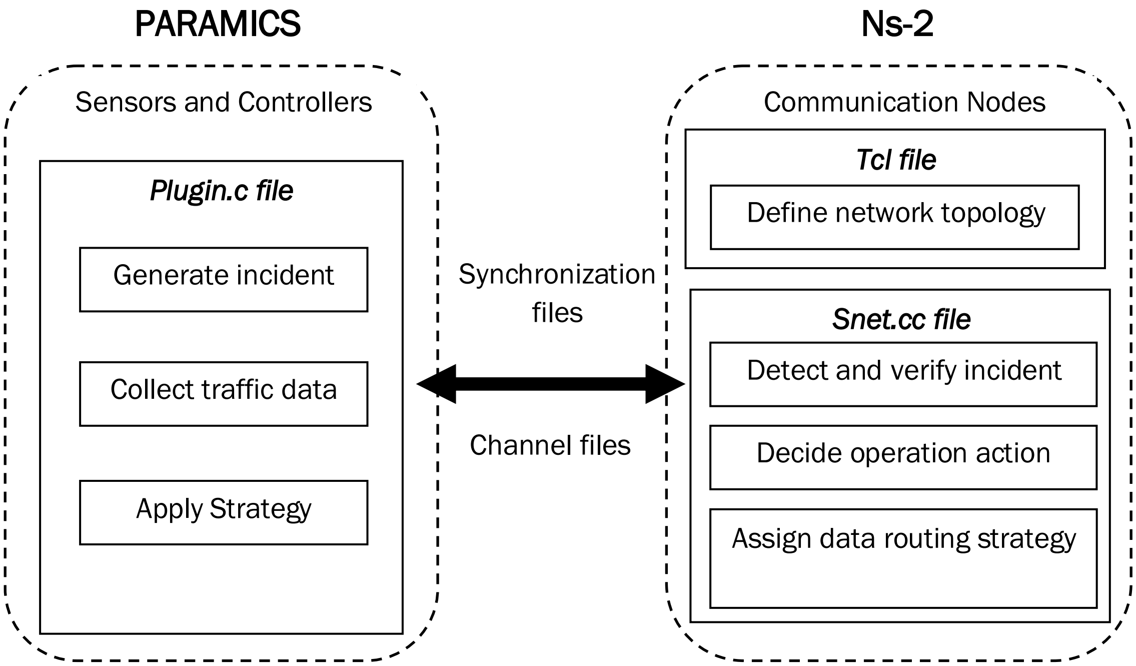


Figure F.1 Integrated simulator architecture

Appendix G Asset Management Survey

The Initial Survey Questionnaire for the requirements development

1. What would be some of the requirements for the ITS asset management system?

2. Are you currently using any asset management application for ITS?

    a) If yes-Are you satisfied with the present application? Could you elaborate on the current system?

