5-2010

Modeling of On-line Traffic Control and Management Network for Operational and Communication Performance Evaluation

Yan Zhou
Clemson University, yzhou@anl.gov

Modeling of On-line Traffic Control and Management Network for Operational and Communication Performance Evaluation

A Dissertation Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Civil Engineering

By

Yan Zhou
May 2010

Accepted by:

Dr. Mashrur Chowdhury, Committee Chair
Dr. Kuang-Ching Wang, Co-Advisor
Dr. Jennifer Ogle
Dr. Ryan Fries

ABSTRACT

Communication systems are the backbone of every effective and reliable traffic control and management application. While traditional fiber optics and telephone communications have long been used in managing and controlling highway traffic, wireless communication technology shows great promise as an alternative solution in traffic management applications due to their suitability for deployment in rural areas, and their flexibility and cost-effectiveness for system expansion. However, the detailed characteristics of various wireless communication technologies and real performance in the field have not been systematically studied. To augment this existing knowledge so that traffic professionals may better utilize these technologies to improve traffic safety, mobility and efficiency, this study aims to 1) identify existing wireless communication technologies used in ITS, and potential wireless communication alternatives that can be widely used in ITS, 2) evaluate the performance, cost and reliability of existing and potential wireless communication technologies in supporting on-line traffic control and management functions, and 3) apply benefit-cost analysis to identify the impacts of using these wireless technologies to support on-line traffic management.

To achieve these research objectives, the author first conducted an interview to discover the specifications of existing communication infrastructures deployed for various ITS related applications and the usage of wireless technologies in different states. Moreover, the author proposed a network design process that considered wireless coverage range and network topology, followed with case studies utilizing Wireless Fidelity (WiFi) and Worldwide Interoperability for Microwave Access (WiMAX) technologies to support a traffic surveillance system in seven metropolitan areas throughout South Carolina. Field tests were conducted to evaluate the performance and reliability of wireless transmissions between adjacent sensor nodes. After that, the author applied a communication simulator, ns-2, to compare the communication performance of a traffic sensor network with WiFi and WiMAX technologies under infrastructure and mesh topologies, and environmental conditions. Based on these simulation results, the author conducted performance-cost analysis for these selected technologies and topologies.

The WiFi field test results indicated that wireless communication performance between two traffic sensors significantly degrades after 300 ft; this distance, however, may vary with the modulation rates and transmission power upon which the system operates. 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 sometimes affected by the characteristics of the client radio. The simulation analysis and benefit-cost analysis indicated a WiFi mesh network solution has the highest throughput-cost ratio, 109 bits/dollar for supporting traffic surveillance systems, while the WiMAX infrastructure option provides the greatest amount of excess bandwidth, 9.15Mbps per device, which benefits the system's future expansion.

This dissertation provides an important foundation for further investigation of the performance and reliability of different wireless technologies. In addition, research results presented in this dissertation will benefit transportation agencies and other stakeholders in evaluating and selecting wireless communication options for different traffic control and management applications.

DEDICATION

This dissertation is dedicated to my father Jianguo Zhou and my mother, Ping Yu.

ACKNOWLEDGMENTS

Far and foremost, great appreciation goes to my advisor Dr. Chowdhury. During my four-year study at Clemson, Dr. Chowdhury not only has guided me in becoming an excellent researcher, but also has taught me to become an intelligent, honest and responsible person. I will always be grateful to him for building self-confidence by encouraging me to engage in research with students not only from Clemson but also around the world. His guidance and encouragement was invaluable to me during the long process of the dissertation writing, as well as in academic publication. I also wish to thank him for his most kind assistance in helping me prepare my presentations so that I could share my results with colleagues at both national and international conferences, and in job interviews. Dr. Chowdhury's profound influence on me as a mentor and researcher has imbued in me a true sense of joy and intellectual rigor regarding the elegant beauty that innovative research can provide, when done correctly and well. I sincerely appreciative of the greatest trust Dr. Chowdhury placed in me by allowing me to manage several research projects as the graduate student leader. His invaluable experience that he has given me and the lessons I have learned enabled me to co-teach several of his classes, which ultimately improved my communication skills and enhance my confidence to engage in public speaking. Lastly, I appreciate his continuous encouragement and magnificent support in urging me to submit many external fellowship, scholarship and award applications. Without his guidance, my transition from ordinary to student to outstanding graduate researcher would have not been possible.

I would also like to thank my co-advisor, Dr. Kuang-Ching Wang for the countless hours he spent with me in researching important research subjects in the realm of Intelligent Transportation Systems, helping me to form effective solutions to these problems, sharpening my skills as a competent researcher, and assisting me in crafting my research papers. I am grateful for his endless patience and support shown during the preparation of this dissertation and my ancillary academic publications that were so critical to this document. I also wish to express my most heartfelt gratitude for his guidance and important suggestions to help me enhance my job interviewing skills.

Other members of my committee also deserve special acknowledgement. Dr. Ryan Fries, assistant professor of civil engineering at Southern Illinois University Edwardsville provided abundant assistance to me with both my course work and research when I first began graduate study at Clemson. His suggestions to improve the quality of this dissertation and other publications were most instrumental in my success. I am also grateful of the support and reference he has given to me in my job search. Additional thanks go to Dr. Jennifer Ogle, assistant professor of civil engineering at Clemson University, for always being there during the last four years whenever I needed assistance in either the classroom or in my research. I took the greatest pleasure in learning from her. Because of her great optimism and passion with which she pursues both her life and work, my uncertainties about my own ability to pursue a career in academia were greatly lessened. I also wish to acknowledge her unyielding support regarding my award applications and job search.

Special thanks go to my parents, Jianguo Zhou and Ping Yu. Without your magnificent inspiration, which instill in me an ethos of setting high standards and achieving them through hard work and preparation, I would never have been able to come to the United States to pursue my doctoral studies. Your boundless love, encouragement and unconditional acceptance have always been my strongest pillar and motivation.

Last, but not least, I wish to thank Mr. Godfrey Kimball, editor in the College of Engineering and Science at Clemson University for his assistance in the partial authoring of this dissertation. I also wish to acknowledge my fellow students and co-workers who collaborated with me on developing solutions to challenging and interesting problems in intelligent transportation system design, and constantly undertaking new research in our chosen area of endeavor. To Dr. Yongchang Ma, Xueying Kang, Lokala Sandeep, Glenn Hamilton Evans, Tupper Lee, Tahera Anjuma, Parth Bhafsa and Yiming He, thank you all for your friendship and hard work.

TABLE OF CONTENTS

Page

CHAPTER

LIST OF TABLES

Table Page

List of Tables (Continued)

LIST OF FIGURES

Figure Page

List of Figures (Continued)

Figure Page

List of Figures (Continued)

Figure Page

CHAPTER ONE

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 assist in making informed decisions and implementing appropriate operational strategies. Intelligent Transportation Systems (ITS) involves the integration of information technology with the existing traffic infrastructure to resolve transportation problems and improve 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 poor performed communication systems, especially during emergency conditions or at the key traffic infrastructures, will significantly affect the traffic management and operations, which not only cause traffic delays and air pollution, but also result in loss of property and increased risks of secondary crashes after traffic incidents. Therefore, a fast, reliable and cost-effectiveness communication systems used to transmit real-time traffic information is paramount for the traffic management and operation to improve traffic safety, mobility and efficiency.

1.1 Problem Statement

The National ITS Architecture presents possible communications between different subsystems via both wireline and wireless communications (USDOT 2007). Subsystems include the center (e.g., traffic management centers, public transit management, and emergency management), the field (e.g., sensor, controller) and the vehicle (e.g., personal, transit). 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 data and informations is transferred from the field to the Traffic Management Center (TMC) via fiber optic cable, either owned by the 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 the rural nature and lack of development in some areas where these components must operate. Because of the nature of system components, a wired system might be turned down completely in some cases under adverse conditions such as hurricane. However, a wireless system may still be capable to support partial transmission. Furthermore, with the increased demand of on-line traffic management system to cover the entire highway system, expansion of the wired system to wide scale can be costly. Moreover, the leased lines cost traffic agencies millions of dollars every year, and will increase during the 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 2008). Moreover, 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 flexiable 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 cut 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 surpporting various kinds of traffic control devices because many potential factors could degrade the communication performance, even shut down the connection entirely(Zhou^1 et al. 2009). There are also concerns of the functionability and reliability of using wireless technologies in adverse conditions such as bad weather (Zhou^2 et al. 2009), terrian and foliage covered area. 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. Furthermore, communication infrastructures are typically the most expensive part of a traffic management system (Gordon et al. 1993). For some wireless communication alternatives, constructing base stations and purchasing numerous client equipments could be very costly. However, this may be a better economic option for long term operational sustainability and large scale applications than satisfying public agencies' wireless communication needs from private enterprises. 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 technicallly feasibile, reliable and commerically cost-effective. As more and more regions throughout the United States move 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 be available to them. 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, long-term 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 can be widely used in ITS. The second objective is to evaluate both the traffic operation and communication performance of using existing and potential wireless communication technologies to support on-line traffic control and management. The third objective is to apply performance-cost analysis to identify the impacts of using these wireless technologies to support an on-line traffic management system.

1.3 Dissertation Outlines

The following categorized chapters present detailed study, analysis and discussion of the conducted research. Chapter 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. Chapter 3 presents the methodology the author utilized to interview selected public agencies, and to perform case study, field tests, simulation analysis and benefit-cost analysis. Chapter 4 presents a summary of interview responses. Case studies of using alternative communication technologies to support traffic surveillance systems of seven metropolitan cities are presented in Chapter 5. Chapter 6 and Chapter 7 present the results of field test and simulation results. The results of performance-cost analysis are discussed in Chapter 7. Lastly, chapter 8 summarizes and concludes the research findings, as well as presents the author's recommendation regarding the implementation of the current work and future research based on the analysis presented in this dissertation.

CHAPTER TWO

2 LITERATURE REVIEW

This chapter 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 telephony 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 WiFi, 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). The 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 and subsequently to optimize the video motion/quality relation.

This dissertation focuses on three selected emerging wireless technologies WiMAX, WiFi, and DSRC. The following contents in this section provide readers the general characteristics, strengths, and weaknesses of using each technology in ITS environments. It is also aimed 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, the WiMAX link rate can reach up to 70 Mbps, and coverage can extend over 10 miles. 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 Equipments (CPE), are similarly deployed as 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 WiFi

WiFi, 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 WiMAX with WiFi, 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 WiFi 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

WiFi hotspots (Dusit 2007). Theoretically, though the WiFi link rate can reach up to 54 Mbps, the coverage range is less than 0.4 miles (Broadcom 2006). Early WiFi 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 still requires further study.

If designed correctly, an optimized WiFi network can support multiple types of ITS components at relatively high throughputs. WiFi networks have the benefit of being the lowest-cost solution for providing wireless access to remote sites, and well-known WiFi technology can add redundant connectivity by enabling mesh mode operation of the access points. WiFi networks can support any ITS components that send non-critical data, as they do not provide any delay or bandwidth guarantees. Further, because WiFi 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 WiFi, 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 WiFi, 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 dramatically affect traffic management and operations, as well as vehicle-to-vehicle and vehicle-to-roadside communications in the future. This study not only evaluated the performance in the field through supporting various ITS devices within different network topologies, it also studied long-term issues such as spectrum usage, future proofing investments as technology cycles, and advanced technologies for creating wireless links that are robust to interference and jamming. Because of the advances of wireless communication have been rapidly changing, the design and implementation of ITS might be different today even compared to a few years ago. The Texas Department of Transportation (TXDOT) studied the trends and impact of market available wireless communication in future Advanced Transportation Management Systems (ATMS) deployment, while the state is moving forward to provide robust, scalable and cost efficient ITS devices (Brydia et al. 2008).

The three wireless communication technologies have already been commonly used for different ITS applications in the United States and around 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 the California DOT in the recent years for providing wireless communication services to travelers (Doucet 2008; Kanafani et al. 2006). 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 (Filis et al. 2007, Gray 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 consisting 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 is 13% lower than expected.

With the trend of deploying WiMAX network for ITS, some researchers have identified the operational feasibility in different applications (Chen 2007, Niyato and Hossain 2008, Bultitude et al. 2007, Wang 2007). Niyato and Hossain (2008) introduced an integrated WiMAX and WiFi network architecture for ITS by providing optimal priced mobile hotspot services. Chen (2007) described a WiMAX and WiFi 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.

2.3.2 WiFi

Several other transportation agencies have studied the usage of WiFi in an ITS environment (Ammana 2008; Brydia et al. 2008; Hwang et al. 2006). The USDOT, comparing WiFi and WiMAX for advanced public transportation systems, found WiFi 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 WiFi and WiMAX for statewide transportation operations (Ammana 2008). Their study found that compared to WiFi and the other wireless technologies studied; WiMAX can potentially provide more robust wireless communication links. The study also found WiFi and WiMAX networks to be very dependent on the terrain characteristics and available infrastructure for mounting antennas.

The City of Phoenix has deployed a WiFi 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 WiFi-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 WiFi 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 has been receiving increasing attention in worldwide because 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 Measurements

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 the communication network. 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). Through measuring the packet delivery ratio of a dense wireless sensor network in different environments, Zhao and Govindan (2003) found the delivery ratio to be affected by the communication range in all three environments. 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 different 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 configuration, which defines 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 pattern 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 reaction decisions.

Several problems arise from the existing centralized traffic surveillance network. 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. Furthermore, the response time of utilizing a centralized decision making system is generally long. Lastly, human operators who monitor the sensors endure high working stress, which in turn decreases the system reliability.

2.5.2 Distributed Network

Distributed control concepts are not new to traffic control systems. To locally optimize traffic delays locally, traffic signal controllers have for long been organized in local clusters. State-of-the-art of such traffic signal control systems include: Split, Cycle, Offset Optimization Technique (SCOOT) (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 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 failures and suffer from scalability issues. With distributed-only systems, there is no single point of control; however, it is more difficult to implement for system-wide optimization. On the other hand, there exist communication medium options, which can be grouped into two categories: wired and wireless.

2.5.3 Ad-hoc Network

Among various wireless communication topologies, wireless ad hoc network is 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 all wireless devices within range of each other to discover and communicate in peer-to-peer fashion without the need of fixed infrastructure to provide central access point (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 wireline system, such as fiber optic, can be very costly, in some cases may limit a large scale implementation. Wireless ad-hoc network provides a cost-effective alternative supplement to a wired system.

Wireless ad hoc network determines which nodes to forward data based on network connectivity; however, each sensor can only communicate with the other sensor within the communication range. As previously mentioned, the maximum communication range depends on the transmission power. Besides 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 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, WiFi, WiMAX and DSRC, have been used for various ITS applications worldwide and has shown great promises of providing broadband access, easy and cost-effective system expansion. However, traffic agencies have concerns about the real world performance of these potential technologies under various physical and environmental conditions while supporting different types of devices demanding a wide spectrum of bandwidths. The affect of different factors, such as distance, transmission power, foliage coverage, weather and terrain, to the wireless link performance are needed to be identified and quantified. Moreover, the maximum distance between the traffic sensors (devices or repeaters) that support reliable system performance requires intensive field studies. Additionally, some of the previous research studied the data gathered from sensors encompassed traffic flow information, such as speed and flow. These types of applications, which is of a light load and insensitive to communication 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.

Applying wireless technologies in specific ITS applications requires several steps beginning with 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 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 distance between WiMAX base stations and signal loss pattern, as presented in this dissertation, provides tools to investigate the potential of WiMAX highway traffic sensor network. Therefore, a general design method has not been conducted 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 have been limited researches 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 dissertation aimed to contribute to the knowledge of performance and reliability of different wireless technologies and topologies for ITS applications. As more information is needed in this area, the study will provide useful data essential for future ITS applications and research.

CHAPTER THREE

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 (U.S. DOT 2006). 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 dissertation focuses on the communication between centers and field devices, and between field devices, shown in Figure 1.

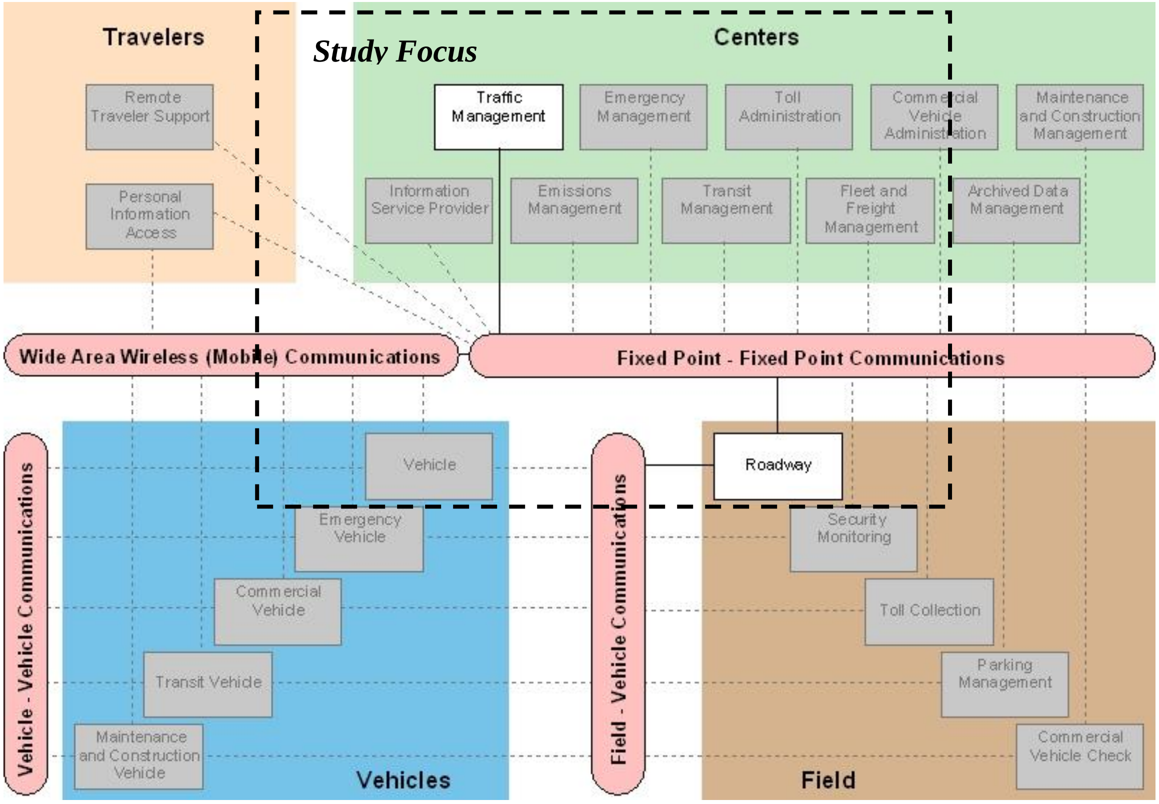

Travelers
Study Focus
Centers
Remote Traveler Support
Personal Information Access
Traffic Management
Emergency Management
Toll Administration
Commercial Vehicle Administration
Maintenance and Construction Management
Information Service Provider
Emissions Management
Transit Management
Fleet and Freight Management
Archived Data Management
Wide Area Wireless (Mobile) Communications
Fixed Point - Fixed Point Communications
Vehicle - Vehicle Communications
Vehicle
Emergency Vehicle
Commercial Vehicle
Transit Vehicle
Maintenance and Construction Vehicle
Vehicles
Field - Vehicle Communications
Roadway
Security Monitoring
Toll Collection
Parking Management
Commercial Vehicle Check
Field

Figure 1: Study Focus (U.S. DOT 2006)

This dissertation employs four different methods to achieve study objectives. First, through a comprehensive literature review, the study identified innovative 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. In order to evaluate different network options, the author 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. Two network topologies, mesh network and non-mesh or infrastructure network, were considered in the case study. 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; WiFi and WiMAX. Different factors that can affect the wireless communication performance and reliability in a real highway environment were considered in these tests. These factors included transmission power, modulation rate, 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 author conducted a quality requirements study of traffic video transmission from field to a center.

A simulation study was conducted to assess the throughput per device under the network topologies presented. Performance-cost analysis was conducted using the results generated utilizing the simulation output. In the end, based on the study results, the author developed recommendations for practical applications of the study findings. Table 1 demonstrates the research methods used in this study and their interconnection. Figure 2 shows how these tools were incorporated in carrying out major research tasks for this dissertation.

Table 1 Research Tools

Tools	Functions
Literature Review/ Interviews	• Identified innovative communication tools and strategies, and evaluation reports; • Conducted telephone/email interviews with selected public agencies with successful ITS programs on their experience with innovative communication options for ITS and any qualitative and quantitative impact data.
Field Tests	• Evaluated the performance and reliability of wireless alternatives under different highway terrain and foliage coverage conditions in a real highway environment; • Evaluated video quality requirements of an on-line traffic surveillance system and proposed suitable threshold value for quality control.
Case Studies	• Proposed 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.
Simulation Analysis	Network Simulation version 2 (ns-2) and an integration of ns-2 and a microscopic traffic simulator Paramics were utilized to evaluate communication and traffic operational control management performance
Performance-Cost Analysis	• Utilized benefit cost analysis to recommend best communication alternatives for ITS

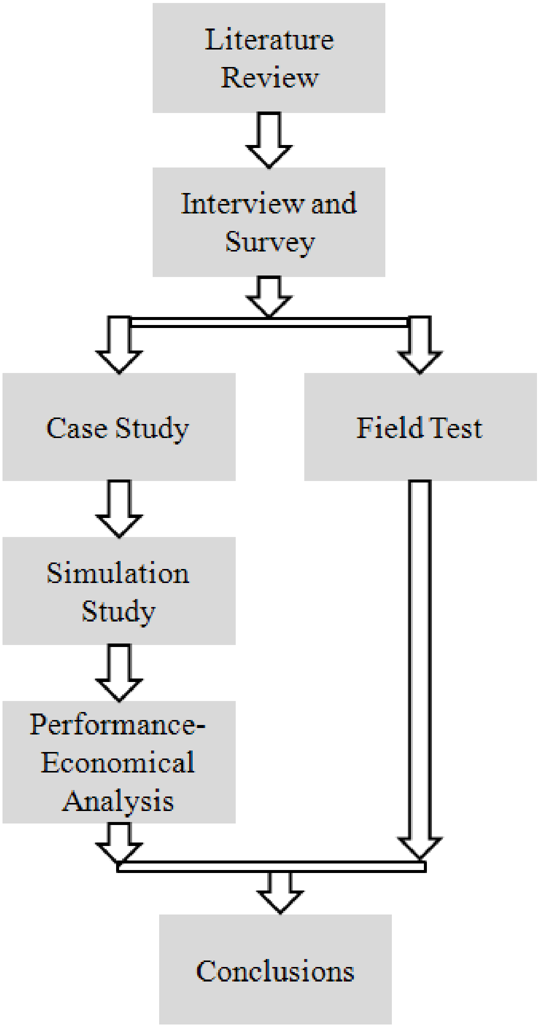


Figure 2 Research Methodology

3.1 Literature Review

The researchers reviewed literature, including reference books, white papers, journal papers, reports and magazine articles regarding the characteristics of wireless communication technologies and their existing applications in ITS. Reference books and white papers provided information on the characteristics and general applications of selected wireless technologies. Journal papers provided details of the performance and reliability issues, as well as potential future applications. Reports and magazine articles provided information on existing ITS applications. In the case study section, this study further complied data regarding the technical aspects of each technology in terms of licenses, frequency, range, link rate, throughput, architecture, network topology and line of sight (LOS) requirements. The information provided in this dissertation can help traffic agencies better understand wireless technologies. Based upon interview findings and literature review, the author summarized the characteristics, reliabilities issues, current and potential applications of three selected wireless technologies: WiFi, WiMAX and DSRC. The literature review summary was presented in Chapter 2.

3.2 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 showed 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. These agencies were selected for interviews based on because of their diverse ITS infrastructure. 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 of 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
- 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

3.3 Case Study

A case study was conducted to present a process of planning for a wireless infrastructure to support an existing traffic surveillance (traffic camera and radar detectors) system in seven metropolitan areas in South Carolina, as showed in Figure 3. Two types of technologies, WiFi and WiMAX combined with two network topologies, mesh and non-mesh (identified as infrastructure in the rest of the dissertation) were considered. Cost analysis of each of the architectures was discussed at Chapter 8. This dissertation presented case studies for two sites, Columbia and Greenville, while same studies for other 5 sites can be found in Appendix C. The output of the case study served as the foundation for the simulation study presented in Chapter 7.

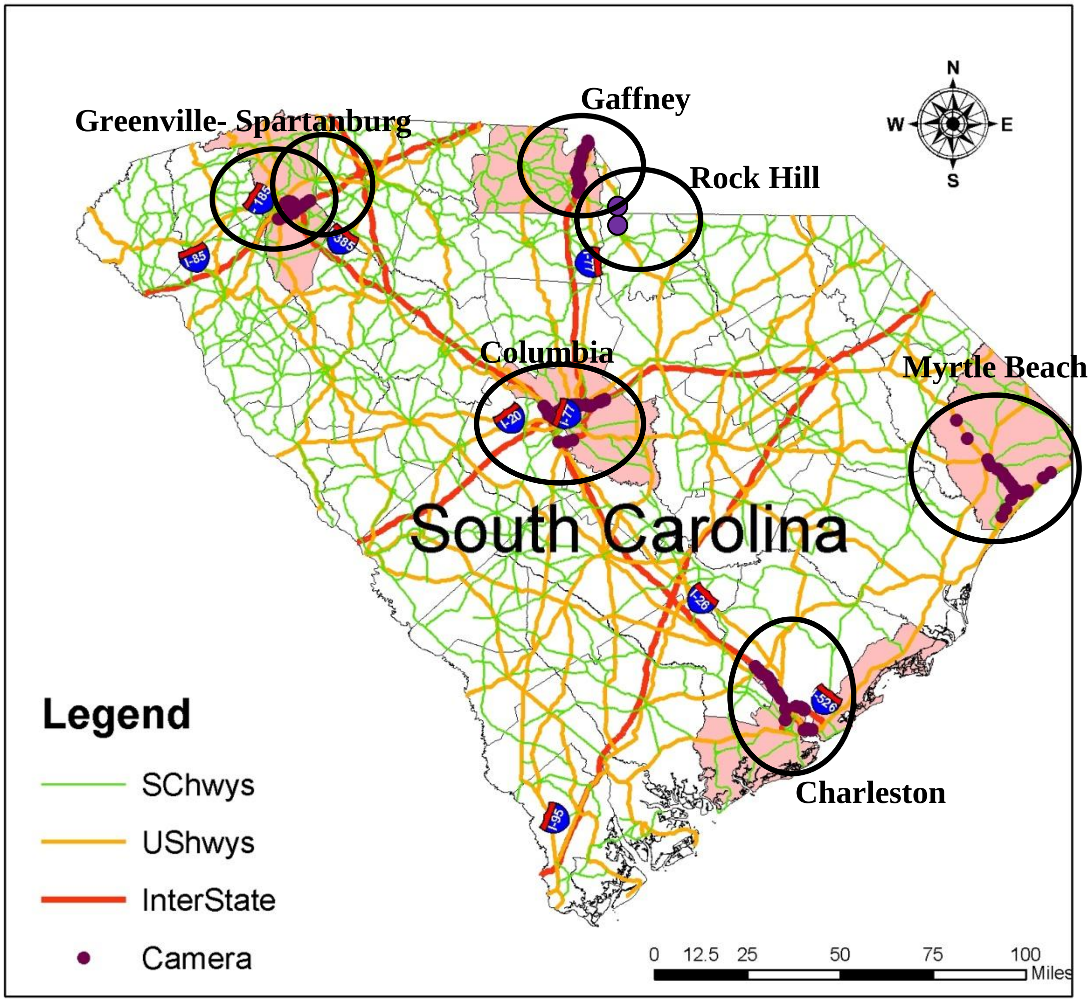


Figure 3 Seven study sites in South Carolina

3.3.1 Simple Network Design Procedure

The planning process for this study site was proposed in [Zhou et al. 2009], shown in Figure 4. 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 of traffic surveillance devices (eg. cameras, or radar detectors) that will be connected to the network and the exact location of each. This is described as the “device locations” in the flowchart. After information regarding camera locations 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” is to be conducted, allowing the cameras to form groups that are within radio range and that reduce the number of fiber optic connections required. The clustering process is repeated, until all cameras have their bandwidth supported. If the clustering process leads to no solution, either an additional access point can be added or the bandwidth requirements for each camera need to be reduced. 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 identified where each camera is connected to one access point and each access point serves multiple cameras.

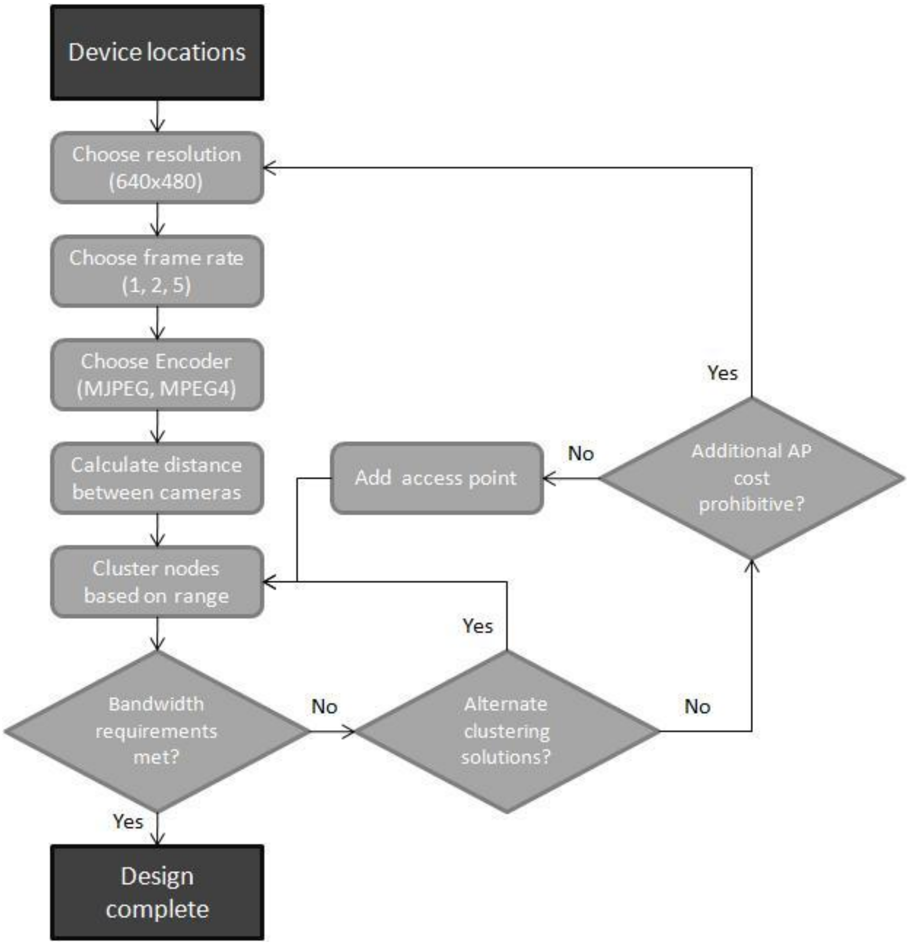

Device locations
Choose resolution (640x480)
Choose frame rate (1, 2, 5)
Choose Encoder (MJPEG, MPEG4)
Calculate distance between cameras
Cluster nodes based on range
Bandwidth requirements met?
Yes
No
Alternate clustering solutions?
Yes
No
Additional AP cost prohibitive?
Yes
No
Add access point
Design complete

Figure 4 Flowchart for preliminary network design

There are three types of traffic surveillance devices, traffic cameras (CCTV), radar detectors and dynamic message signs (DMS), considered in this study. Radar detector and DMS normally are implemented with traffic camera on the same pole, so each node considered in this study might consists of several different types of devices. Table 2 summarized the number of traffic surveillance devices and their locations in these seven major cities (SCDOT 2008).

Table 2 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

With the throughput requirements, estimated range for access points and network characteristics identified, this case study followed the proposed network design process presented in this dissertation utilizing WiFi and WiMAX technologies to support the traffic surveillance system in seven cities, as presented in details in Chapter 5.

3.4 Field Test

As mentioned earlier, this study focused on the communication between field devices and from field devices to traffic management centers. The traffic cameras and detectors are deployed along highways to detect and record traffic information in real time. Therefore, two types of information, video image and traffic data, were considered in the field study. Because each node is directly connected to other nodes (or local controllers) by a wireless interface, the detected traffic information is transmitted from one node to the next, finally arriving at a traffic management center (TMC) for further processing. This processed exchanged information communicated between roadside devices and traffic management centers can provide TMC with most updated traffic conditions for use in identifying incidents to reduce congestion and save lives. However, few inherent characteristics of a wireless network make it problematic for traffic management. First, each node 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 these measures also can be affected by different transmission powers. Traffic agencies are interested in identifying effective communication ranges to place the access points and sensors, and to operate the system in an optimized modulation rate. Moreover, it is important to quantify the effects of different factors in a highway environment, such as modulation rate, distance and transmission power, which provide traffic agencies a reference for future ITS applications. Besides data transmission between the field devices, this dissertation 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 author first conducted two types of field tests to evaluate the performance, reliability and feasibility of using WiFi and WiMAX for ITS applications in the field environment under prevailing roadway conditions. Then, the author conducted a study to assess the performance of wireless transmission between field traffic cameras and a monitoring station. Because DSRC is used more for vehicle to vehicle communication and vehicle to infrastructure communication, it was not studied in this dissertation.

Three field tests are titled as “WiFi communication between two adjunct nodes”, “WiMAX Regional Network,” and “Quality Requirements of Online Traffic Surveillance”. The following sections explain how the experimental tests were designed and conducted. Measures of effectiveness (MOEs) were carefully selected for each test to quantify the factors that affect the performance and reliability of wireless communications.

3.4.1 WiFi Communication between Two Adjunct Nodes

As mentioned earlier, the wireless communication connection between two adjacent nodes can only be maintained within a certain distance. The wireless signal strength degrades over the distance, which affects the transmission performance. 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. However, this communication range and corresponding performance can be affected by transmission power and modulation rates. Therefore, this study involved conducting a field experimental test to evaluate the effects of transmission power and modulation rates on the wireless communication performance between two sensors at different distance on a two lane two way (TLTW) state highway. Modulation is the technique that a carrier wave used to carry information from one place to another (Tse and Viswanath 2005). The wave is modified in amplitude, phase, or frequency, so that the information is present on the wave, and can be decoded at the receiving end. Field tests were conducted for the three following purposes:

- Identify major measure of effectives (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.

MOE Selection

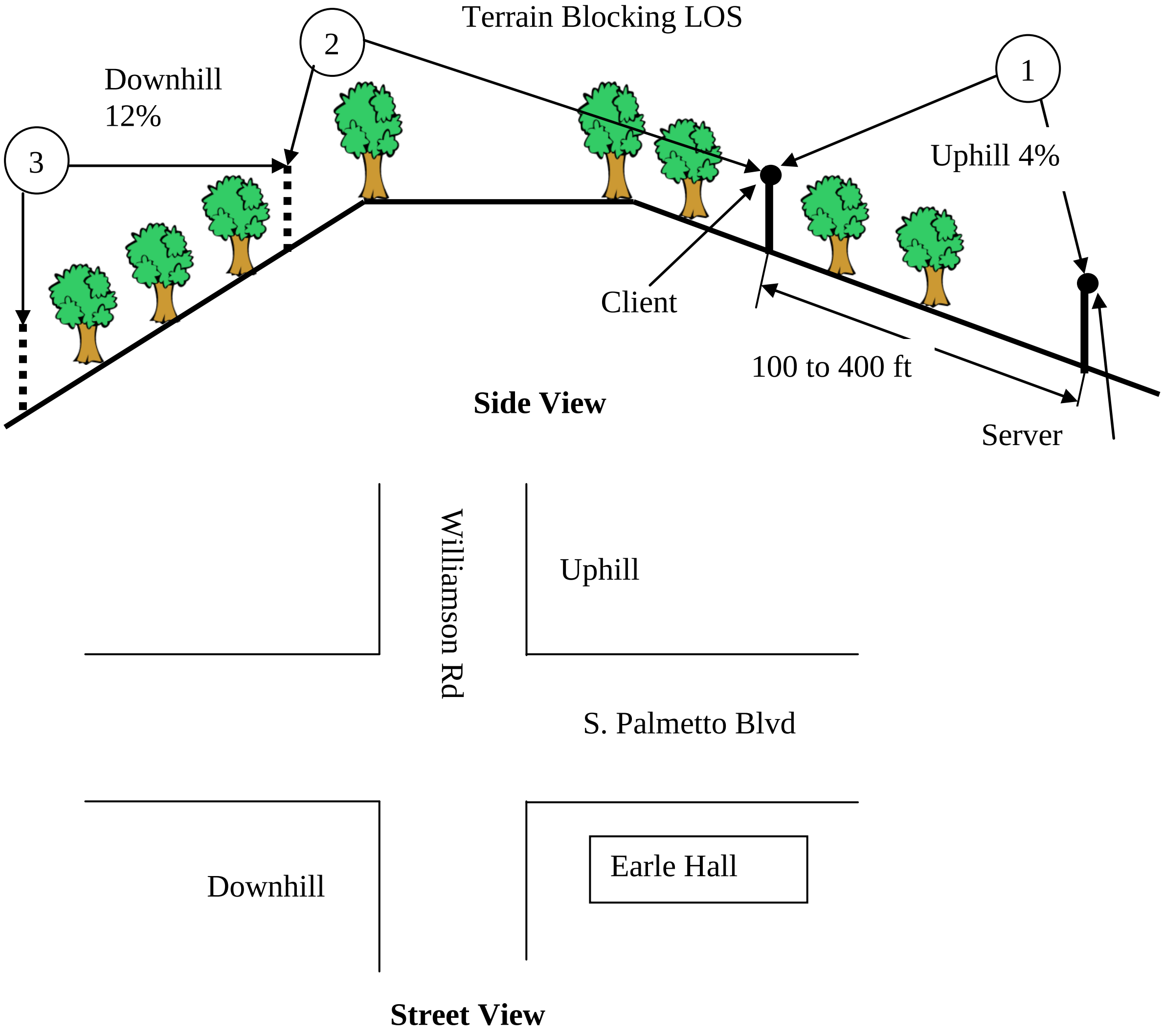
Effective traffic management applications rely on the real time traffic information collected by roadside devices to improve the traffic safety and mobility, such as incident response and clearance, traveler information assistance and commercial vehicle management (Gordon 2005, Chowdhury and Sadek 2004). Therefore, a reliable communication network is the foundation for effective and timely traffic monitoring and operations. According to the respective components' functionalities, MOEs for the communication system can include its bandwidth and data rate, where bandwidth of a network is given by bits of data that can be transmitted over the network in a certain period of time (Peterson and Davis 2003). However, the achievable network throughput can be affected by many factors, and is normally less than the system bandwidth. As reported in the literature, 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.

This study selected four relevant MOEs that can represent the effect of on-line traffic management functions under prevailing roadway and terrain conditions: 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, which this field study was able to systematically analyze and quantify the communication performance under different conditions.

Experimental Setup

The field tests were conducted from May 2008 to December 2009 in two locations: South Carolina State Highway 93 (SC 93) and Williamson Rd, near the Clemson University campus in the city of Clemson, South Carolina.

First, the field test was conducted on a segment of Williamson Rd, which is a two lane two way (TLTW) road, showed as location 1 in Figure 5. The presence of large amounts of foliage near the roadside didn’t prevent direct line of sight between the two nodes.



Side View

Street View

Figure 5 Field test locations on Williamson Rd

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. Openwrt is a communication community that develops open source software for the type of routers necessary to support ad hoc networking (Openwrt 2009). 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 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 received signal strength in average. Figure 6 demonstrates the experimental setup. Wireshark is a network protocol analyzer which can measure the signal strength, track each data packet, and record related information, such as protocol, arrival time, source and destination (Wireshark 2009). 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.

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. Iperf is a network testing tool used to measure the maximum throughput of this two-node ad hoc wireless communication network under different scenarios. Originally created in University of Illinois, 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.

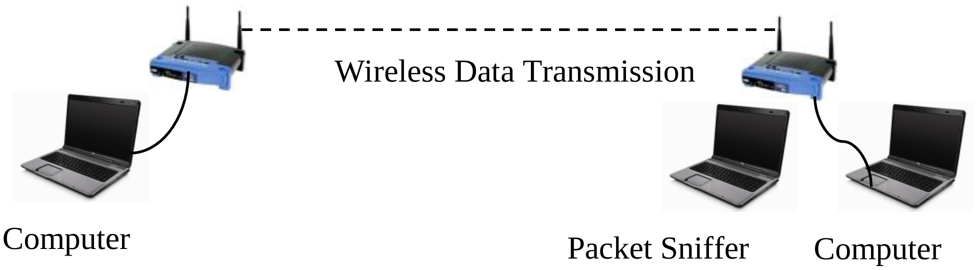


Figure 6 Field test experimental setup on Williamson Rd

Then, the similar test was conducted in another location on South Carolina state highway SC 93, as shown in Figure 7. 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.

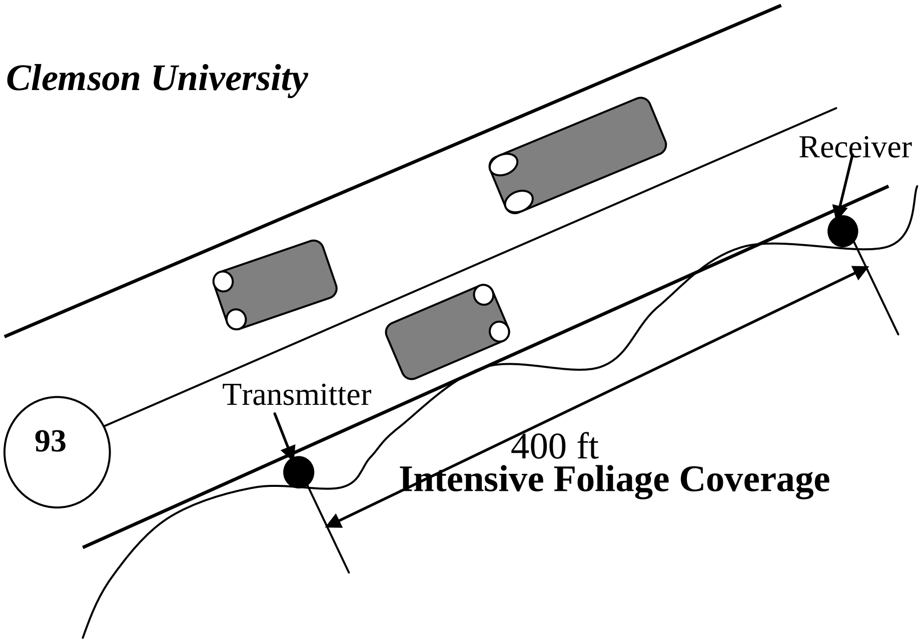


Figure 7 Test location and experimental setup on SC 93

Lastly, this study assessed the effect of the highway terrain characteristics on wireless communication between the two nodes. As shown in Figure 5, 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 4% upgrade and 12% downgrade, shown in Figure 5.

Measurements

First, five distances were selected, starting at 100 ft and increasing to 500 ft using 100ft intervals. At each distance, the author first measured the saturated throughput under seven modulation rates and four transmission power 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 study aimed to assess the communication performance, the throughput and reliable communication range, of both 802.11g and 802.11b WiFi technologies. 802.11g and 802.11b support different modulation rates, However, the author selected eight modulation rates, shown in Table 3. Modulation rate is the speed that data is being put in the carrier, which can be achieved through different modulation scheme. Table 3 summarized the main parameters used in the field test.

Table 3 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 transit power range up to 70 mW. The transmission power was set as 50 mW when testing the effects of highway terrain characteristics. Moreover, although 802.11g has a maximum throughput of 54

Mbit/s, a significant percentage of this bandwidth is used for communications overhead; the effective maximum throughput was about to be about 25 Mbit/s when measured in the lab environment at close distance. Many factors, such as metal, water, and particularly thick walls absorb signals and decrease the transmission range significantly (Peterson and Davis 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.

3.4.2 WiMAX Field Study

According to the literature review, the author 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 in this study 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. This field study was aimed to discuss 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.

As discussed in Chapter 2, WiMAX is based on IEEE 802.16 family of standards and designed to deliver high-speed wireless broadband access to fixed, nomadic and mobile users (Filis, 2007). In a fixed WiMAX environment (802.16d), a base station connects to fixed or slowly moving client devices. In a mobile WiMAX environment (802.16e), a base station connects to potentially fast moving clients and ensures seemless handoffs as a client moves into the range of a different base station. For example, the client is a vehicle that is moving at a high speed on the highway. Nomadic application falls between fixed and mobile environments, where clients may change locations and connect to different base stations through the relatively disruptive hard handoff process.

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 is a modulation scheme which conveys data by changing the amplitude of two carrier waves (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 SNR signals. The further the client subscriber is from the base station, the greater possibility that of a modulation rate, as shown in Figure 8 (H'mimy 2005).

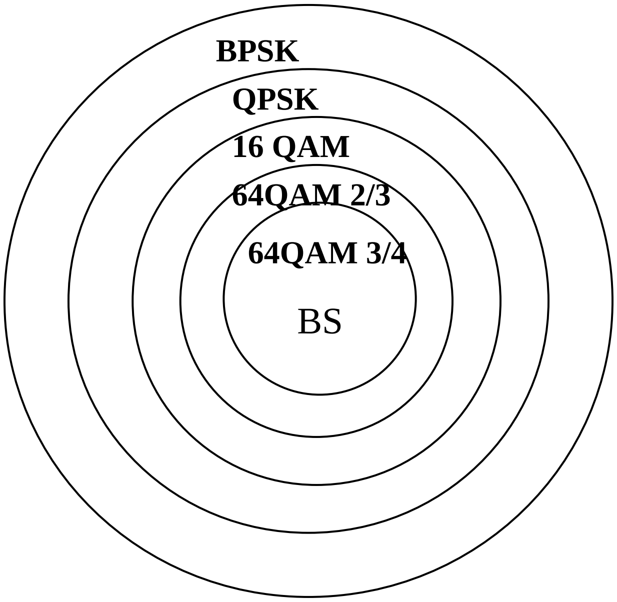


Figure 8 WiMAX modulations with respect to distance

The WiMAX Testbed

This field study was conducted in Fairmount, West Virginia. The WiMax network at Fairmount 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 9). 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 about 160 ft. Figure 9 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 4.

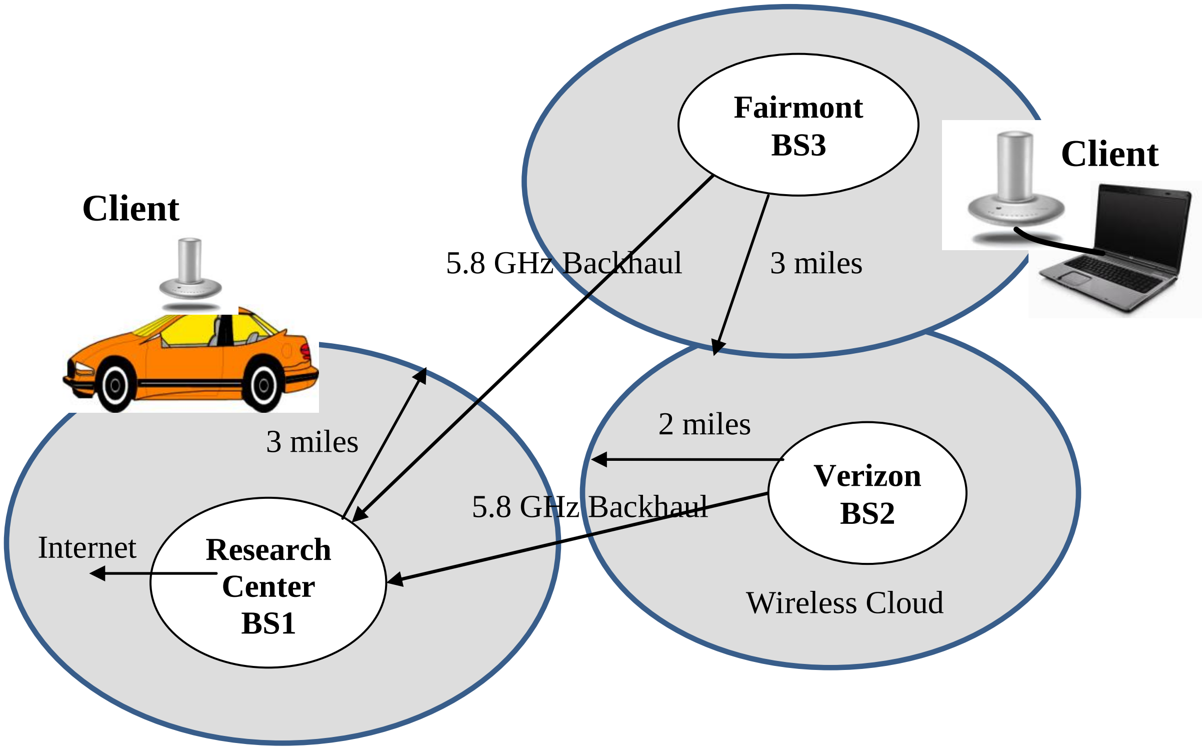


Figure 9 Network diagram and coverage of the WiMAX experiments

Table 4 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 Tx 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

Experimental Setup

The field tests were conducted from June through July, 2008. The project objectives were to measure and assess the performance of the WVHTC's WiMAX network. 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 9 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.

3.4.3 Quality Requirements of 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 interactive 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). Given each packet's end-to-end delay, jitter is the difference between every two consecutive packets. If high jitter spikes occur then for the human eyes, the video may jump 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. Possible reasons that might cause jitter in online traffic surveillance systems include the available bandwidth, number of users and required video image size. Next, the packet loss rate, which is the percentage of lost data packets when compared to the total data packets sent, can cause a video to appear distorted if the loss rate 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. The higher frame rate, the quicker that the video image updated or flashed in a unit of time. Normally, low jitter and high frame rates indicate a smooth video quality. However, 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).