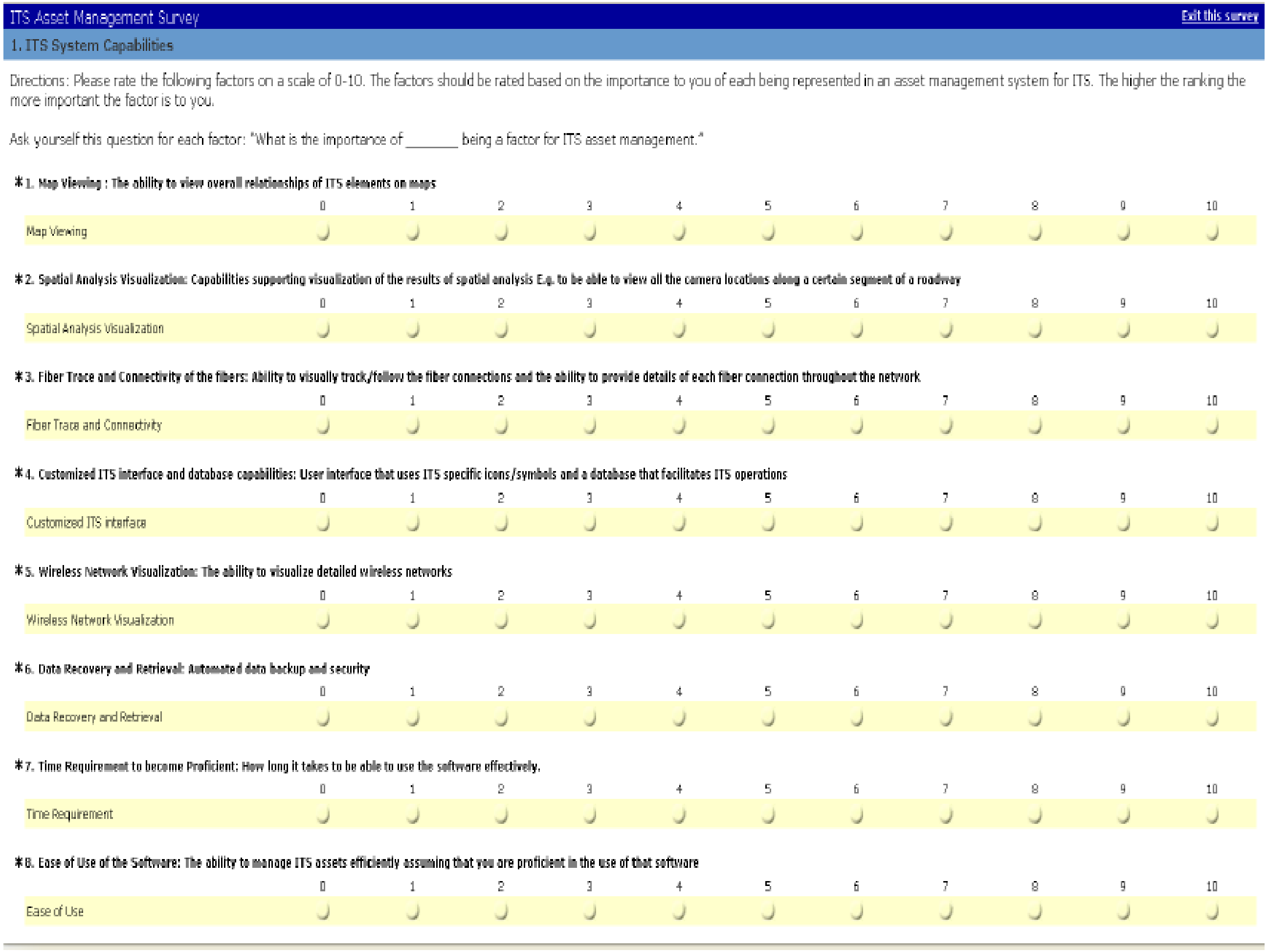
    b) If No-Are you interested or feel the need for an ITS asset management system?

3. Do you have any plan to update the present asset management application?

4. Do you feel that your current system performs well? Explain.

5. Can you provide us with the evaluation report or data or any documentation?

The Final Survey for the requirements of ITS systems



ITS Asset Management Survey

1. ITS System Capabilities

Directions: Please rate the following factors on a scale of 0-10. The factors should be rated based on the importance to you of each being represented in an asset management system for ITS. The higher the ranking the more important the factor is to you.

Ask yourself this question for each factor: "What is the importance of _______ being a factor for ITS asset management."

***1. Map Viewing : The ability to view overall relationships of ITS elements on maps**

	0	1	2	3	4	5	6	7	8	9	10
Map Viewing	○	○	○	○	○	○	○	○	○	○	○

***2. Spatial Analysis Visualization: Capabilities supporting visualization of the results of spatial analysis E.g. to be able to view all the camera locations along a certain segment of a roadway**

	0	1	2	3	4	5	6	7	8	9	10
Spatial Analysis Visualization	○	○	○	○	○	○	○	○	○	○	○

***3. Fiber Trace and Connectivity of the fibers: Ability to visually track/follow the fiber connections and the ability to provide details of each fiber connection throughout the network**

	0	1	2	3	4	5	6	7	8	9	10
Fiber Trace and Connectivity	○	○	○	○	○	○	○	○	○	○	○

***4. Customized ITS interface and database capabilities: User interface that uses ITS specific icons/symbols and a database that facilitates ITS operations**