The objectives of this study include mapping the jitter and packet loss rate with real-time video quality, recommending tolerated jitter values and acceptable buffer sizes for effective online traffic surveillance.

Equipments Setup

A case study with an on-line traffic surveillance system over a wireless network was conducted between May and July 2009 in Clemson, South Carolina. One traffic camera provided by the South Carolina Department of Transportation (SCDOT), was located on a side of the State Highway 39 (Perimeter Road), and was wirelessly connected to a router located in a nearby building which was about 1000 ft away as shown in Figure 10. The router was then connected to the campus computer Ethernet (wired system), which connected to the research laboratory computers as shown in Figure 11. The research lab was about three miles away from the camera location.

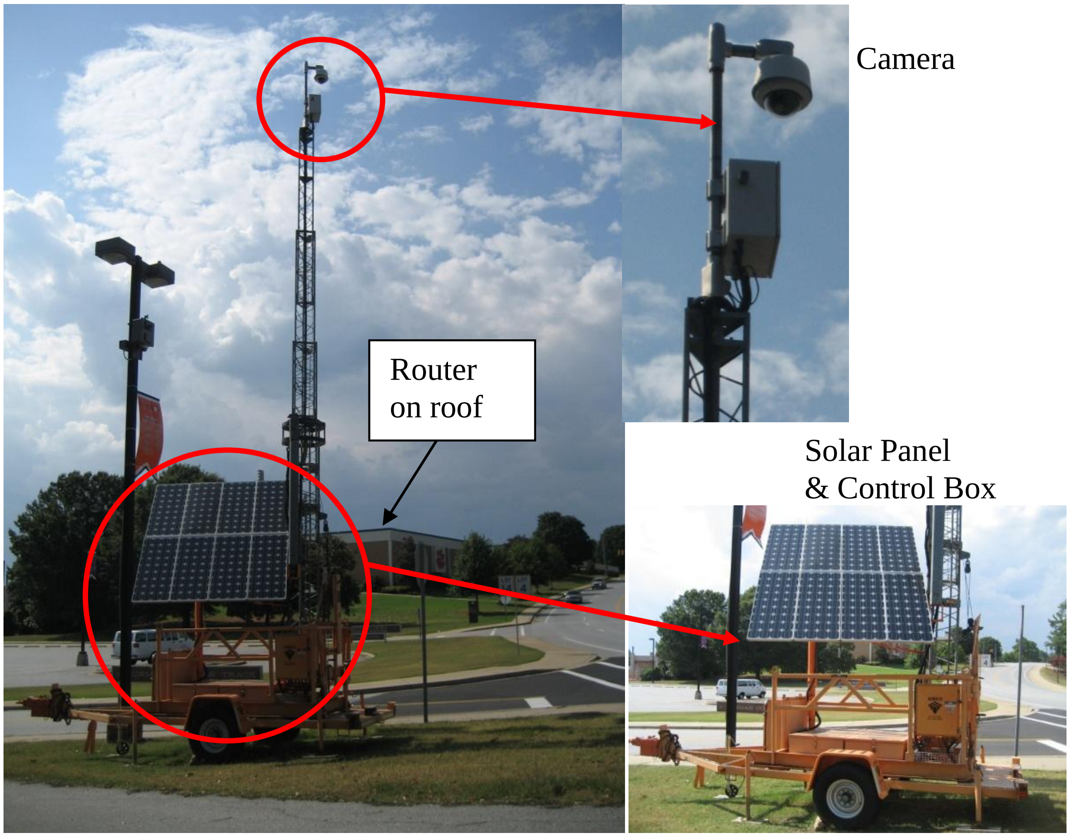


Figure 10 Solar power supported mobile traffic camera

The video data was sent to our lab computers first over the wireless network, and then the wired network. Figure 11 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 an IP surveillance software that can record incoming video streams to files and allows a single connection with a camera (MOXA 2009).

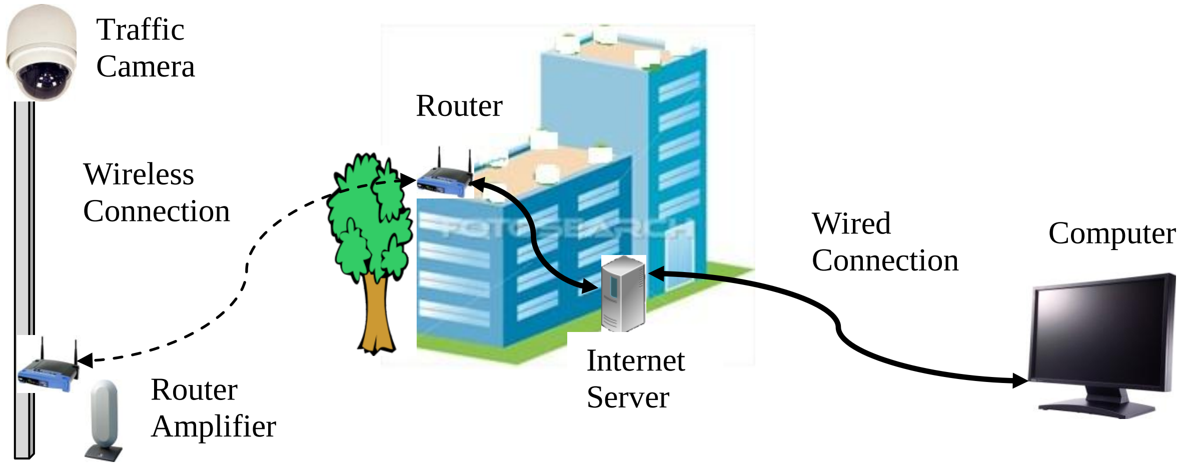


Figure 11 Video quality test experimental setup

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.

3.5 Simulation Analysis

The objective of the simulation study is to evaluate the performance of a large scale traffic sensor network deployed in two different network topology options as proposed in case study. Then the performance will be used for performance-cost analysis presented in next section. Using WiFi as an example, two types of simulation study were conducted. The first one is to evaluate the communication reliability and performance of traffic sensor network using communication simulator ns-2. The other simulation study is to assess 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 discussed the simulation site selection and evaluation scenarios in detail.

3.5.1 Ns-2 Simulation

To support online traffic management, wireless sensor networks have the potential 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. This part was aimed at obtaining a comprehensive quantitative assessment of a wireless traffic sensor network's dependency on communication errors and topology decisions through an ns-2 simulation analysis. 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 12 shows the methodology for analyzing the communication network performance with selected 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.

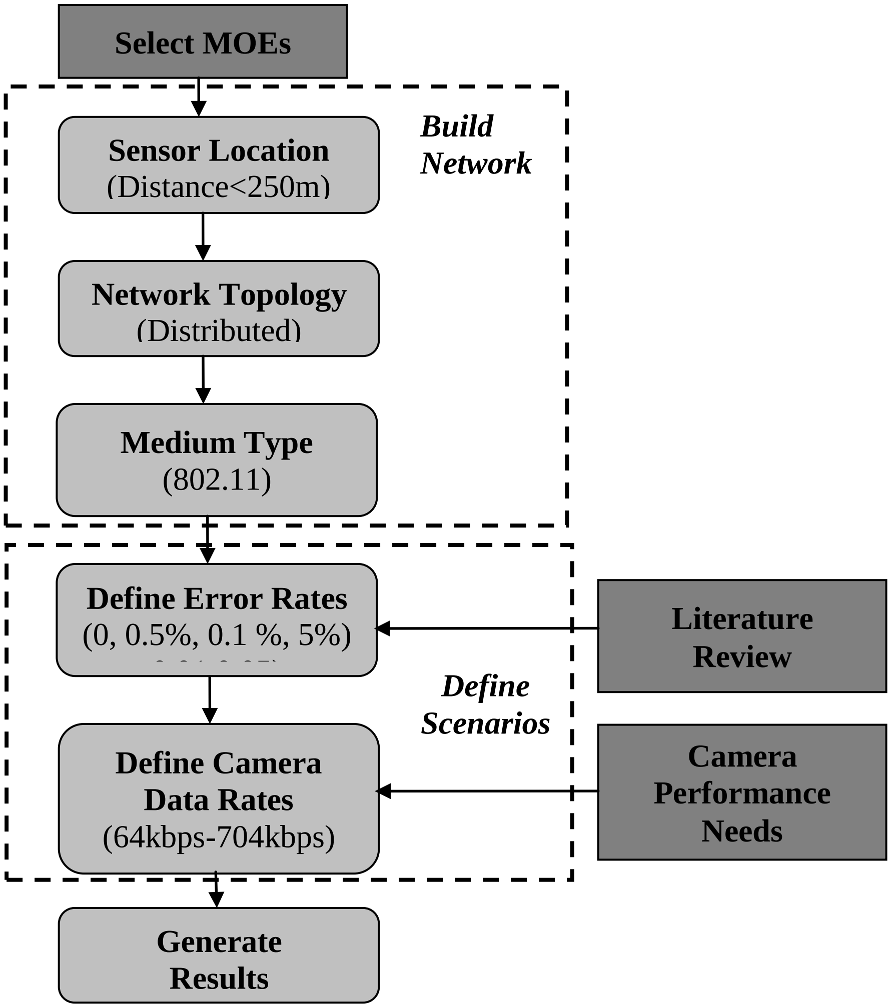


Figure 12 Ns-2 simulation methodology

A video surveillance camera requires higher bandwidth than other traffic devices such as highway advisory radio (HAR) and dynamic massage 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 over wired Internet connectivity. Figure 13 illustrates the distributed wireless sensor network topology and terminology.

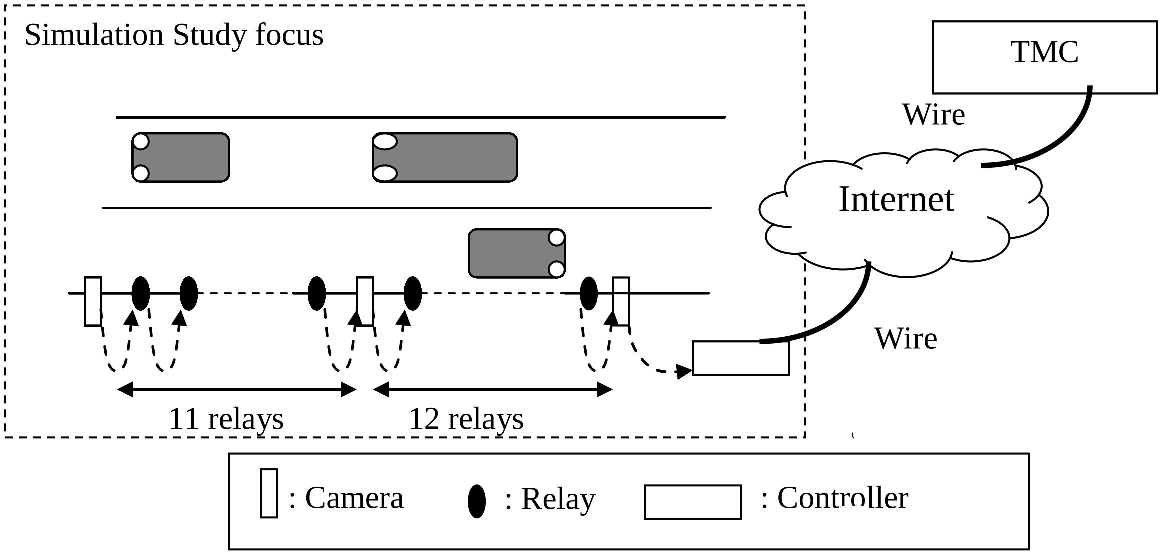


Figure 13 Ns-2 simulation network for on-line traffic management

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, in which bandwidth of a network is given by bits that can be transmitted over the network in a unit time (Peterson and Davis, 2003).

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 this study, the transmission errors under adverse conditions are modeled.

Similar to the field test, this study selected two MOEs related to communication reliability for on-line traffic management requirements, the *saturated throughput* and the *successful delivery ratio*. *Saturated throughput* is limit throughput reached by the system as the offered data load increases (Pourahmadit et al. 2005). *Delivery ratio* is the percentage of packets sent by the sensors that can be successfully received by their designated receiver (Zhao and Govindan, 2003). 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.

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. This study simulated a 3- mile highway section with roadside traffic cameras wireless connected and communicated one by one. In this study, 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 13, there were a total of 25 relays, 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, this study chooses 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. This study 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). Detailed results are explained in Chapter 6. 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).

3.5.2 Integrated Simulation

The second type of simulation study utilized an integrated simulation platform which integrates the microscopic 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 in previous chapter, 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 is 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 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 another word, 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" in this study. In 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 study, 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 14.

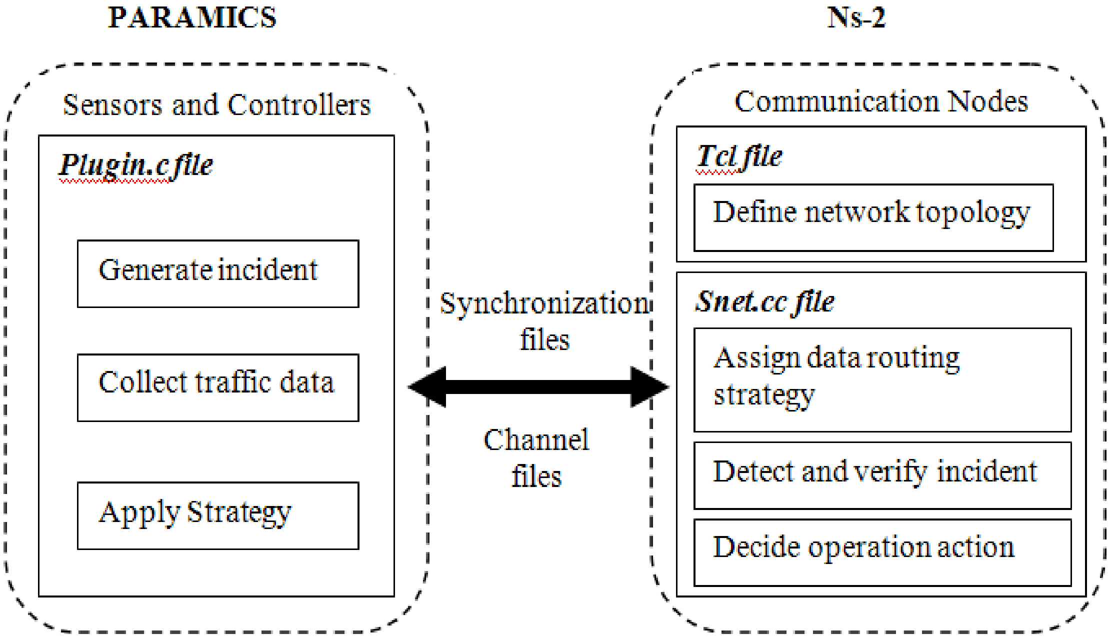


Figure 14 Integrated simulator architecture

Traffic detectors are normally placed in distance intervals longer than the typical communication range of wireless sensors, which depends on the technology. This study simulated 802.11g which requires less than 250 meters (700 ft) distance between sensors. Hence, wireless relays are needed to enable ad hoc network communication with all detectors without demanding excessively more detectors to be placed. 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.

Simulation Network

This study 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. It serves the traffic to and from the Greenville metropolitan area with a population of 601,986 according to the 2006 census estimate.

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 author 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 study 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).

Simulation Scenario

This study 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 in charges of five sensors. Traffic sensors collect the traffic information, and send to presiding controller in every pre-defined time interval. Each controller gathers the information from sensors and implemented 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 incident 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 15 demonstrates the network and traffic sensor deployment.

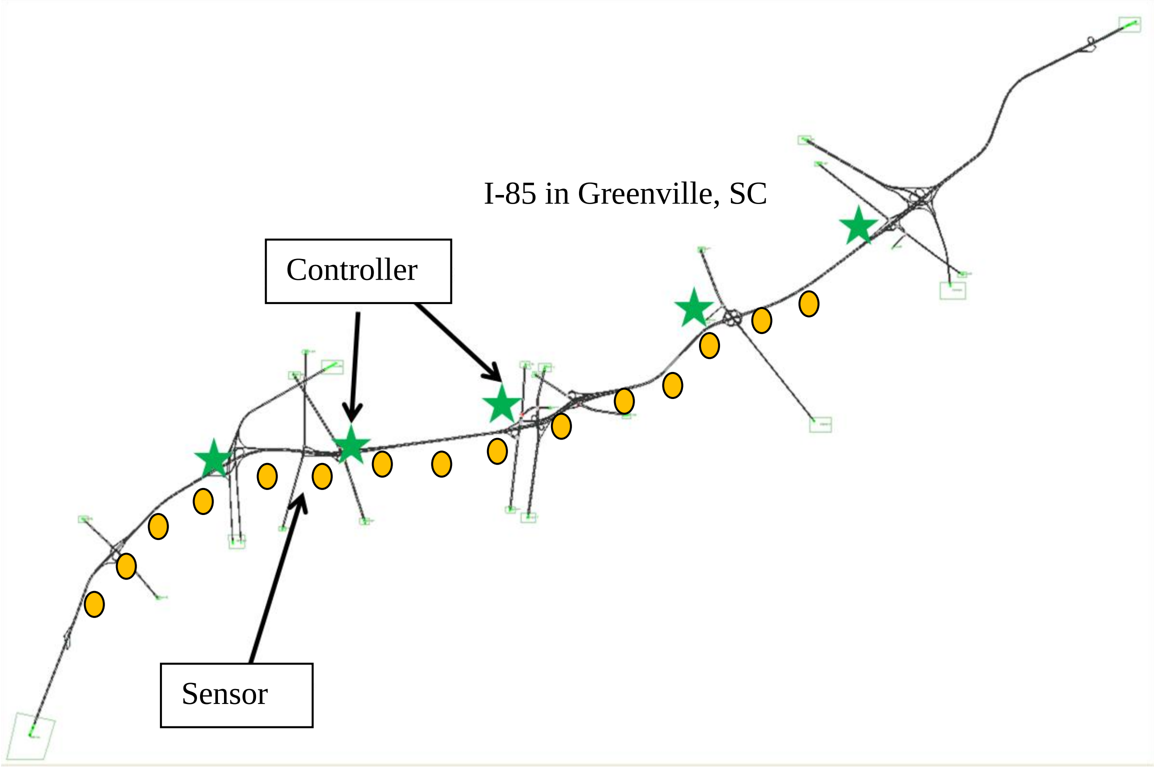


Figure 15 Simulation Network Deployment

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 study, each traffic sensor only detects one side and one direction of the highway traffic. Controller only gathers the information and implements detection algorithm but not collects 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.

Incident Detection Algorithm

This study implemented one of the first incident detection algorithms, California algorithm to detect incident. As one type of comparative algorithms, California algorithm serves as the basis of comparison to many other algorithms. The algorithm is utilized to detect an incident based on the measured occupancy from two adjacent detectors (Martin et al. 2001). A potential incident is declared when values from the three different tests surpass preset thresholds. The three tests are defined as follows:

1. The difference between the upstream station occupancy (OCCi) and the downstream station occupancy (OCCi+1) is checked against threshold value T1. If the threshold value is exceeded, then proceed to step two.

2. The ratio of the difference in the upstream and downstream occupancies to the upstream station occupancy (OCCi. OCCi+1)/OCCi is checked against threshold T2. If this threshold is exceeded, proceed to step three.

3. The ratio of the difference in the upstream and downstream occupancies to the downstream station occupancy (OCCi . OCCi+1)/OCCi+1 is checked against threshold T3. If this threshold is exceeded, a potential incident is indicated and step two is repeated. If this threshold is again exceeded, a potential incident is flagged. An incident state is terminated when threshold T2 is no longer exceeded. The thresholds are calibrated from empirical data.

As an example showed in Figure 16, sensor 1 to sensor 5 sends occupancy information to the controller at a preset interval. For the same sensor, the controller compared the current occupancy with the previous data. For adjacent sensors, the controller compared the difference between them. Once incident occurs between sensor 2 and sensor 3, sensor 3 senses drop in downstream occupancy immediately, while sensor 2 will detect significantly increased upstream occupancy after a while. The occupancy difference between sensor 2 and sensor 3 will be used by controller to alarm, detect and verify an incident. Using five sensors and their presiding controller as an example, detailed detection procedure based on the California algorithm is presented in the following.

Step 1: Sensor #1 to #5 send occupancy and flow information to controller #1 every 30 seconds

Step 2: Controller #1 compares the occupancy difference with previous data log of each sensor in every 30 seconds. eg. Occ3(i+1) - Occ3(i)

Step 3: Controller #1 compares the occupancy difference between adjacent sensors 1 & 2, 2 & 3, 3 & 4, and 4 & 5. eg. Occ3(i) -Occ2(i)

Notes: Steps 1 to 3 are implemented simultaneously at controller 1.

An event where a traffic incident occurred between sensor 2 and sensor 3,

Step 4: When Occ3(i+1) - Occ3(i) = 0, proceed to step 5

Step 5: Compare the occupancy difference between upstream and downstream sensors

If the [Occ3-Occ2] < T1, go back to steps 1-3

If the [Occ3-Occ2] > T1, **Flag a incident**, T1 = 0.1

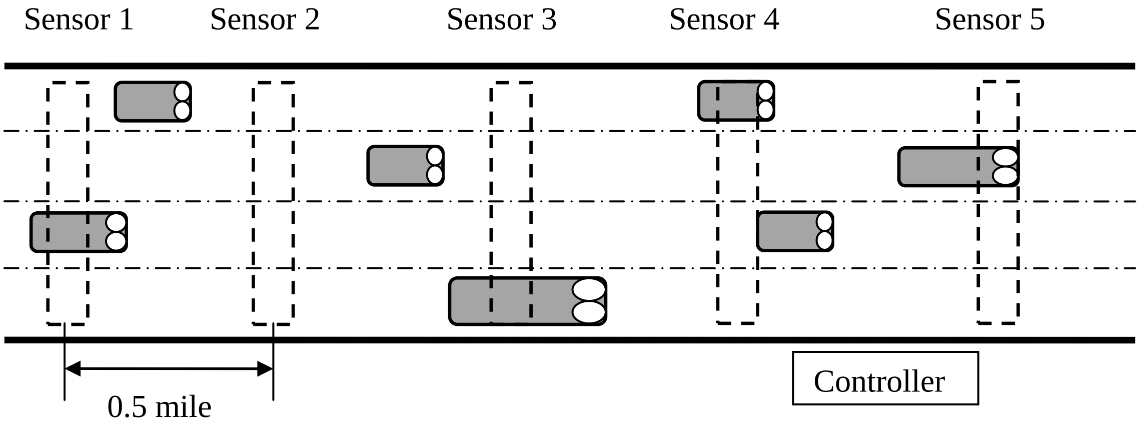


Figure 16 An example of sensors and controller deployment

In PARAMICs network, the occupancy data collected by each sensor does not update if there is no vehicle passing the sensor. Therefore, the downstream occupancy stays at constant after incident happen. In step 4, if the occupancy of two consecutive time step remains the same or very close, a potential incident is alarmed. Threshold value T1 was defined based on simulation results by taking the average of occupancy difference at the same sensor or between adjacent sensors of several different runs. Average value of several different runs is taken until the variance fall within five percent.

MOEs Selection

For the study scenario with incidents, the vehicular traffic simulator randomly generated incidents on segments under surveillance of traffic cameras during the PM peak hours. 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 in this study 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 5 summarized the study scenarios and MOEs.

Table 5 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)

3.6 Performance-cost Analysis

Based on the simulation results, the author 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 study was to analyze the cost effectiveness of using 802.11g wireless technology to support traffic surveillance systems in Greenville, SC, as proposed in the case study section. Besides of literature review, cost information was also reference to typical used default value 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 estimation.

Use the Greenville network as an example, 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 difference of these two network topologies were explained in the Case Study section. 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 Figure17.

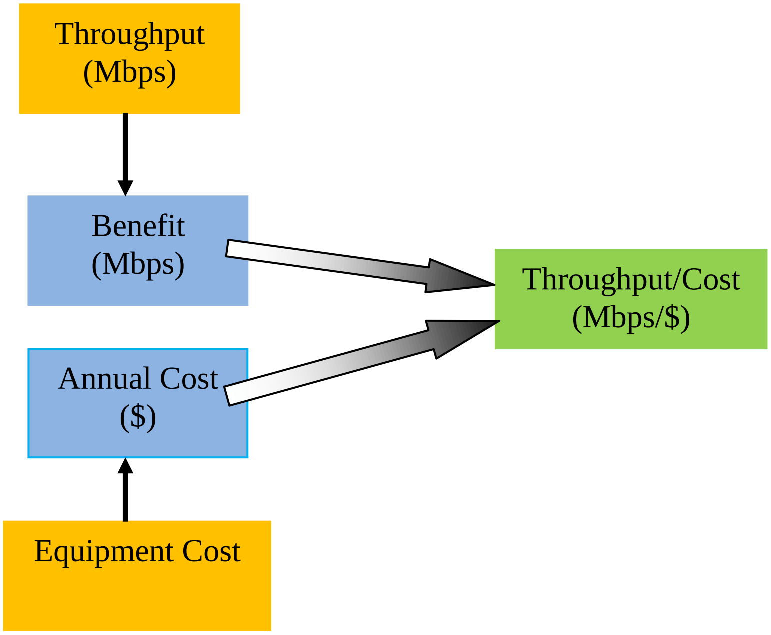


Figure 17 Throughput/Cost analysis procedure

Maintenance cost, operation cost and transmission power cost can be easily converted to yearly value. The equipment costs, actually 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 equipments in years; 1, 2, etc.