	0	1	2	3	4	5	6	7	8	9	10
Customized ITS interface	○	○	○	○	○	○	○	○	○	○	○

***5. Wireless Network Visualization: The ability to visualize detailed wireless networks**

	0	1	2	3	4	5	6	7	8	9	10
Wireless Network Visualization	○	○	○	○	○	○	○	○	○	○	○

***6. Data Recovery and Retrieval: Automated data backup and security**

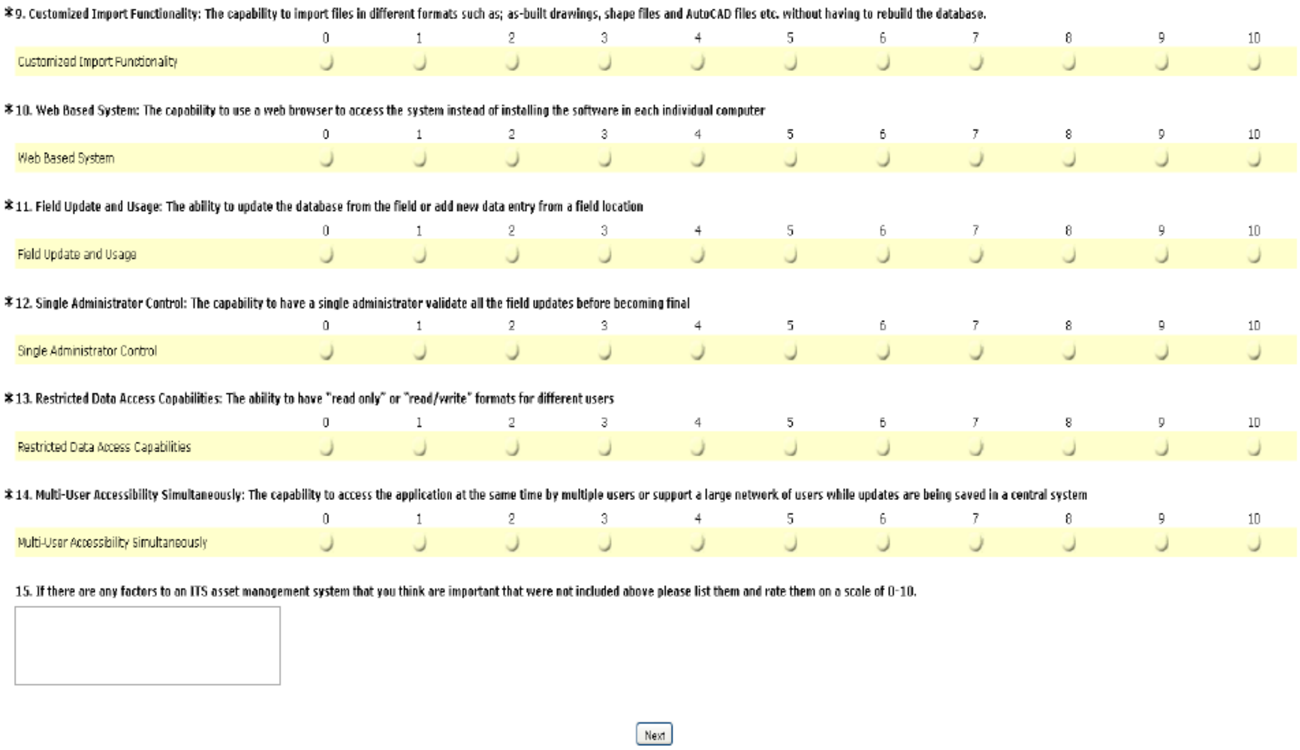
	0	1	2	3	4	5	6	7	8	9	10
Data Recovery and Retrieval	○	○	○	○	○	○	○	○	○	○	○

***7. Time Requirement to become Proficient: How long it takes to be able to use the software effectively.**

	0	1	2	3	4	5	6	7	8	9	10
Time Requirement	○	○	○	○	○	○	○	○	○	○	○

***8. Ease of Use of the Software: The ability to manage ITS assets efficiently assuming that you are proficient in the use of that software**

	0	1	2	3	4	5	6	7	8	9	10
Ease of Use	○	○	○	○	○	○	○	○	○	○	○



*9. Customized Import Functionality: The capability to import files in different formats such as; as-built drawings, shape files and AutoCAD files etc. without having to rebuild the database.