The traffic surveillance system in Greenville is mainly consisted 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 where are needed, depending on the network topology. Moreover, the transmission power cost was also considered using the commercial electric price in South Carolina. This study assumed that traffic camera works 8 hours a day, and 365 days a year.

CHAPTER FOUR

4 INTERVIEW/SURVEY

This section presents a synthesis of interview responses received as of October 1, 2009. As summarized in Table 6, 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 WiFi to connect 96 traffic signals within 25 square miles. In other states, WiFi 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. To be clear, 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 6 Summary of interview responses

Categories	Responses
Types of communication infrastructure	Wired: T1, Fiber (9) Wireless: unlicensed wireless (9), Cellular (9), WiFi (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), WiFi (4), Wireless 5.1-5.8 GHz (2)
Future plans to use any new, currently non-existing, wireless alternative	Yes (9) such as WiFi
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: ( ) 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 plan. 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 WiFi 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 Chapter 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 7, 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. This table does not reflect a complete list of possible ITS applications, rather it is a sample of the more common uses.

Table 7 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 Syetem	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

State	Project	Technology	Description
Illinois		2.4, 4.9, 5.1-5.9 GHz radios	Used for temporary and/or permanent links to fiber backbone.
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, WiFi, 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, WiFi, 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

State	Project	Technology	Description
New York	State-wide network	Land Mobile Radio	Integrated wireless public safety/service radio network for interagency and intergovernmental communications
	Commercial Vehicle Infrastructure Integration Program	DSRC, IEEE 802.11p	Development, testing, and demonstration of commercial vehicle-based data communication 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

State	Project	Technology	Description
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

CHAPTER FIVE

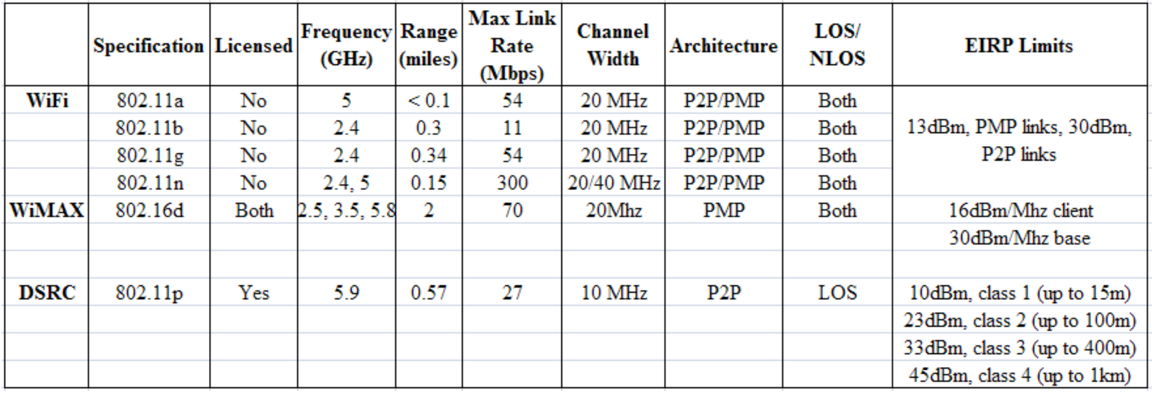
5 CASE STUDY

Traffic surveillance devices can be deployed in different network topologies which lead to different system performance and cost. The case study presented in this chapter used two selected technologies, WiMAX and WiFi, to support existing traffic surveillance system (includes CCTV, radar and Dynamic message signs (DMS)) under mesh and non-mesh topology for seven major metropolitan areas in South Carolina. The case study was conducted based on proposed design flowchart described in Chapter 3. The seven cities are Columbia, Greenville, Spartanburg, Gaffney, Rock Hill, Florence and Myrtle Beach. This chapter uses Columbia and Greenville as examples to demonstrate the network design process. Case studies for other five cities can be found in Appendix C. The network designed for Greenville was then used in performance-cost analysis.

5.1 Network Design

Designing an ITS network requires careful planning of both the type of wireless technology to be deployed and the location of the access points. Planning an ITS network begins with determining the requirements that the various sensors, cameras, and other ITS components will necessitate. In addition, considerable thought should be put into choosing the wireless network architecture to be deployed. As stated earlier, the two wireless technologies considered are WiFi 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 8 was synthesized in [Zhou et al 2009] with columns containing pertinent information for a network engineer designing an ITS environment. To aid in comprehension of this information, an explanation regarding how each column affects ITS network design is shown below.

Table 8 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 7 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 18.

Figure 18 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 19.

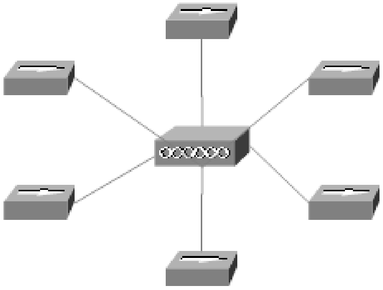


Figure 19 A typical PMP architecture link

- *Mesh* – A mesh network allows any node in the network to transmit to any other node. Both WiFi 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 20.

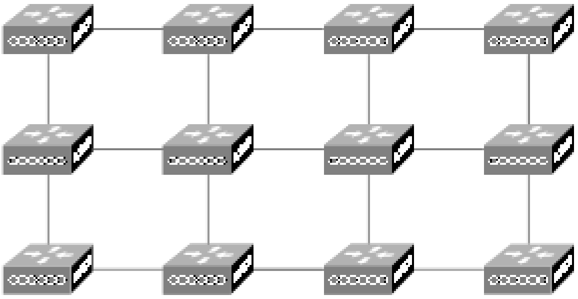


Figure 20 A typical mesh architecture link

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.

EIRP **–** 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 WiFi 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 21 is generated using measured range and throughput data (Cisco 2009).

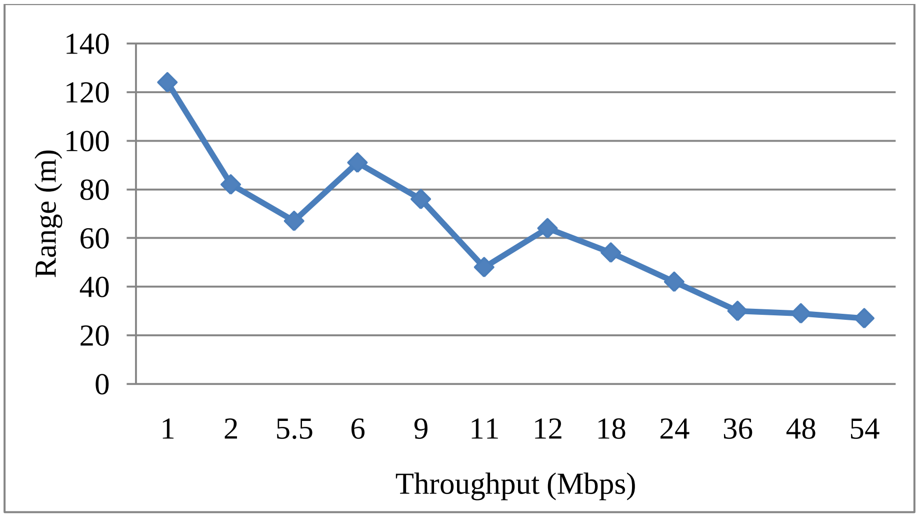


Figure 21 Range vs. Throughput for IEEE 802.11g (Cisco 2009)

***Mesh vs. Infrastructure* –** Two network deployment architectures (topology) are considered in the following case study for each wireless technology (WiFi and WiMax), the mesh network architecture and the infrastructure, or PMP, model. Both WiMAX and WiFi 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 9 for exact requirements. These are experimentally calculated figures, and should provide a rough tool that can be used for future design purposes.

Table 9 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 WiFi 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, also with an omni-directional antenna.

5.2 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 wireless connected. All these devices are located on I-20, I-26 and I-77, showed in the Figure 22.

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.

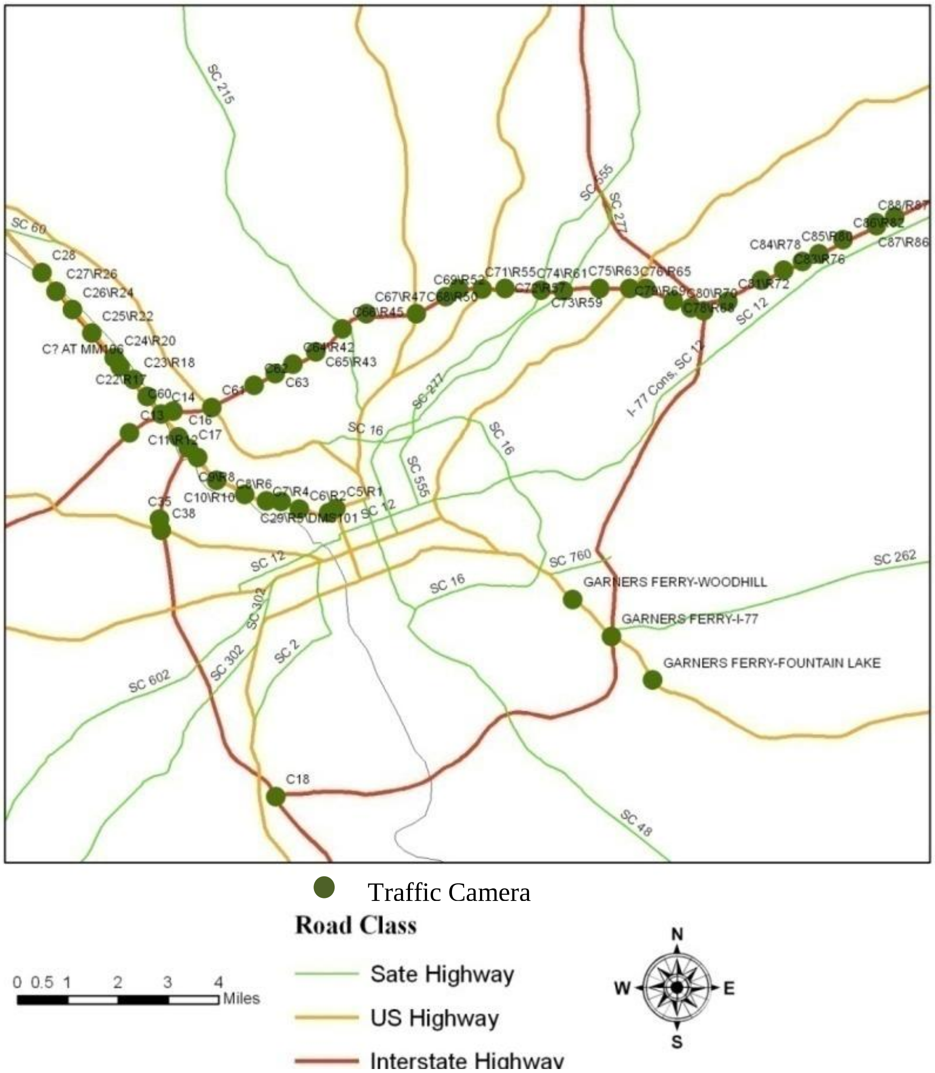


Figure 22 Traffic Surveillance Devices in Columbia, South Carolina

There are a total of four network deployments considered in this case study. There is both a WiFi 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 the pictures below the stars signify that they are connected to a fiber optic Internet connection.

5.2.1 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. Then, the study divided all these devices into 13 sub-networks, each containing at a maximum five nodes within 2 miles, shown in Figure 23.

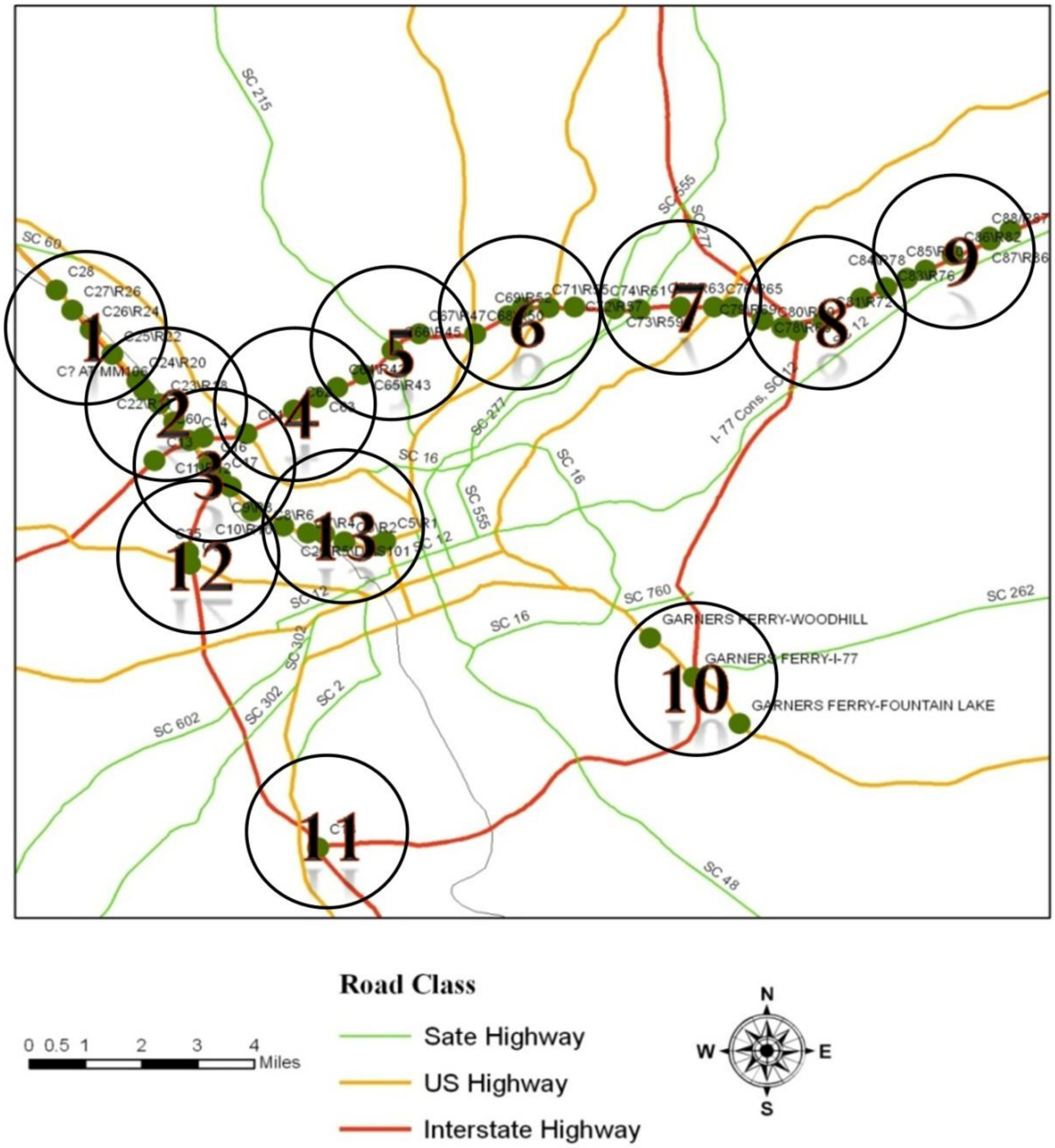


Figure 23 WiMAX infrastructure model of Columbia site

As seen in the Figure 24, 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 10 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, showed as a blue star in Figure 21. 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 author use the term “Satellite node” is a term used to 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 10 Traffic monitoring devices of Columbia network: group one

Group 1	**C27\R26**	**C25\R22**	**C24\R20**	**C28**	**C26\R24**	**C AT 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. Primary	*1.0925*	*1.5655*	*2.2296*	*1.5655*	*0.9609*	*2.4380*
Avg. Dist. Primary	*0.5135*	*0.8157*	*1.4800*	*0.7499*	*0.5134*	*1.6882*

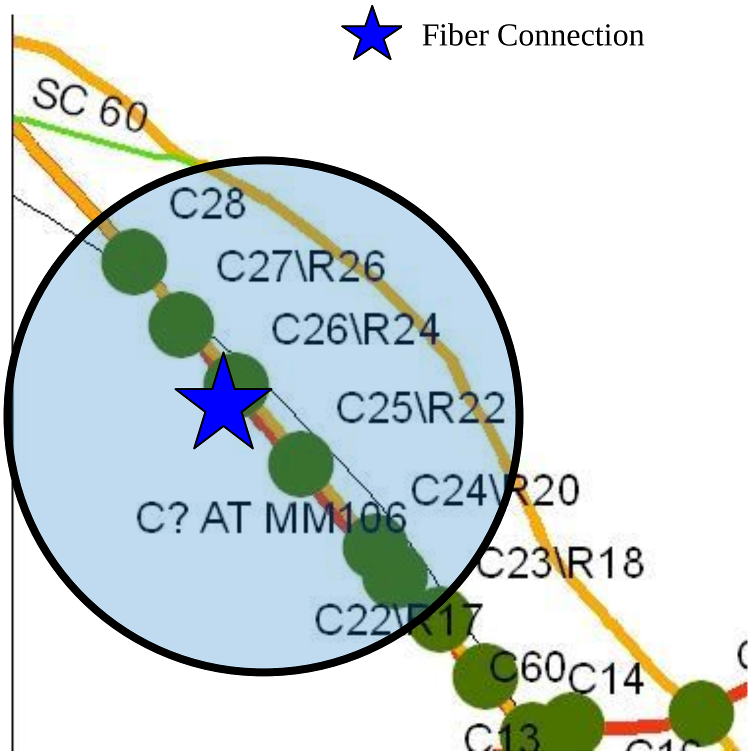


Figure 24 Fiber Optic Connection of Group One of Columbia Network

5.2.2 WiFi Infrastructure Network

The WiFi infrastructure model is shown in Figure 25 below, and 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.

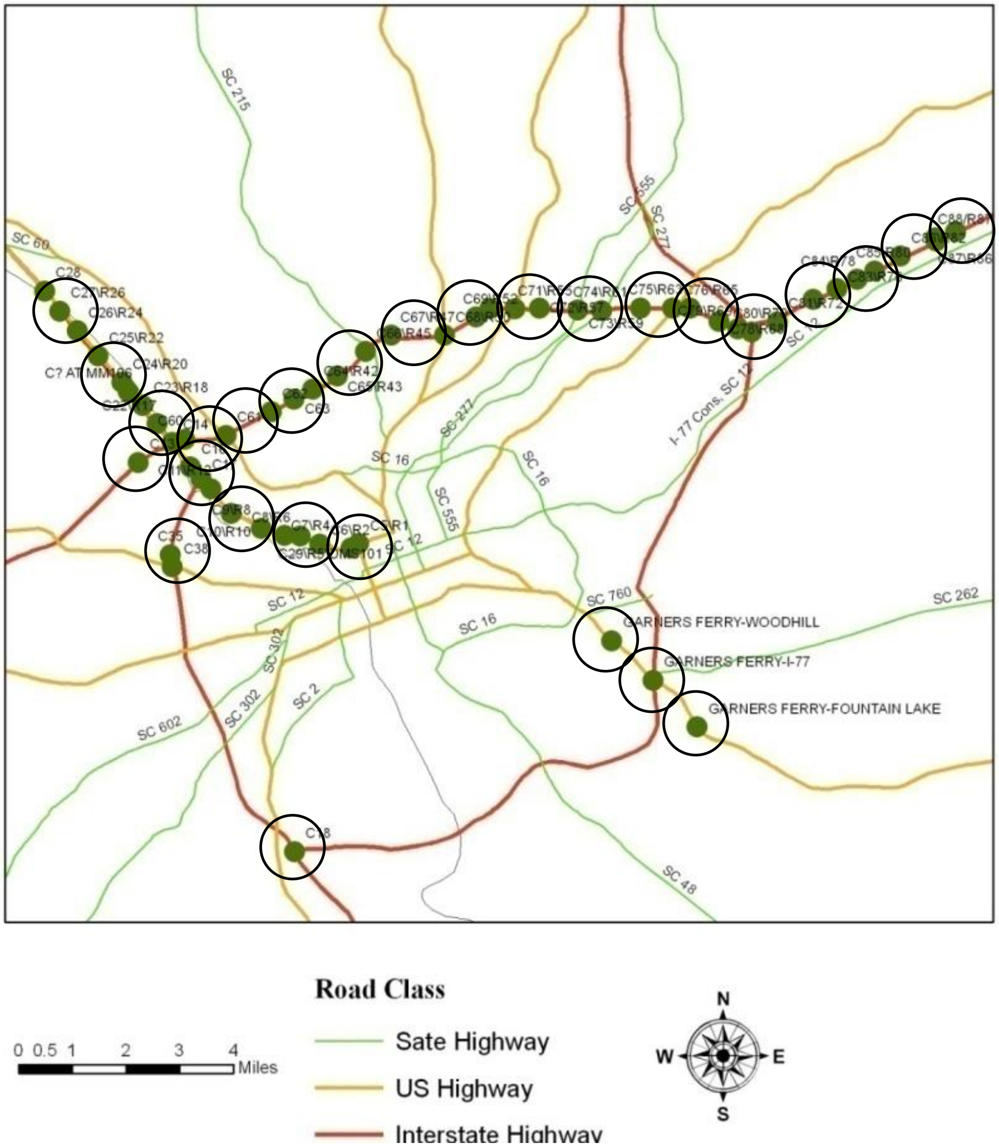


Figure 25 WiFi Infrastructure Model of Columbia Site

5.2.3 WiFi Mesh Network

The WiFi mesh model is shown in Figure 26, and divides the twenty-eight clusters into four mesh clusters, one supporting a group of fifteen clusters, another connecting group of nine, a third for a group of four and a final cluster to support one satellite node. The reason is the distance between the satellite node and other mesh clusters are farther than 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. The reason is the distance between the two mesh clusters is farther than the standard Cisco access point can reach at a minimum of 11Mbps. 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.

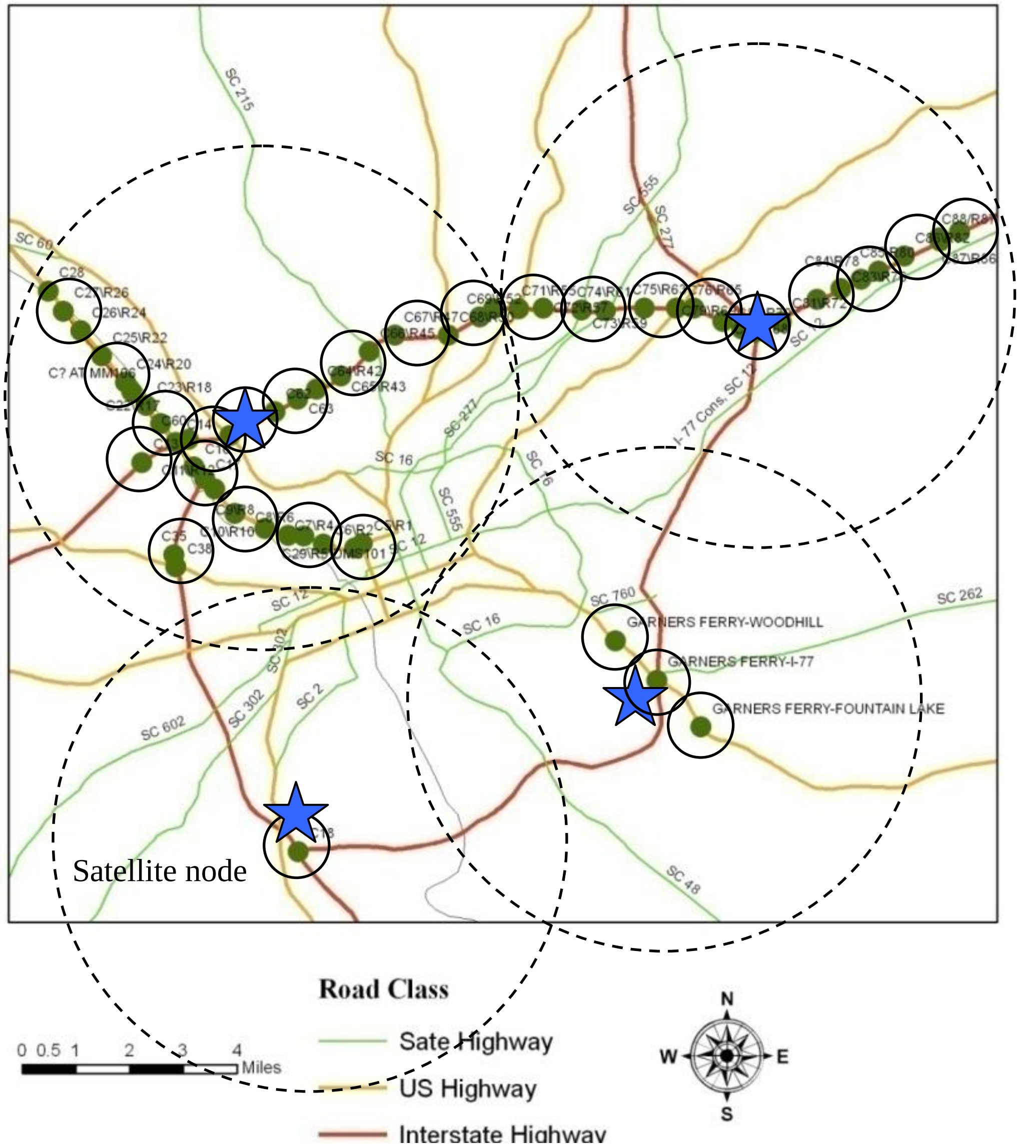


Figure 26 WiFi Mesh Network Model for Columbia, SC

In this scenario, there would be a total of three fiber optic Internet connections required, and fourteen 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.