	0	1	2	3	4	5	6	7	8	9	10
Customized Import Functionality	○	○	○	○	○	○	○	○	○	○	○

*10. Web Based System: The capability to use a web browser to access the system instead of installing the software in each individual computer

	0	1	2	3	4	5	6	7	8	9	10
Web Based System	○	○	○	○	○	○	○	○	○	○	○

*11. Field Update and Usage: The ability to update the database from the field or add new data entry from a field location

	0	1	2	3	4	5	6	7	8	9	10
Field Update and Usage	○	○	○	○	○	○	○	○	○	○	○

*12. Single Administrator Control: The capability to have a single administrator validate all the field updates before becoming final

	0	1	2	3	4	5	6	7	8	9	10
Single Administrator Control	○	○	○	○	○	○	○	○	○	○	○

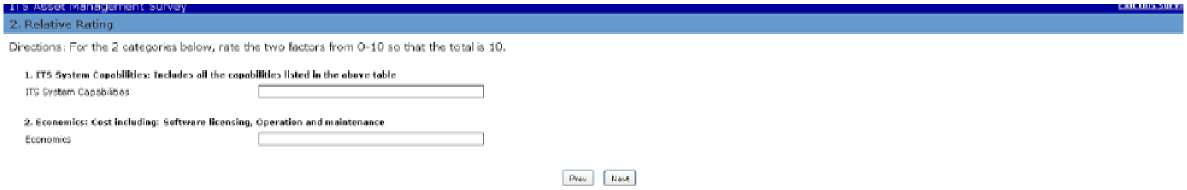
*13. Restricted Data Access Capabilities: The ability to have "read only" or "read/write" formats for different users

	0	1	2	3	4	5	6	7	8	9	10
Restricted Data Access Capabilities	○	○	○	○	○	○	○	○	○	○	○

*14. Multi-User Accessibility Simultaneously: The capability to access the application at the same time by multiple users or support a large network of users while updates are being saved in a central system

	0	1	2	3	4	5	6	7	8	9	10
Multi-User Accessibility Simultaneously	○	○	○	○	○	○	○	○	○	○	○

15. If there are any factors to an ITS asset management system that you think are important that were not included above please list them and rate them on a scale of 0-10.



ITS Asset Management Survey

2. Relative Rating

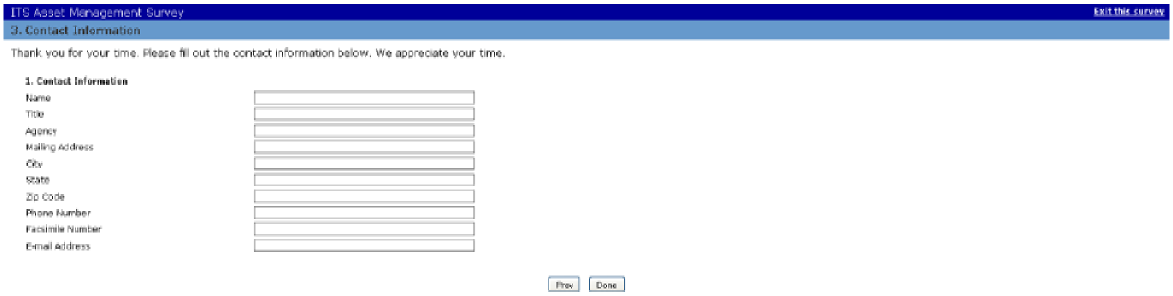
Directions: For the 2 categories below, rate the two factors from 0-10 so that the total is 10.

1. ITS System Capabilities: Includes all the capabilities listed in the above table

ITS System Capabilities

2. Economics: Cost including: Software licensing, Operation and maintenance

Economics



ITS Asset Management Survey

3. Contact Information

Thank you for your time. Please fill out the contact information below. We appreciate your time.