5.2.4 WiMAX Mesh Network

The WiMAX mesh model is shown in Figure 27 below, and divides the twenty-eight clusters in the same manner as the WiFi mesh model; with into three 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 28 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 WiFi mesh network.

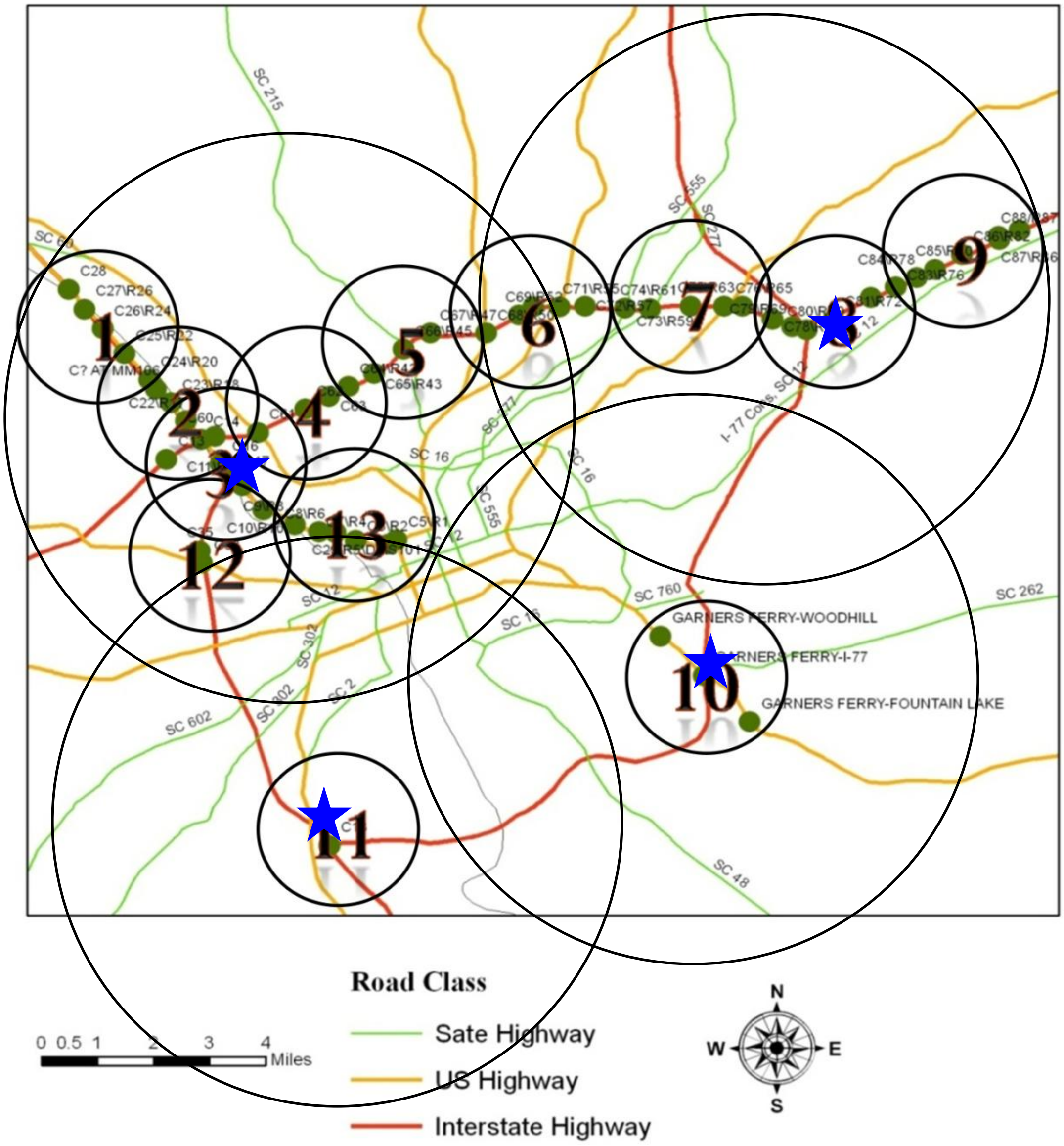


Figure 27 WiMAX Mesh Network Model for Columbia, SC

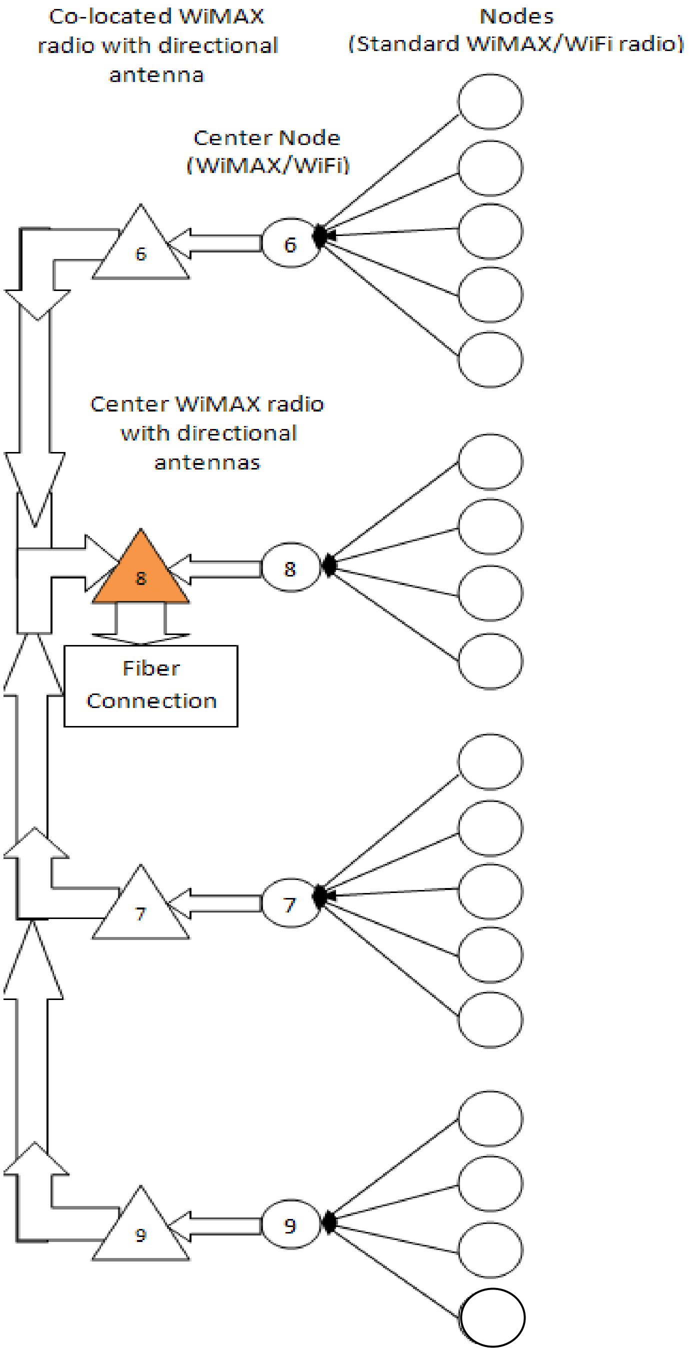

Co-located WiMAX radio with directional antenna
Nodes (Standard WiMAX/WiFi radio)
Center Node (WiMAX/WiFi)
6
6
Center WiMAX radio with directional antennas
8
8
Fiber Connection
7
7
9
9

Figure 28 Data transmission within one mesh cluster

5.3 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 provide 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 below in Figure 29.

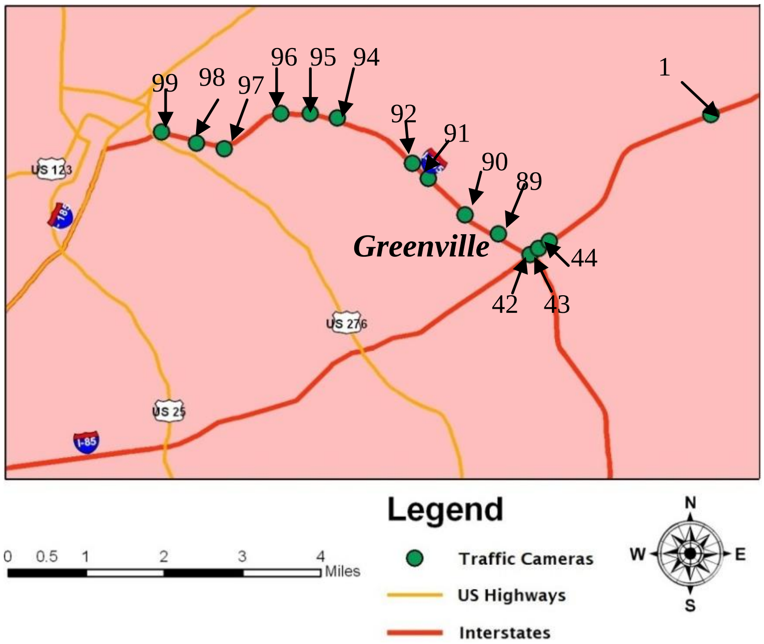


Figure 29 Traffic Surveillance Systems in Greenville, SC

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 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.

5.3.1 WiFi 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 WiFi mesh model, shown in Figure 30, divides the fourteen traffic surveillance cameras into two mesh clusters, a group of six and a group of eight. 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 11, 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 maximum 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 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 the network is already utilized.

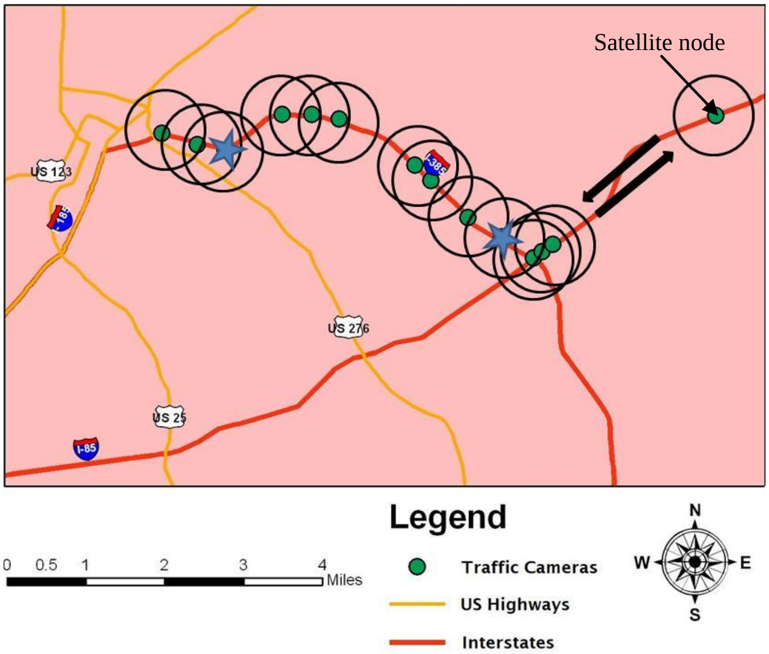


Figure 30 WiFi Mesh Network Model for Greenville, SC

5.3.2 WiMAX Mesh Network

The WiMAX mesh model, shown in Figure 31 below, divides the fourteen traffic surveillance cameras into two a groups of six and a group of eight mesh clusters, respectively. This configuration is identical to the WiFi mesh model. Each node possesses its own Motorola WiMAX base station, with each node in the two clusters forwarding data from the other nodes. Again, the access point locations with Internet access were chosen to minimize this maximum hop-count. Within this network there are three nodes require 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. However, this relatively expensive solution to wirelessly enable the traffic surveillance cameras has the same expandability drawbacks as the WiFi mesh network.

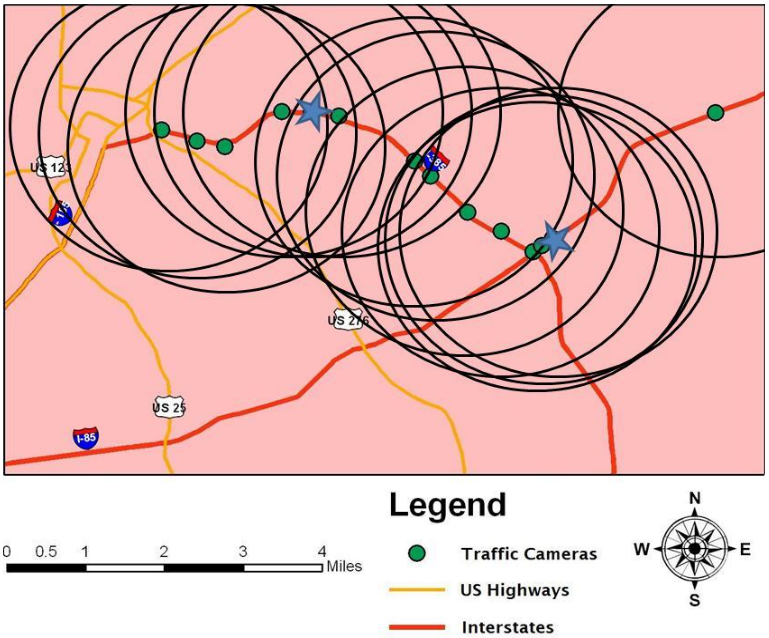


Figure 31 WiMAX mesh network model for Greenville, SC

5.3.3 WiFi Infrastructure Models

The WiFi infrastructure model, shown in Figure 32, 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.

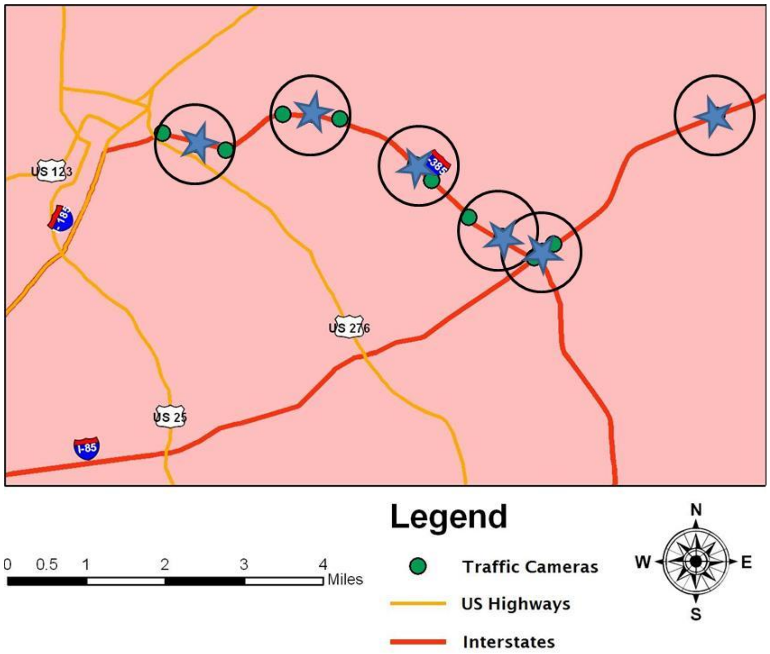


Figure 32 WiFi infrastructure network model for Greenville, SC

5.3.4 WiMAX Infrastructure Models

The WiMAX infrastructure model, shown in Figure 33 below, 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.

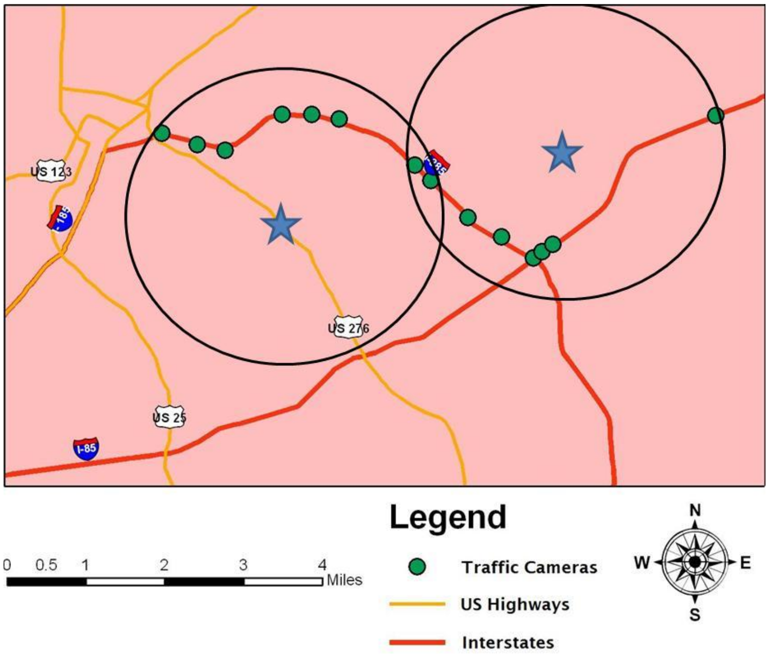


Figure 33 WiMAX Infrastructure Network Model for Greenville, SC

CHAPTER SIX

6 FIELD STUDY

In order to assess the performance of two selected wireless technologies, WiFi and WiMAX, in a real highway environment to support communication between field devices, and between field devices and TMC, three types of field test were conducted; WiFi communication between two adjacent nodes, the performance of a regional WiMAX network, and quality requirements of internet-based real-time traffic video surveillance. Factors that affect the communication performance and reliability, such as transmission power and modulation rates, were considered in the field study. The following sections are summarized in four sub-sections based on different types of tests. The field test results were utilized to develop recommendations for practical applications

6.1 WiFi Communication between Two Adjunct Nodes

Figures 34 through Figure 41 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.

To determine if the average throughput taken during 120 sec represents the average communication performance, this study 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 34, 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.

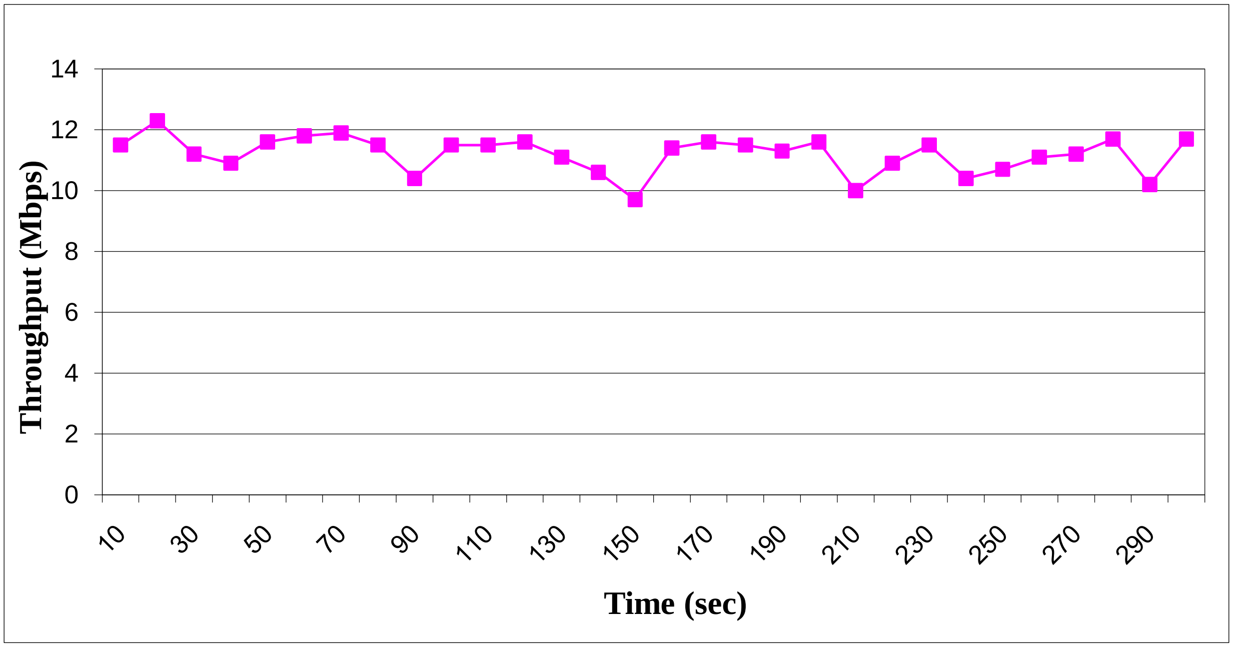


Figure 34 Throughput Variations with Time (TCP)

Figures 35 a) to 35 f) present the saturated throughput at different distances between transmitters and receivers under four different transmission powers corresponding to the frequency modulation rates of 2 Mbps, 5.5 Mbps, 6 Mbps, 11Mbps, 24 Mbps and 48 Mbps, respectively. As seen from Figure 35, 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 35a)), 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. 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. Obviously, there is a trade-off between performance and cost. Although deploying two access points or traffic sensors close to each other can improve the performance and ensure the reliability, this type of deployment also increases the implementation and operation costs.

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 is the propagation phenomenon that results in radio signals reaching the receiving antenna by two or more paths, thereby resulting destructive cancellation. 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 36. 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. The other reason 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 in practice. There was not much increase in power between 30 mW to 70 mW.

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 33, higher modulation rates provides 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.

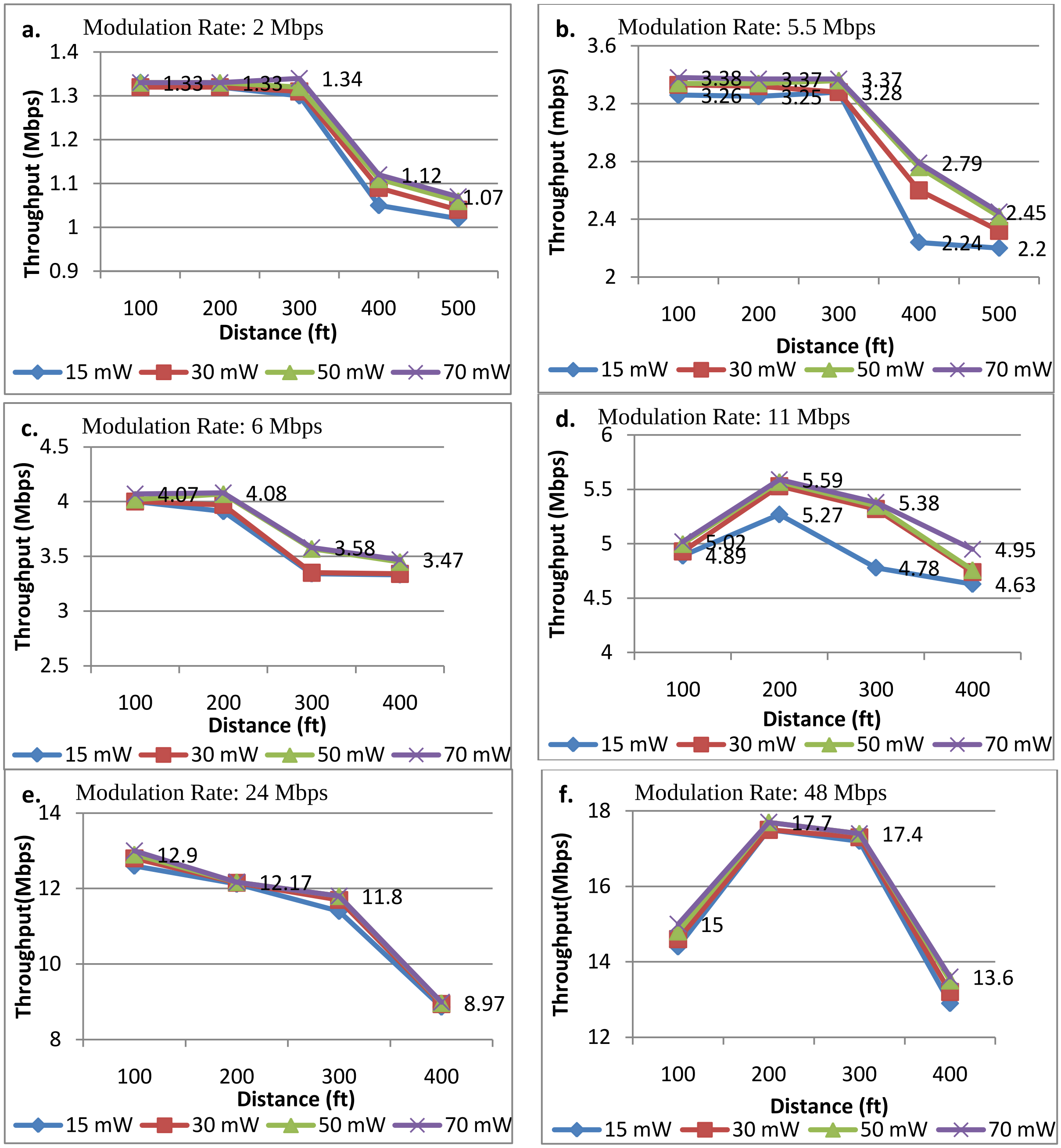


Figure 35 Saturated throughputs (TCP)

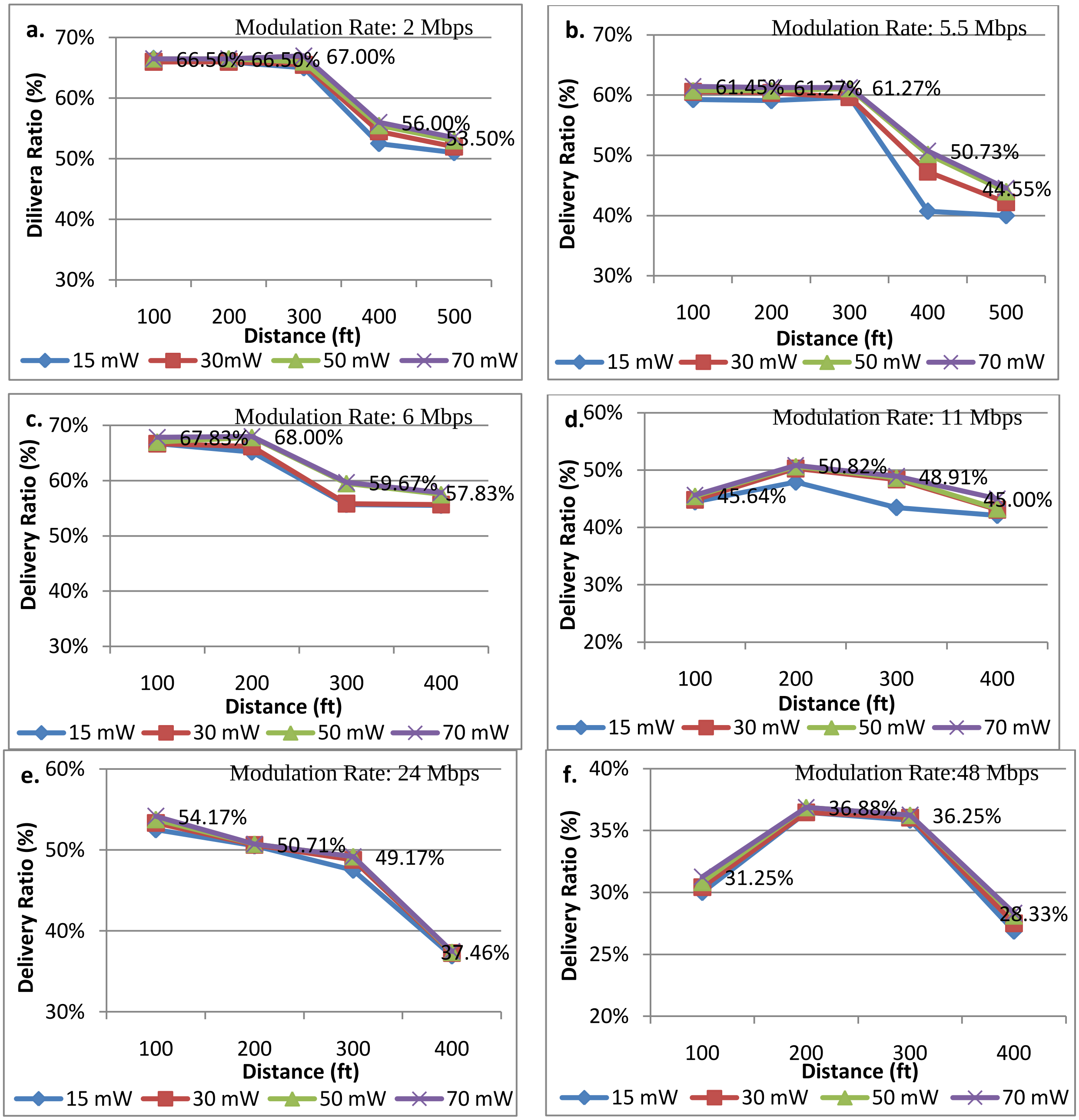


Figure 36 Delivery Ratios (TCP)

Another experiment was conducted to set up the modulation rate as auto, which means that at each second, the modulation varies according to the received signal strength. Because the field test focus on studying the 802.11 b and g technologies, modulation rate options vary among 11 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps. Figure 37 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 of each modulation rate studied during the 120 seconds test period and the average rate for each scenario, as presented in Figure 38. 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, it seems 48 Mbps and 36 Mbps were chose more frequently than 54 Mbps. The reason is the signal's strength is lower at longer distance, so given roughly the same noise and interference it needs a more robust modulation. Thus, the system automatically dropped to the lower rates in the auto mode.

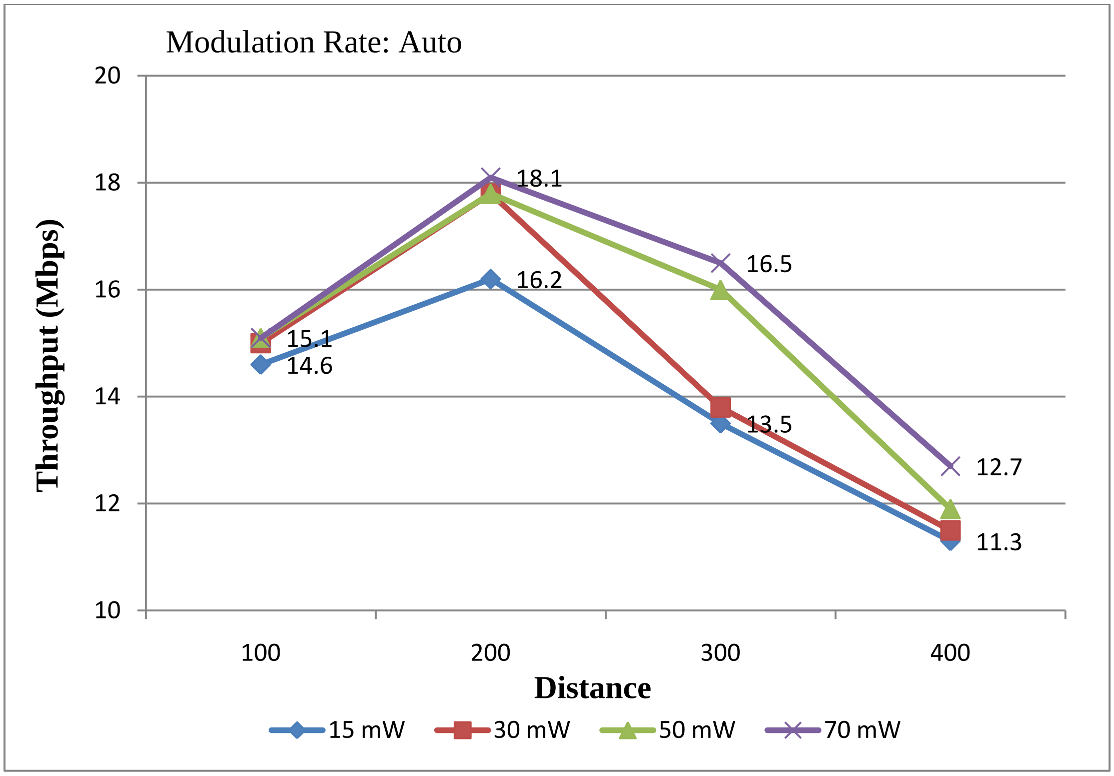


Figure 37 Saturated Throughputs at Modulation Rate Auto

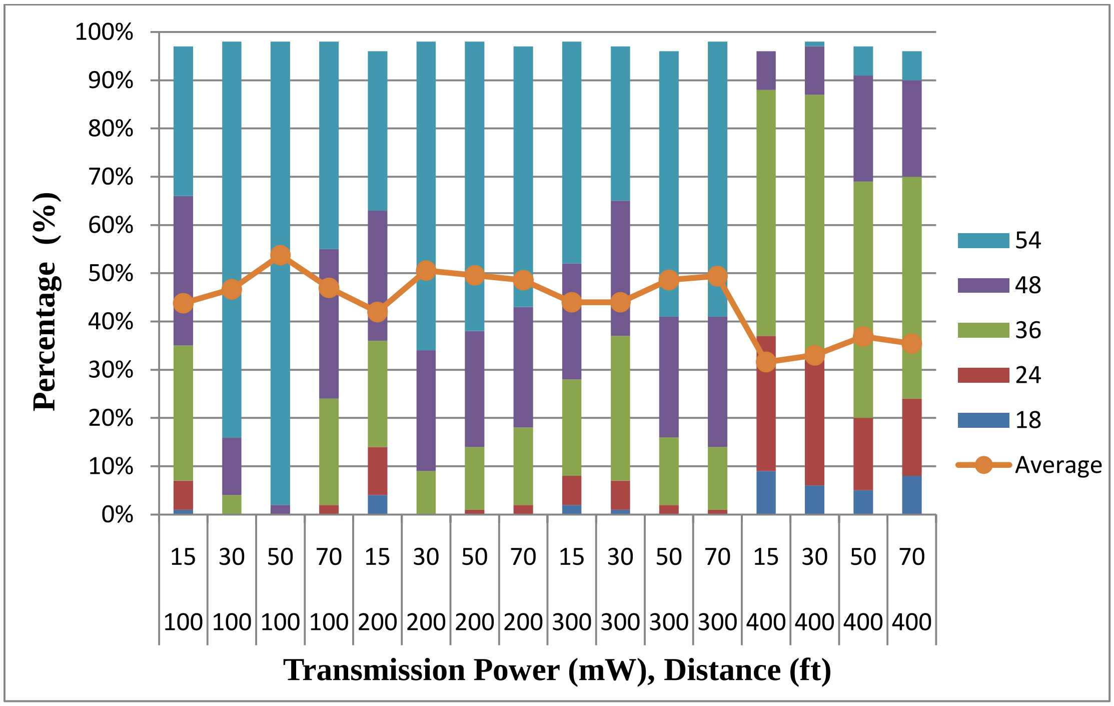


Figure 38 Percentages of Different Modulation Rates Used

Received transmission power is another important performance metric studied in the field test. The height of the antenna and the antenna gain 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):

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

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. In this study, the author 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, given the G_T, G_R, ht and hr, the product of $G_T G_R \frac{\left(h_t h_r\right)^2}{d^4}$ can be considered as a constant, K. Take the 10log10 of both side of $P_R = P_T G_T G_R \frac{\left(h_t h_r\right)^2}{d^4}$ 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 lost 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 39 a) to 39 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_t equal to 5 ft and 3 ft, respectively. The calculated K is shown in red color. As seen in the Figure 39, the measured pass 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. However, distance 400 ft is the reverse based on the test results. The author collected one data sample for each scenario at 400 ft. Further study need to be conducted to carefully look into this issue. At the same modulation rate, the path loss generally decreases with 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 pass loss at modulation rate 2 Mbps, 5.5 Mbps and 6 Mbps.

Therefore, 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 for different locations. 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 in the field for ITS applications.

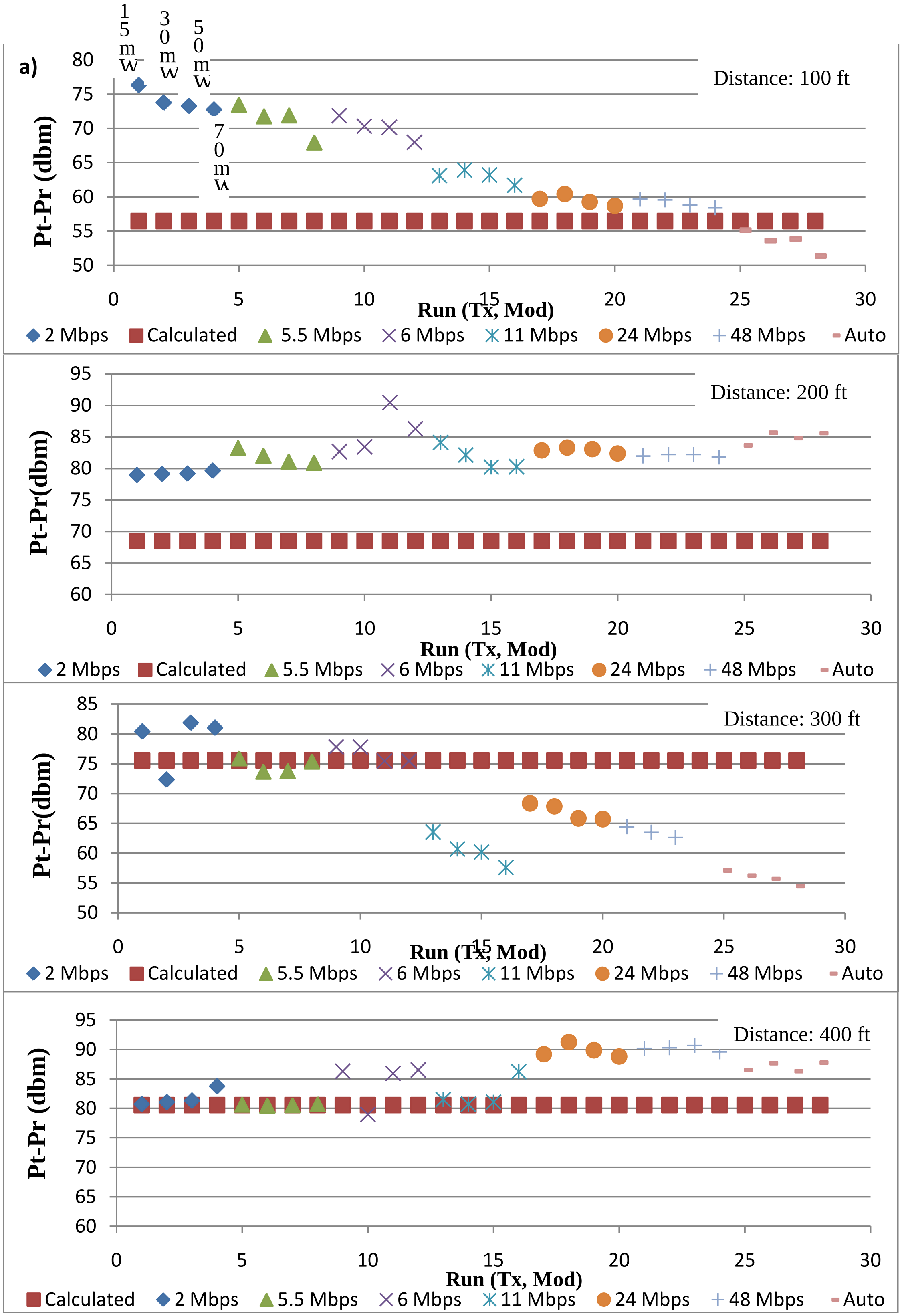


Figure 39 Path loss at different distance

Similar tests were conducted at SC State 93 between May to August, 2008. Only saturated throughput was measured at one distance using iperf. Figure 40 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 40, 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 36). 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. Therefore, 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 tests need to be conducted following the procedure proposed in this dissertation.

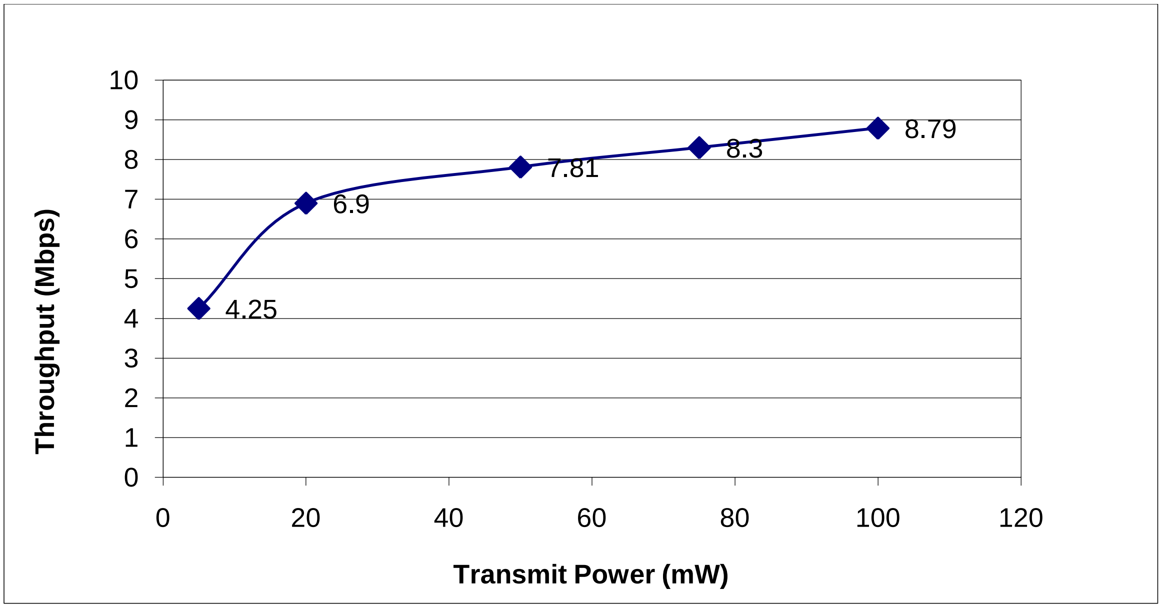


Figure 40 Saturated throughputs at different transmission power (TCP)

Tables 11 demonstrates field measurements in three scenarios, uphill, terrain blocking LOS, and downhill. 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 41 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 41, 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 on-line traffic management, effective operation relies on the amount of data that can be successively received by a TMC. If there is significant lost of traffic data in the network due to signal blocked by the roadway peak, the data that can finally transferred to a TMC would be much less than required, even if the rest of the network operated in an ideal condition. The network wide performance depends on the weakest link. Therefore, the impacts of different terrain determine ITS communication performance.

Table 11 Field measurements of 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

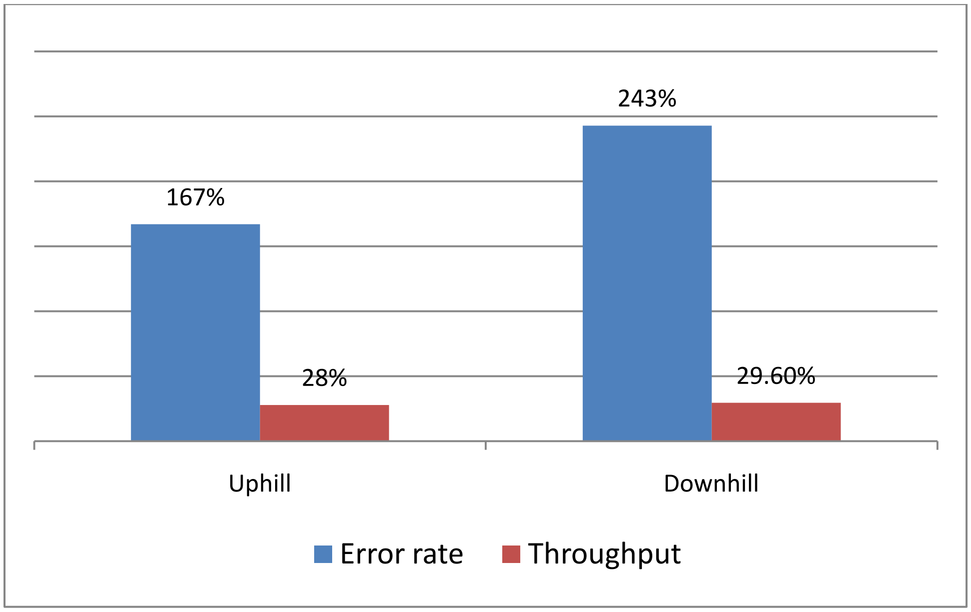


Figure 41 Improvement in error rate and throughput compared to "Over the Hill"

6.2 WiMAX Field Test

Two types of test, fixed operation and mobile test were conducted to assess the field performance of a regional WiMAX network. This section describes the test network, experimental setup and the methodologies used to collect field data of both fixed and nomadic operation test in a real highway environment.

6.2.1 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 12 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 12 Performance measurement results of WiMAX fixed operation test

Location No.	Avg US TCP Throughput (Mbps)	Avg 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 10, 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 author 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.

6.2.2 WiMAX Nomadic Operation Test

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 periodically (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 42 shows the legend used in the visualization results.

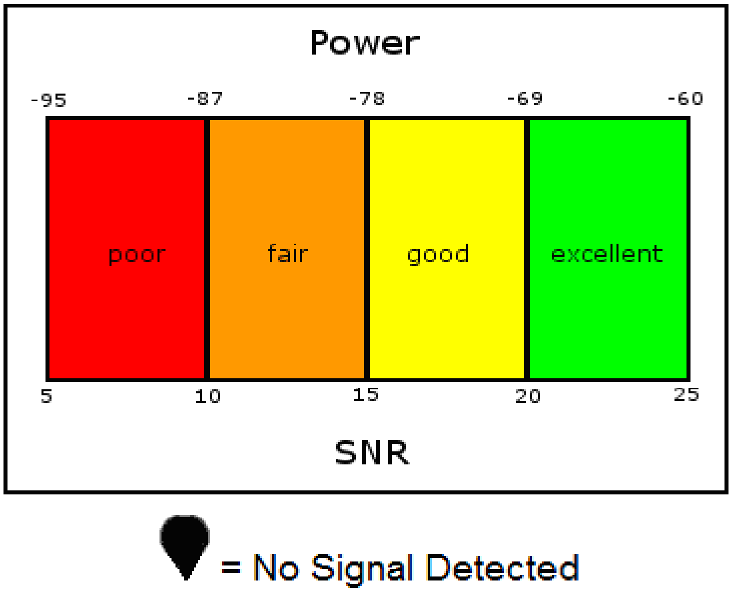


Figure 42 Legend of connectivity level

Figure 43 to Figure 45 illustrates 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. 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 43, signals level was very good at the beginning points, however 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.

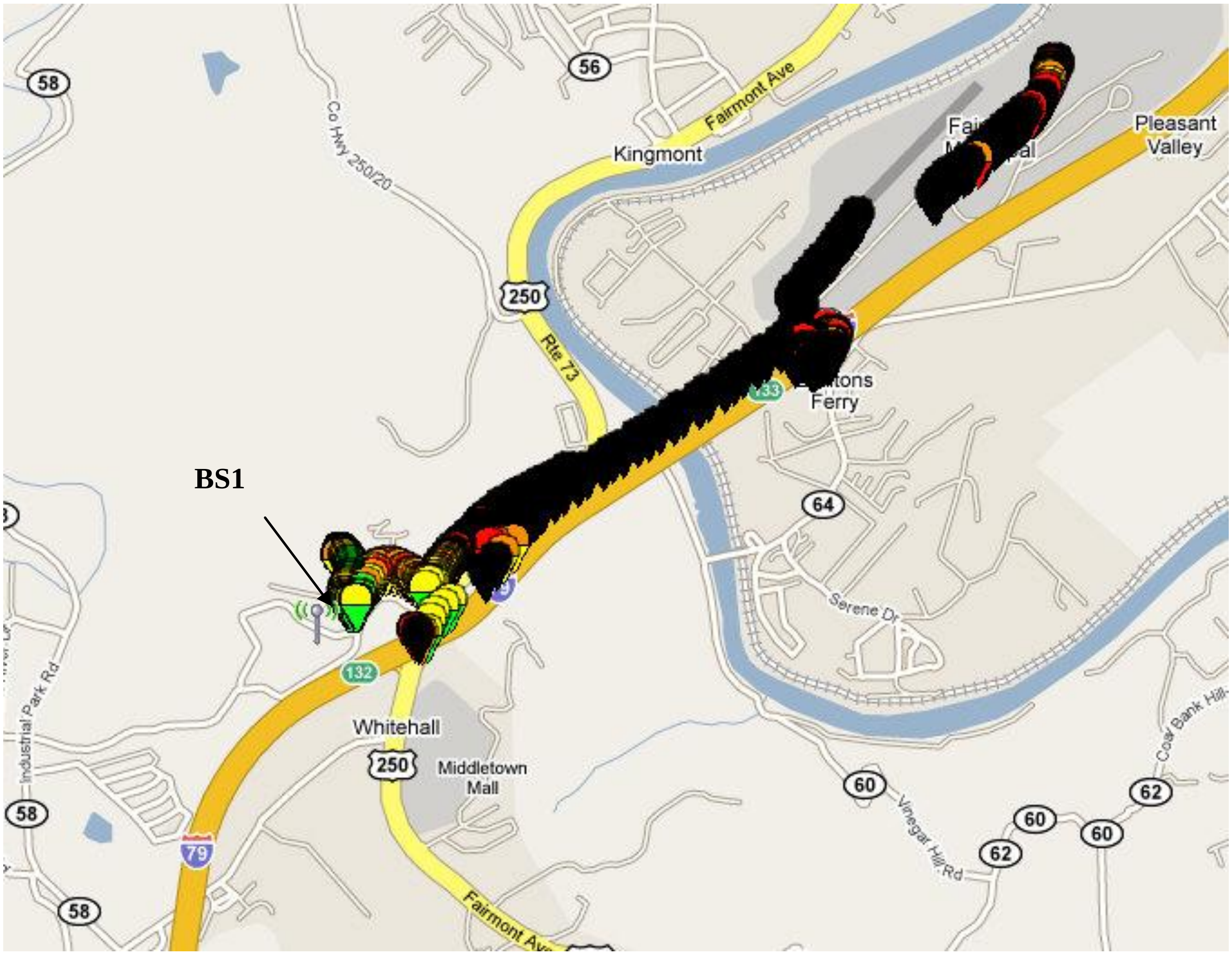


Figure 43 Connectivity level when associated with BS1

Figure 44 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 45 shows very good connectivity all along the way because the BS 3 located at very high altitude on the top of a hill; however detail altitude information was not available. In this case, the client always has very good LOS which ensures an operational link.