1. Contact Information

Name

Title

Agency

Mailing Address

City

State

Zip Code

Phone Number

Facsimile Number

E-mail Address

Appendix H ns-2 Source Code

```
# experiment.tcl
# Glenn Evans & Yan Zhou
# SCDOT Research project

# start time of the simulation
set simStart [clock seconds]

#
========================================================================
# Define options
#
========================================================================
set val(chan)          Channel/WirelessChannel    ;# channel type
set val(prop)          Propagation/TwoRayGround   ;# radio-propagation model
set val(netif)         Phy/WirelessPhy            ;# network interface type
set val(mac)           Mac/802_11                 ;# MAC type
set val(ifq)           Queue/DropTail/PriQueue    ;# interface queue type
set val(ll)            LL                         ;# link layer type
set val(ant)           Antenna/OmniAntenna        ;# antenna model
set val(ifqlen)        50                         ;# max packet in ifq
set val(nn)            23                         ;# number of mobilenodes
set val(ps)            100                        ;# packet size (bytes)
set val(rp)            SnetRout                   ;# routing protocol
set val(adhocRouting)   AODV;
set val(x)             11000                      ;# size of grid, in X
set val(y)             4000                       ;# size of grid, in Y
set val(stop)          10900                      ;# stop time of simnulation
#set val(fnloc)         "./nodeLocations.txt"      ;# locations of the nodes
#set val(fnadd)         "./nodeAddresses.txt"      ;# addresses of nodes
#set val(fnFN)          "./nodeOutput.txt"  ;# output file names

#
========================================================================
# Main Program
#
========================================================================
set arg_1 cent_aggr
set arg_2 364000
set arg_3 1
set arg [lindex $argv 0]
```

```
set arg_4 1 ;# Number of Highways
#
# Initialize Global Variables
#
set ns_          [new Simulator]
$ns_ use-newtrace
set tracefd     [open tOut.tr w]

#set namtrace [open experiment1.nam w]
#$ns_ namtrace-all-wireless $namtrace $val(x) $val(y)

$ns_ trace-all $tracefd

# set up topography object
set topo       [new Topography]

$topo load_flatgrid $val(x) $val(y)

#
# Create God
#
create-god $val(nn)

#
# Create the channel
#
set chan_1 [new $val(chan)];

#
# Create mobilenodes
#

$ns_ node-config -adhocRouting $val(rp) \
        -llType $val(ll) \
        -macType $val(mac) \
        -ifqType $val(ifq) \
        -ifqLen $val(ifqlen) \
        -antType $val(ant) \
        -propType $val(prop) \
        -phyType $val(netif) \
   -channel $chan_1 \
        -topoInstance $topo \
```

```
            -agentTrace ON \
            -routerTrace ON \
            -macTrace ON \
            -movementTrace OFF

for {set i 0} {$i < $val(nn) } {incr i} {
           set node_($i) [$ns_ node]
    set ragent_($i) [$node_($i) get-ragent]
    set ifqq_($i) [$node_($i) get-ifq]
           $node_($i) random-motion 0
}



$ns_ color 0 red
$ns_ color 1 blue
$ns_ color 2 chocolate
$ns_ color 3 red