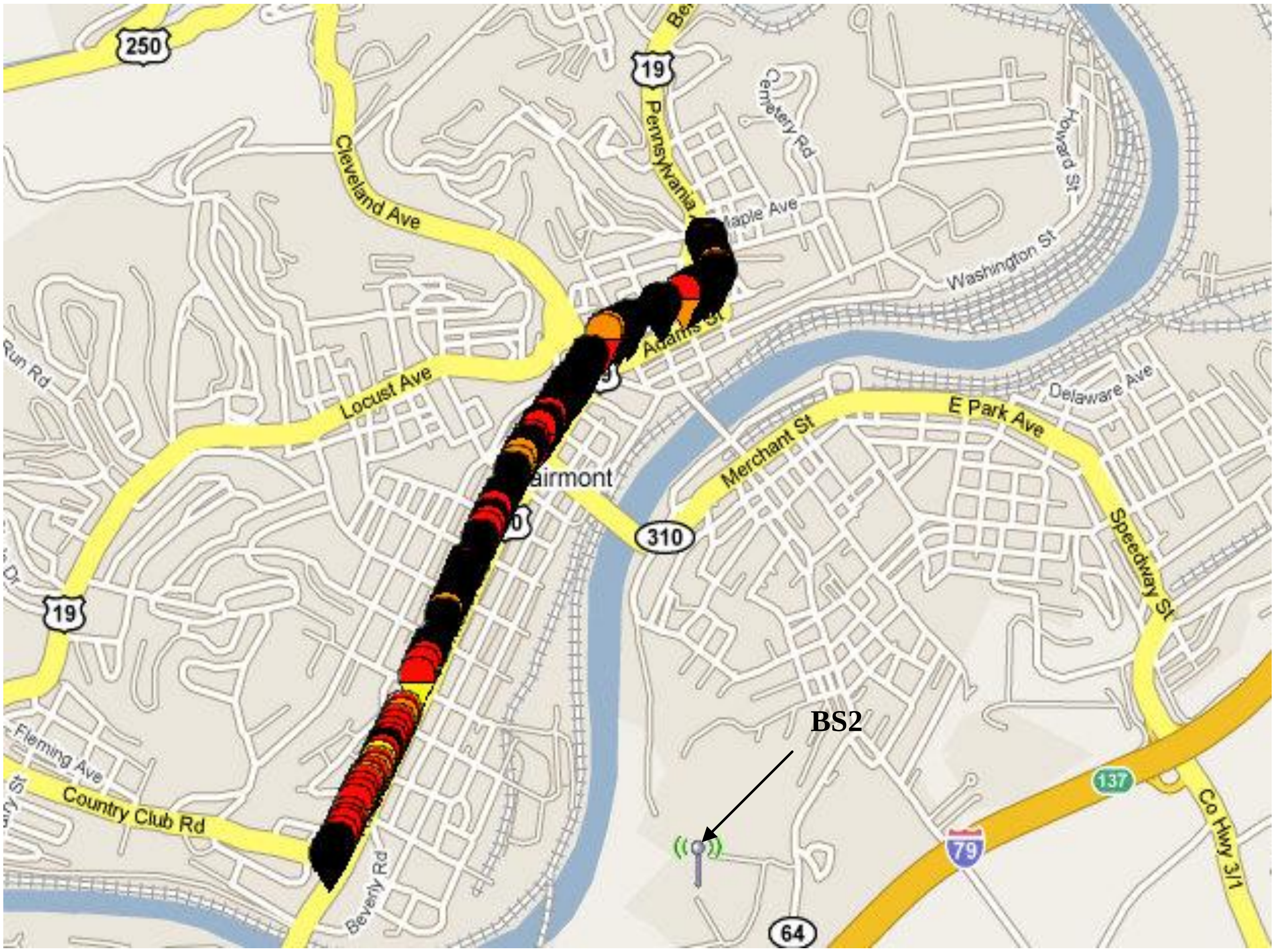


Figure 44 Connectivity level when associated with BS2

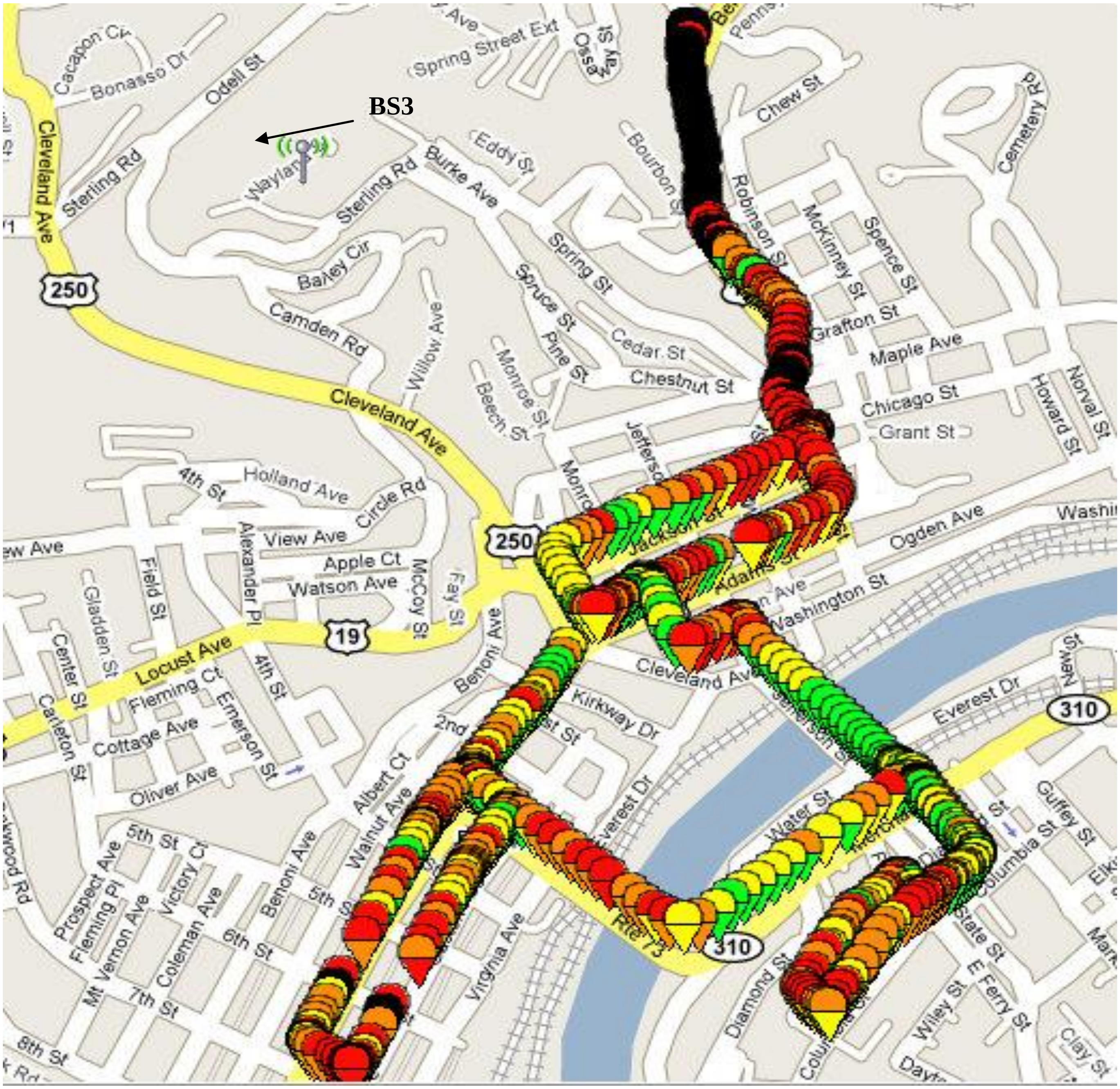
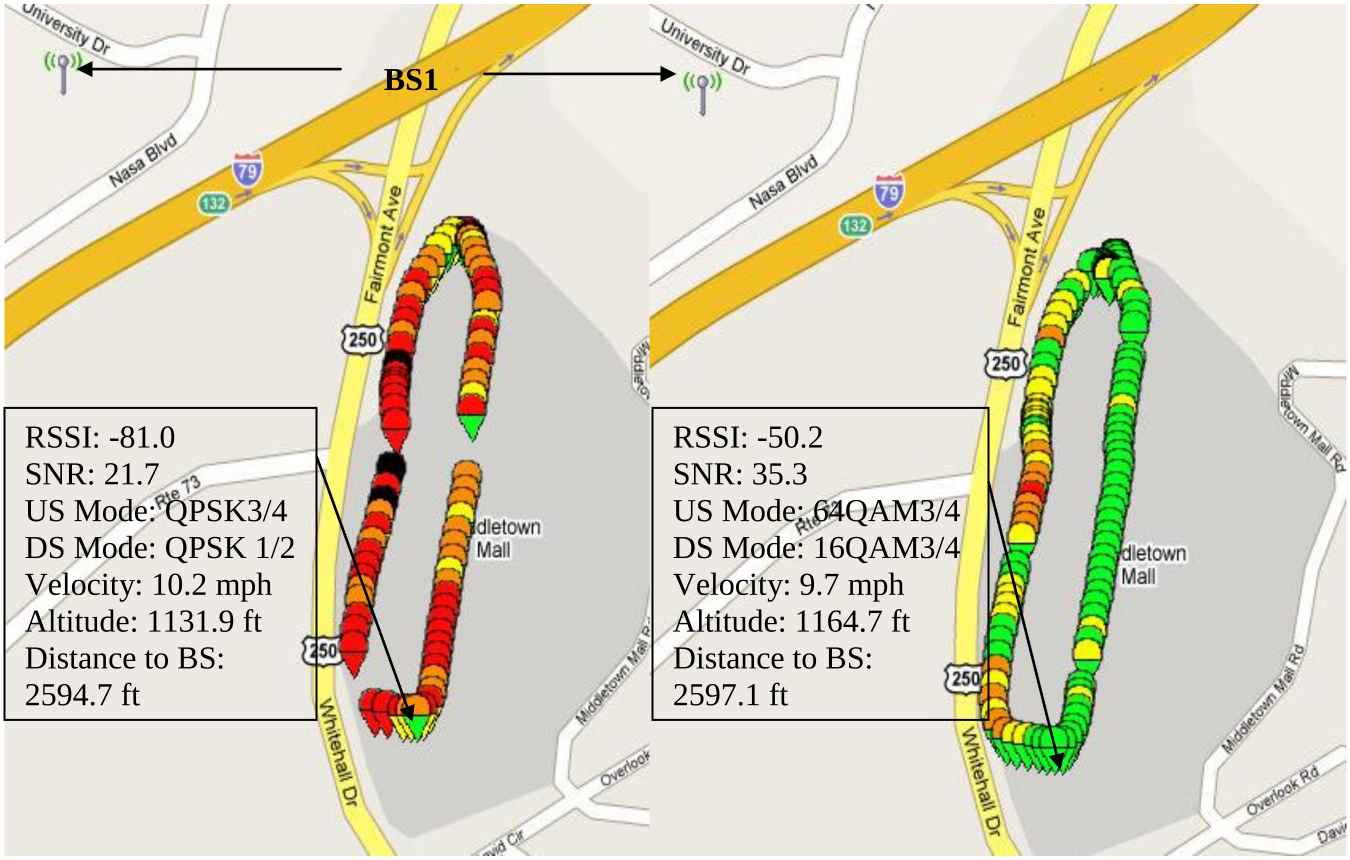


Figure 45 Connectivity level when associated with BS3

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.

Another factor however is the specific client devices, and in particular the quality of the antenna system.

Figure 46 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.



RSSI: -81.0
SNR: 21.7
US Mode: QPSK3/4
DS Mode: QPSK 1/2
Velocity: 10.2 mph
Altitude: 1131.9 ft
Distance to BS:
2594.7 ft

RSSI: -50.2
SNR: 35.3
US Mode: 64QAM3/4
DS Mode: 16QAM3/4
Velocity: 9.7 mph
Altitude: 1164.7 ft
Distance to BS:
2597.1 ft

Figure 46 Connectivity comparisons between different client devices

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.

6.2.3 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 study 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. Currently, 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 13 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 region, 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 13 (ITERIS 2008, BP Solar 2008*)* assuming the traffic camera is working 8 hours/day to support continues traffic monitoring. Solar module means that several solar cells combined into a module with the purpose of harvesting solar energy. Among several available solar modules, this study chose SX-40 and SX-50 as examples, which are general-purpose modules suitable for single-module 12-volt applications with DS 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 13 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 then 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 then the required amount.

As shown in Table 13, 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 study.

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.

6.3 Quality Requirements of Online Traffic Monitoring

The researchers first conducted correlation analysis of the jitter and missed video time in seconds. Table 14 demonstrates examples of the data collected during these tests. The correlation coefficient of these two parameters was 0.944, indicating a high correlation between the jitter and video quality. Therefore, these results that jitter is a key indicator of the video continuity of the real-time video streaming, supporting the findings of previous studies.

Table 14 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
…	...	…

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 47. The first significant jump, about 7 seconds, (see packet 84 in Figure 47) was caused by the initial link connection and was not considered in the video quality analysis. The second jump shown in Figure 47 (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 47. Similarly, the researchers found each of the other two jumps also caused approximately four seconds of video to be missing.

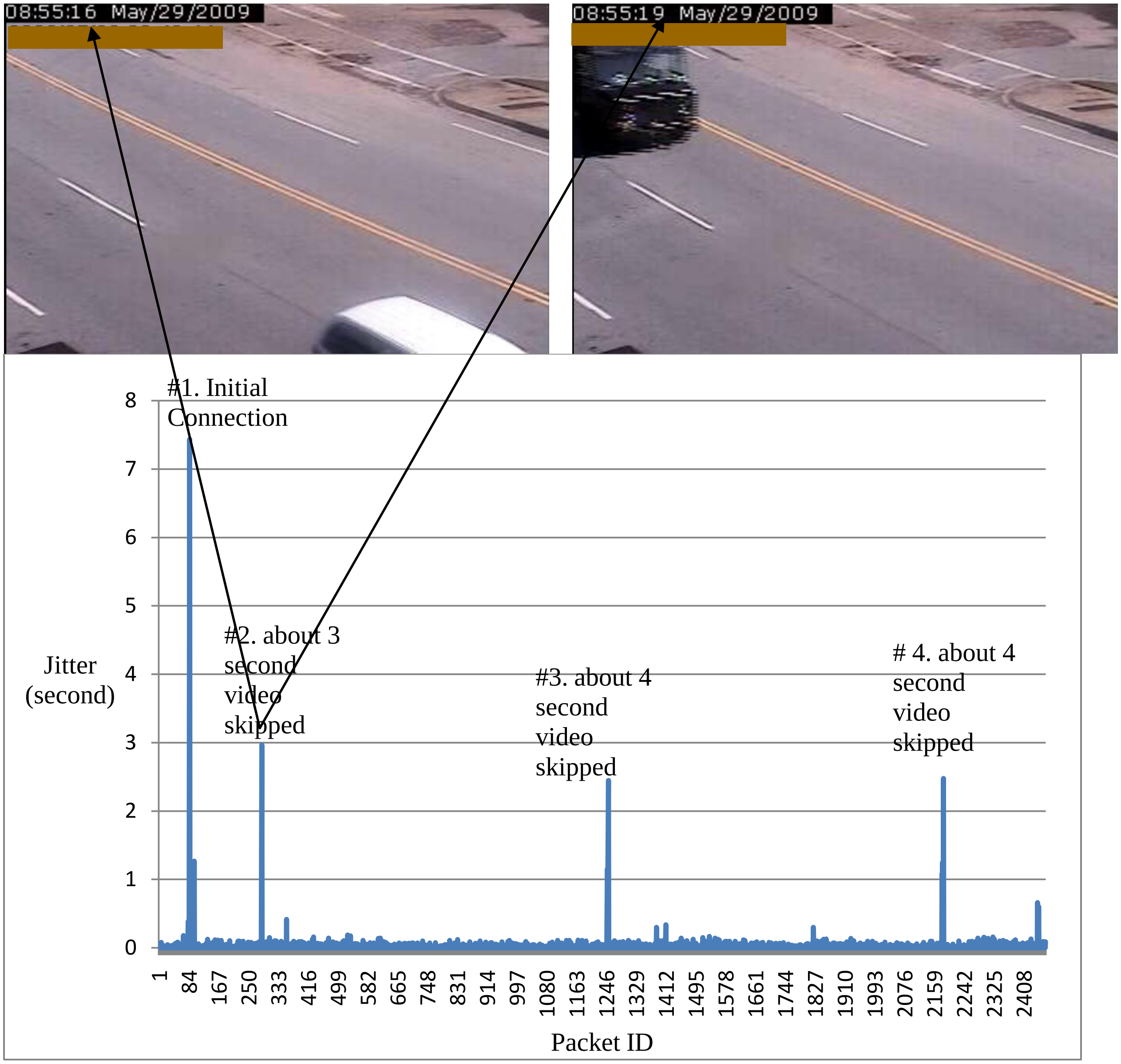


Figure 47 Example of the connection between jitter and video continuity

Figure 48 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 due to the allowable buffer.

Herein, the question is that which tolerated jitter value affects the smoothness of the real-time video quality. The results of all sixty five cases indicated that jitter values lower than 1 sec do not cause any data frame skips in the real-time video streaming, as shown in Figure 45. However, jitter between 0.5 to 1 second most likely slow down the video, so actually user can see the vehicle slowly passed the camera spot, albeit not in real-time. Therefore, the author proposes one second as the jitter threshold, above which, video discontinuity is most likely expected. For real-time traffic surveillance, smoothness and continuity are quite important especially at critical highway segments, key infrastructures and facilities. Traffic officers at TMCs are not able to see all the vehicles which have passed the surveillance spots if video frames are dropped or skipped. Effective techniques are needed to control the jitter below one second to prevent this. Moreover, it is not necessary to minimize the jitter in all the cases. Using appropriate jitter thresholds should ensure decent video quality for wireless supported traffic surveillance.

Another option is that a TMC can adopt a one second buffer to ensure smooth video transmission. The assumption made was that one second delay would not affect the effectiveness of on-line traffic management.

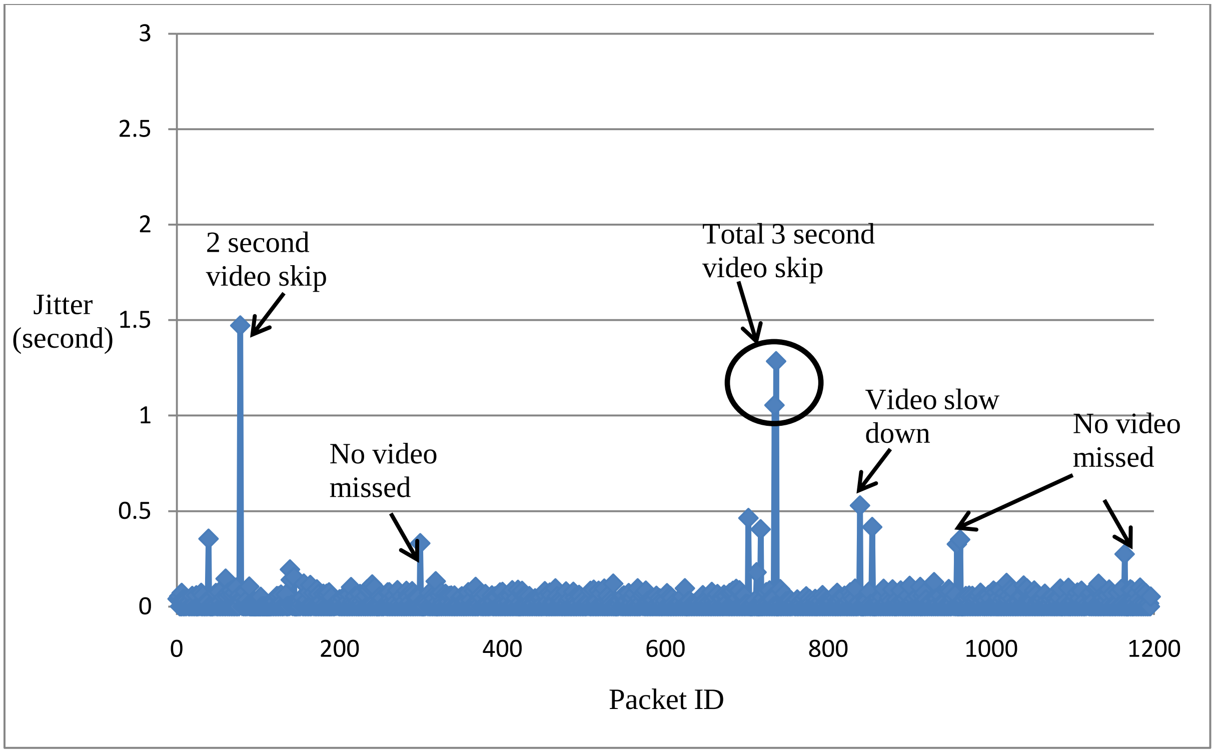


Figure 48 Example of the connection between jitter and video continuity

The next research question is which packet rate range provides acceptable quality of real-time traffic surveillance video. Although a JPEG codec can internally process 30 frames per second, the overall performance in the field is subject to many different factors, such as network throughput, number of users sharing the same bandwidth, and the image size (MOXA 2004). Generally, the link rate on a local network environment can achieve over 200 Kbytes per second, and approximately 10 to 20 frames per second. The general frame size of the traffic camera, in ideal conditions, is illustrated in the Table 15 as a reference for traffic agencies. This study chose quality level ‘Standard’ during the test period, so the corresponding theoretical bandwidth requirement was about 1784 Kbps.

Table 15 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

Figure 49 shows the percentage distribution function (PDF) of the average packet rates in second (frame rate). Average packet rate is taken for one minute video after each test. As seen from Figure 49, although the packet rate varies within a wide range, from poor (~3 packets/second) to extremely well (~ 50packets/second), the majority of observed packets were received at a rate between 23 to 33 packets/second. When the rate was lower than 15, one or multiple disconnections were observed, while videos with rates higher than 40 had no disconnections or slow downs. Average packet rate was around 26.3 packets/sec. Derived from the PDF graph, a cumulative distribution function (CDF) graph is generated as shown in Figure 50. 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 50. 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 author concluded that similar to many other video streaming applications, the quality of the real-time traffic surveillance is acceptable when the packet rate is above 23 packets/sec.