$ns_ color 4 brown
$ns_ color 5 tan
$ns_ color 6 gold
$ns_ color 7 black

#
# Define locations of fixed nodes
#
 $node_(0) set X_ 2700
 $node_(0) set Y_ 1900
 $node_(0) set Z_ 0

 $node_(1) set X_ 2785.37
 $node_(1) set Y_ 2070.73
 $node_(1) set Z_ 0

 $node_(2) set X_ 2977.44
 $node_(2) set Y_ 2084.45
 $node_(2) set Z_ 0

 $node_(3) set X_ 3169.51
 $node_(3) set Y_ 2098.17
 $node_(3) set Z_ 0

 $node_(4) set X_ 3361.59
```

```
$node_(4) set Y_ 2111.89
$node_(4) set Z_ 0

$node_(5) set X_ 3553.66
$node_(5) set Y_ 2125.61
$node_(5) set Z_ 0

$node_(6) set X_ 3745.73
$node_(6) set Y_ 2139.33
$node_(6) set Z_ 0

$node_(7) set X_ 3938.11
$node_(7) set Y_ 2155.18
$node_(7) set Z_ 0

$node_(8) set X_ 4142.38
$node_(8) set Y_ 2149.70
$node_(8) set Z_ 0

$node_(9) set X_ 4346.65
$node_(9) set Y_ 2144.21
$node_(9) set Z_ 0

$node_(10) set X_ 4550.91
$node_(10) set Y_ 2138.72
$node_(10) set Z_ 0

$node_(11) set X_ 4755.49
$node_(11) set Y_ 2133.84
$node_(11) set Z_ 0

$node_(12) set X_ 4934.76
$node_(12) set Y_ 2156.71
$node_(12) set Z_ 0

$node_(13) set X_ 5114.02
$node_(13) set Y_ 2179.57
$node_(13) set Z_ 0

$node_(14) set X_ 5300.00
$node_(14) set Y_ 2203.05
$node_(14) set Z_ 0
```

```
 $node_(15) set X_ 5485.98
 $node_(15) set Y_ 2226.52
 $node_(15) set Z_ 0

 $node_(16) set X_ 5671.95
 $node_(16) set Y_ 2250.00
 $node_(16) set Z_ 0

 $node_(17) set X_ 5858.84
 $node_(17) set Y_ 2273.48
 $node_(17) set Z_ 0

 $node_(18) set X_ 6031.10
 $node_(18) set Y_ 2294.82
 $node_(18) set Z_ 0

 $node_(19) set X_ 6203.35
 $node_(19) set Y_ 2316.16
 $node_(19) set Z_ 0

 $node_(20) set X_ 6375.61
 $node_(20) set Y_ 2337.50
 $node_(20) set Z_ 0

 $node_(21) set X_ 6547.87
 $node_(21) set Y_ 2358.84
 $node_(21) set Z_ 0

 $node_(22) set X_ 6716.77
 $node_(22) set Y_ 2382.32
 $node_(22) set Z_ 0


# Set up the connections between the nodes
for {set i 0} {$i < $val(nn) } {incr i} {
   # Set the UDP agent
   set udp_s($i) [new Agent/UDP/UDPsnet]

   $ns_ attach-agent $node_($i) $udp_s($i)

   # Set packet size for UDP
```

```
    ##$udp_s($i) set pktsize_ $val(ps)


    # Set the appilcation agent
    set snet_s($i) [new Application/Snet]

    # Attach the routing agent to the UDP agent
    $snet_s($i) attach-agent $ragent_($i)

    # Attach the application agent to the UDP agent
    $snet_s($i) attach-agent $udp_s($i)

    # Set the packet size for application agent
    $snet_s($i) set pktsize_ $val(ps)

    # This command is used to pass to the nodes application agent its identity
    # Basically using this there is a varable in the C++ code of snet.cc
    # that tells the node number
    $snet_s($i) set nodenumber_ $i

    # Argument specifying type of experiment
    $snet_s($i) type-exp $arg_1

    $snet_s($i) set roundnumber_ $arg

    # Argument specifying the rate of input trafic

    $ragent_($i) rate-exp $arg_2

    # Argument specifying type of experiment

    $ragent_($i) type_exp $arg_1

    # Argument specifying the run of  experiment

    $ragent_($i) run_exp $arg_3
}

# Setting the number of highways
$ragent_(0) Number_Highways $arg_4
$ragent_(22) Number_Highways $arg_4
```

```
#
# Define address of fixed nodes
#
$snet_s(0) addr IX1.0000.2.2
$snet_s(1) addr IX1.5095.1.2
$snet_s(2) addr IX1.5195.1.2
$snet_s(3) addr IX1.5295.1.2
$snet_s(4) addr IX1.5395.1.2
$snet_s(5) addr IX1.5495.1.2
$snet_s(6) addr IX1.5595.1.2
$snet_s(7) addr IX1.5695.1.2
$snet_s(8) addr IX1.5795.1.2
$snet_s(9) addr IX1.5895.1.2
$snet_s(10) addr IX1.5995.1.2

#This is the controller.The adddress does not match with snet.cc file

$snet_s(11) addr IX1.6100.1.2

$snet_s(12) addr IX1.6200.1.2
$snet_s(13) addr IX1.6300.1.2
$snet_s(14) addr IX1.6400.1.2
$snet_s(15) addr IX1.6500.1.2
$snet_s(16) addr IX1.6600.1.2
$snet_s(17) addr IX1.6700.1.2
$snet_s(18) addr IX1.6800.1.2
$snet_s(19) addr IX1.6900.1.2
$snet_s(20) addr IX1.7000.1.2
$snet_s(21) addr IX1.7100.1.2
$snet_s(22) addr IX1.7200.2.2

#
# Define filename of fixed nodes
#
$snet_s(0) filename TEMPORARY
$snet_s(1) filename C:\\det1.txt
$snet_s(2) filename TEMPORARY
$snet_s(3) filename TEMPORARY
$snet_s(4) filename TEMPORARY
$snet_s(5) filename TEMPORARY
$snet_s(6) filename TEMPORARY
$snet_s(7) filename C:\\det2.txt
```

```
$snet_s(8) filename TEMPORARY
$snet_s(9) filename TEMPORARY
$snet_s(10) filename TEMPORARY
$snet_s(11) filename TEMPORARY
$snet_s(12) filename TEMPORARY
$snet_s(13) filename C:\\det3.txt
$snet_s(14) filename TEMPORARY
$snet_s(15) filename TEMPORARY
$snet_s(16) filename TEMPORARY
$snet_s(17) filename TEMPORARY
$snet_s(18) filename TEMPORARY
$snet_s(19) filename TEMPORARY
$snet_s(20) filename TEMPORARY
$snet_s(21) filename TEMPORARY
$snet_s(22) filename TEMPORARY

# added by Joann in 11/13/09
$snet_s(1) send-to IX1.7200.2.2
$snet_s(7) send-to IX1.7200.2.2
$snet_s(13) send-to IX1.7200.2.2

for {set i 0} {$i < $val(nn)} {incr i} {
        $node_($i) color red
    $node_($i) shape box
        $ns_ initial_node_pos $node_($i) 1

        $snet_s($i) time_duration 3 START 90
        $snet_s($i) time_duration 3 END 110
        $snet_s($i) time_duration 4 START 130
        $snet_s($i) time_duration 4 END 150
}

for {set i 0} {$i < $val(nn)} {incr i} {
   $ns_ at 0.0 "$snet_s($i) start"
        $ns_ at $val(stop).0 "$snet_s($i) stop"
   $ns_ at $val(stop).0 "$node_($i) reset"
}


#Define a 'finish' procedure
proc finish {} {
   global ns_ namtrace tracefd
```

```
        global simStart

        $ns_ flush-trace
   close $tracefd
    #Execute nam on the trace file
    #puts "running nam..."
        #exec ../nam-1.11/nam VII_sp.nam &

        set simEnd [clock seconds]
   set execTime [expr $simEnd-$simStart]
        # display some statistics.. nice for very long simulations
   puts "Finishing ns... Execution time: $execTime seconds (End: [clock format $simEnd -
format {%d.%m.%y %H:%M:%S}])"
        exit 0
}

proc getthetime {} {
        set now [exec date]
        puts stdout "$now"
}

puts "Setting up finish to run at time $val(stop)"
$ns_ at $val(stop).0001 "finish"
###$ns_ at $val(stop).0002 "puts \"NS EXITING...\" ; $ns_ halt"

#puts $tracefd "M 0.0 nn $val(nn) x $val(x) y $val(y) rp $val(adhocRouting)"
#puts $tracefd "M 0.0 sc $val(sc) cp $val(cp) seed $val(seed)"
#puts $tracefd "M 0.0 prop $val(prop) ant $val(ant)"

$ns_ at 0.0 "$ns_ set-animation-rate 150ms"
$ns_ run
```