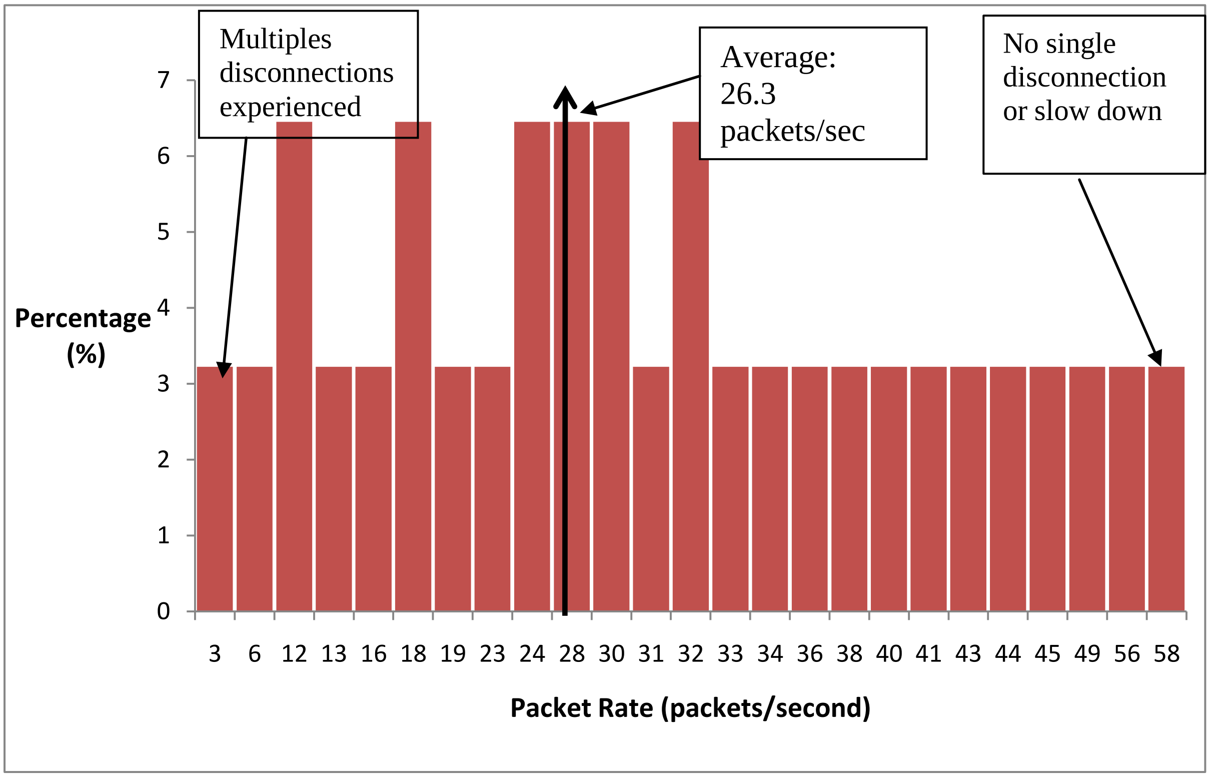


Figure 49 Percentage distribution function

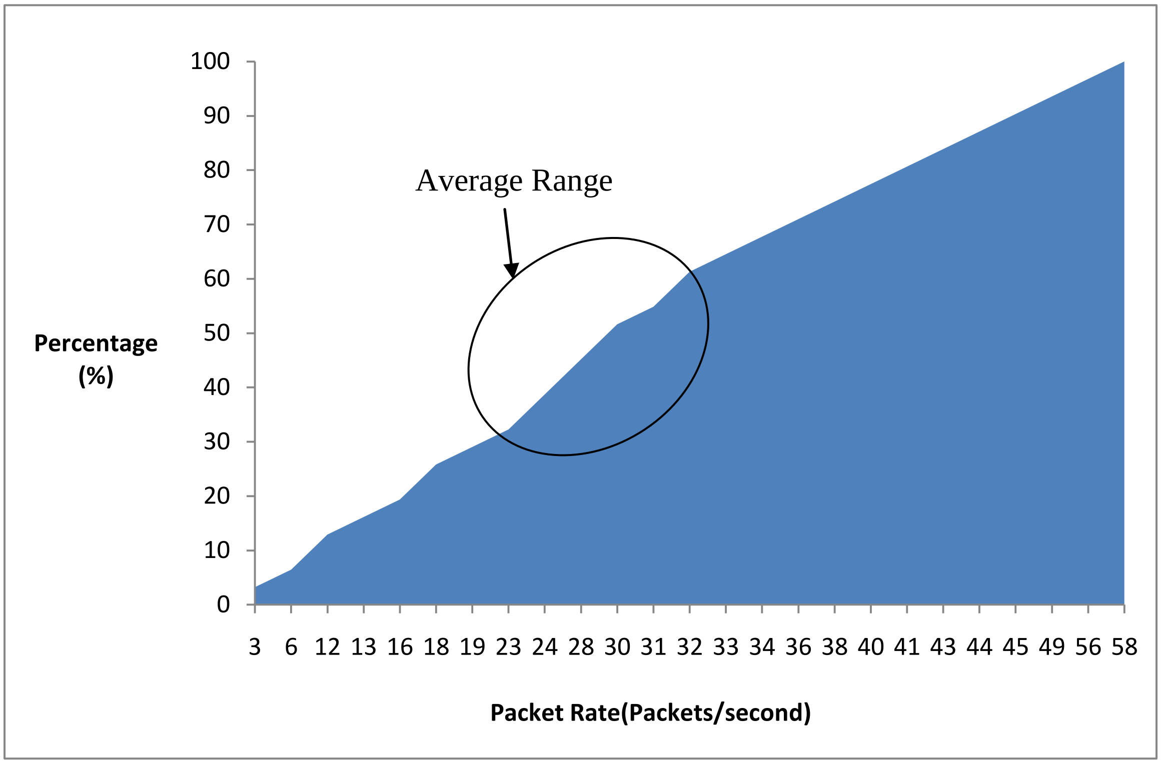


Figure 50 Cumulative distribution function of packet rate

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, 98Kbits/sec for two receiving computers. 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 the Table 15. 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 51 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. Therefore, the 802.11g wireless network cannot support two users simultaneously with smooth video image. Of course, this might change with an increased data rate of each camera. This study assumed that standard video quality is the minimum quality level for effective real-time traffic surveillance. 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. Therefore, when there are two flows (same source but two different receivers), if one of the flow drops more packets than the other during a short time, it may cause a short term observable degradation for that flow when the other goes well (Peterson et al. 2003).

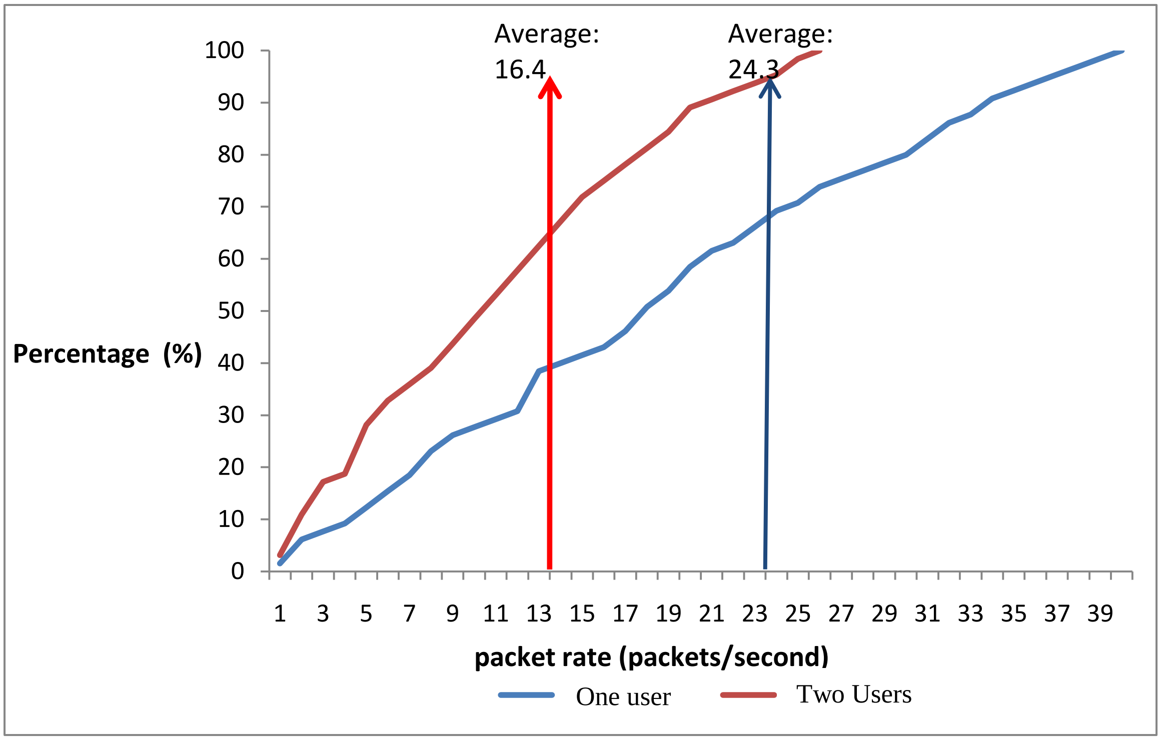


Figure 51 CDF Comparison of one and two receiving computers

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, this study 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.

CHAPTER SEVEN

7 SIMULATION AND PERFORMANCE-COST ANALYSIS

Based on the network topology presented in Chapter 5, a simulation study was conducted to assess the performance and reliability of a large scale wireless traffic sensor network. The simulation outputs were used to relate performance with costs for WiFi and WiMAX under two network topologies; infrastructure and mesh. Therefore, four different network options; WiFi mesh, WiFi infrastructure, WiMAX mesh and WiMAX infrastructure, were considered in the performance-cost analysis. Two different simulation studies were performed. One study evaluated the communication performance of wireless traffic sensor networks under two network topologies and the other evaluated the performance under different adverse conditions. Communication Network simulator ns-2 was utilized for both of these studies. Based on the performance analysis from the simulation study, a performance-cost relationship was developed to help compare between selected alternatives.

7.1 Ns-2 Simulation Analysis

The section presents the results of simulation analysis, ns-2 simulation and integrated simulation. The result of the ns-2 simulation was used in performance-cost analysis. The two selected MOEs, saturated throughput and delivery ratio, were analyzed with respect to different error rates, the number of relays (distance), and data rate for standard traffic cameras. 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.

The distance between the camera and controller is represented by the number of relays in between them. Figure 52 shows per-camera throughput in the three-mile network (three cameras sending video packets to one controller). The effects of different camera deployment distances were studied with different number of relays; each relay is placed 200 meters (650 ft) from the nearest camera or relay in both directions along the highway. As IEEE 802.11 has a randomized and shared medium access scheme, the more relays are expected to have a higher chance of collision among nearby wireless links (i.e. more colliding transmissions and retransmissions). The study serves to quantify the extent of such impacts. 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 52 shows, with 25 relays, 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.

Figure 53 and Figure 54 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. 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.

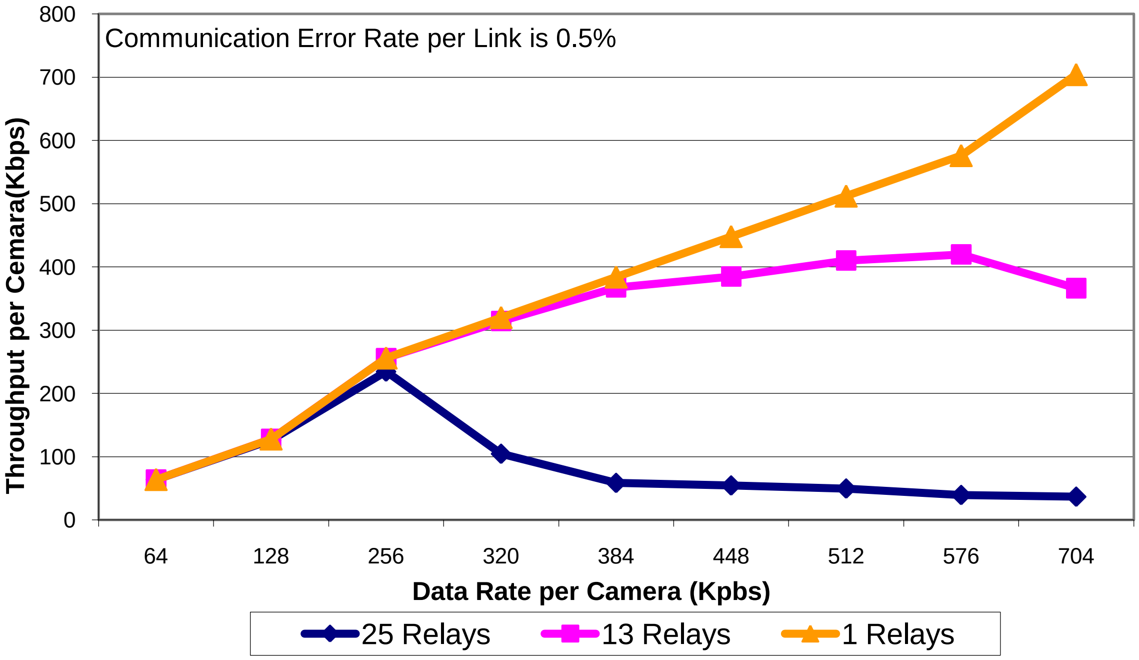


Figure 52 Farthest camera throughput with different number of relays

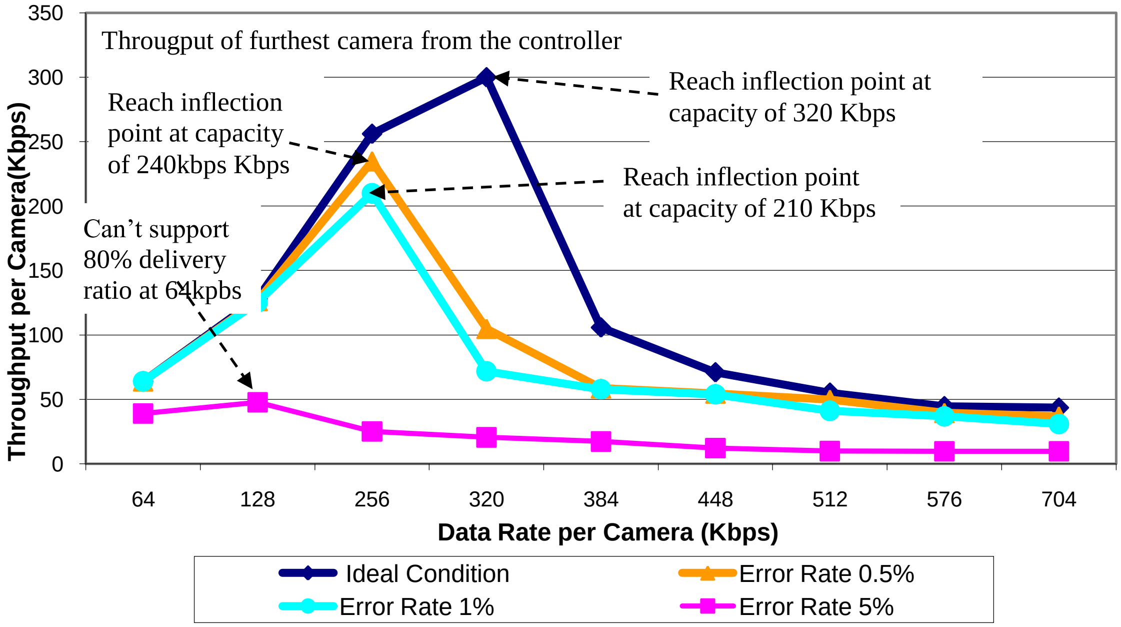


Figure 53 Farthest camera throughput at different error rates

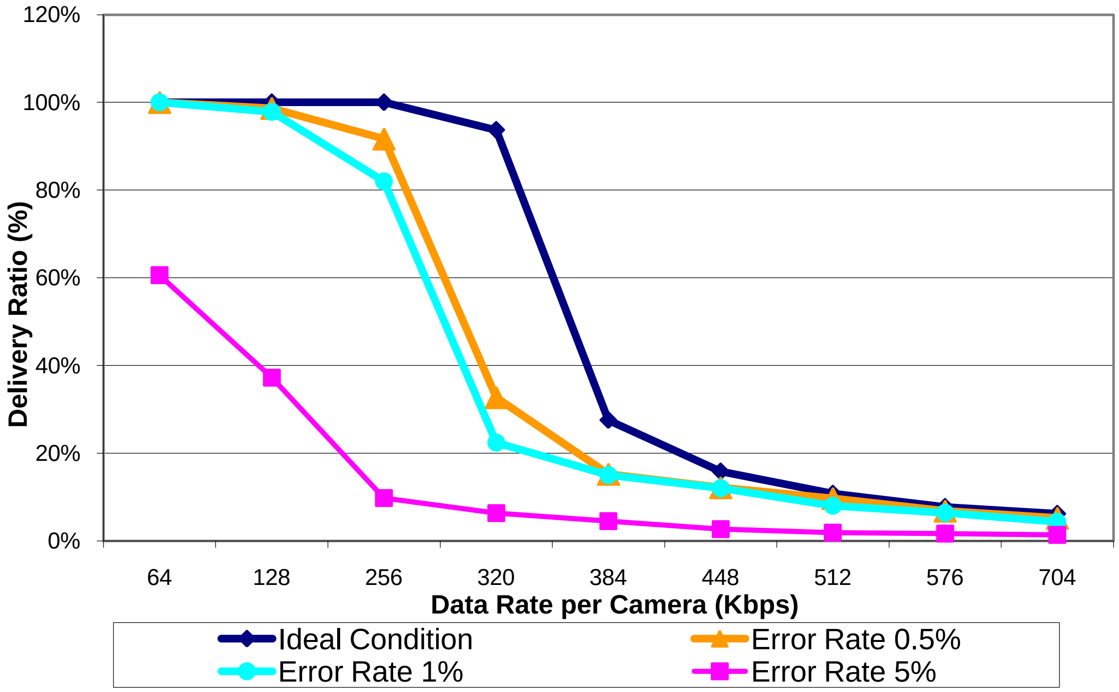


Figure 54 Farthest camera delivery ratio at different error rates

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 55. When only one camera is connected to the controller, the network performance is more tolerant to the use of more relays. 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. 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. The saturating throughput for each sensor (camera) need not be maximized; instead, it needs only to meet its specific throughput requirement. However, for key traffic infrastructure such as tunnel and bridges, traffic agencies might need to have camera directly connected to TMC with a dedicated link to ensure the surveillance quality in adverse conditions.

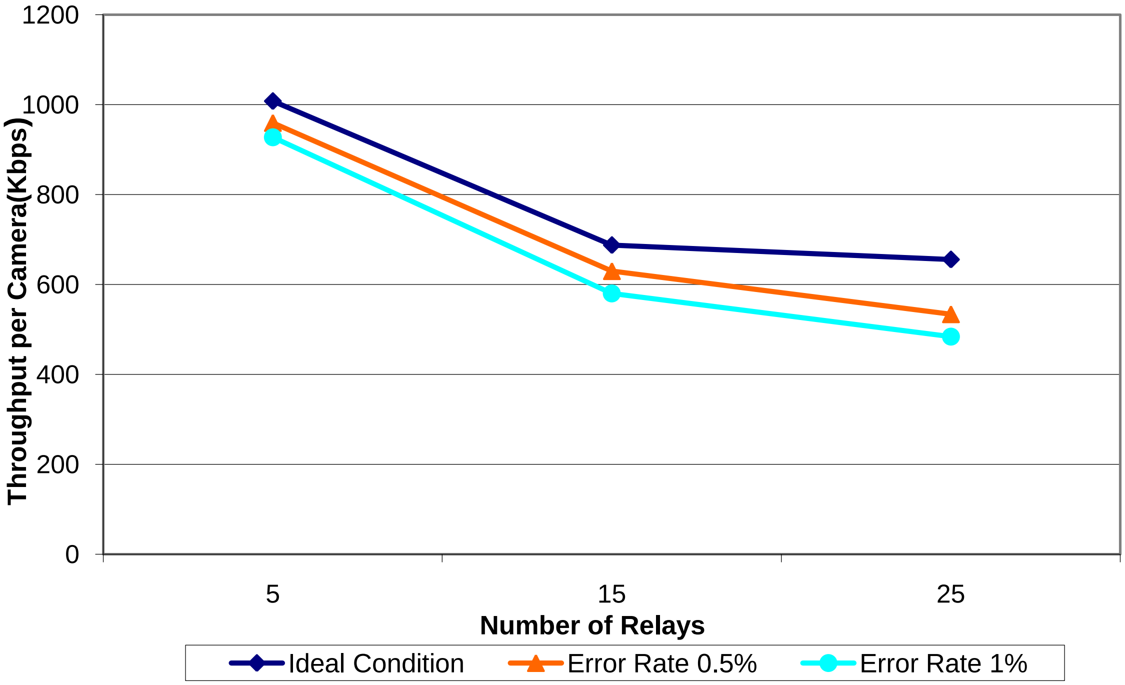


Figure 55 Throughput of one camera at different locations with different system error rates

In general, a trade-off analysis is necessary for making investment decisions for additional communication infrastructures to meet specific performance requirements. The throughput and error rate relationship studied in this dissertation provides a template for such analyses. For example, Table 16 lists the tolerable wireless error rates with respect to different camera quality requirements.

Table 16 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%	NA	NA
Medium	384	5%	3%	2%
Low	256	7%	4%	3%

NA: The system can not 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). Similarly, the analysis can be based on the number of cameras. For a network where the farthest camera is 15 relays away, Table 17 shows the tolerable error rates with different quality and number of cameras.

Table 17 Tolerated Error Rate at Different Number of Cameras (15 relays to the controller)

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

NA: The system can not support this saturated throughput

7.2 Integrated Simulation

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. With sensor spacing 0.4-0.5 mile, Figure 56 shows an example of variation of communication latency in 600 second simulation time after an incident. As showed in Figure 56, the communication latency with 32 Kbps data rate varies in the range of 0.2- 0.35 sec with an average 0. 263 second, while the 1024 Kbps varies in the similar range. The average communication latency of all the simulation cases is about 0.266 sec for both 32 Kbps and 1024 Kbps data rate. 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, this doesn't indicate that the communication throughput is not saturated when sending 1024 Kbps because only the latency of the data package that successfully received by the controller is measured. 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 is over saturated. Therefore, communication latency only shows that 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 TMC likely to experience video slow down or disconnection. Table 18 summarizes the communication and traffic operational performance.

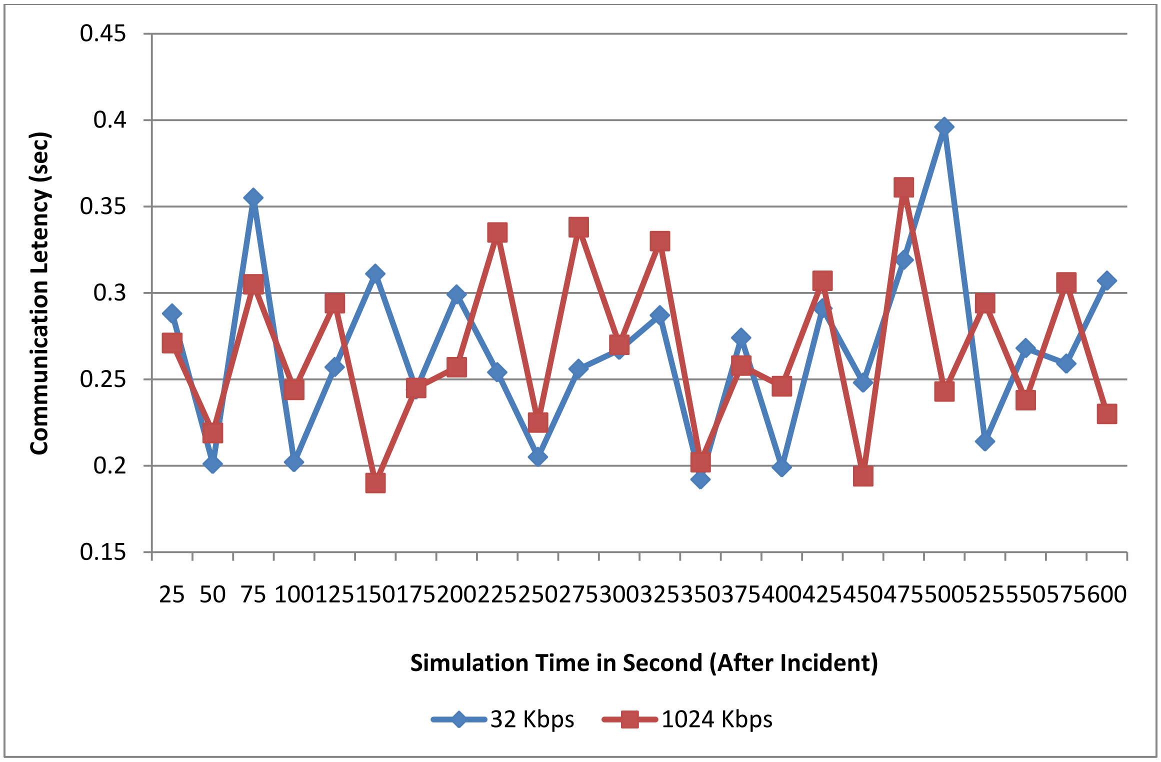


Figure 56 Examples of Communication Latency at Different Data Rates

Table 18 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 18, 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 a incident in a timely fashion. However, the incident scenario studied is the most severity case which blocks all the traffic lanes in one direction. The traffic queue builds very fast and no vehicle is going to 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 study did not test other incident scenarios in terms of incident severity.

7.3 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 19. 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 19 does not consider any recurring cost resulting from leasing the connectivity from an ISP, nor does it show any maintenance related costs. This cost should be same for all four scenarios, so it would not affects the comparison outcomes.

For Greenville network, Table 19 lists the cost and number of base stations and client radios required for both the mesh and infrastructure architectures. For the WiFi infrastructure network, seen from Figure 32 (p.112), 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 (WiFi 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 WiFi 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, shown as the blue star in Figure 30 (p. 110). 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, WiFi infrastructure requires 14 Cisco 1410 radios, while WiFi 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 33 (p.113) 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 19. With this information we can see that the WiFi Mesh architecture provides the lowest cost solution, while the WiMAX infrastructure architecture is the most expensive.

Table 19 Cost Analysis for Greenville Network

Architecture	Technology	Base Stations	Unit Cost	Client Radios	Unit Cost	Total Cost for Radios	Fiber Connections
Mesh	WiFi (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	WiFi (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

As discussed in Chapter 3, the benefit is measured as total throughput needed for the Greenville traffic surveillance network. The ns-2 communication simulator was used to model the network and communication between devices. For the WiFi 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 57 (Ma et al. 2009). The results of the previous section, ns-2 simulation analysis, also indicated the average link rate that each camera can receive depends on the rate of the last link within the same mesh cluster.

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 dissertation. 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 WiFi 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.

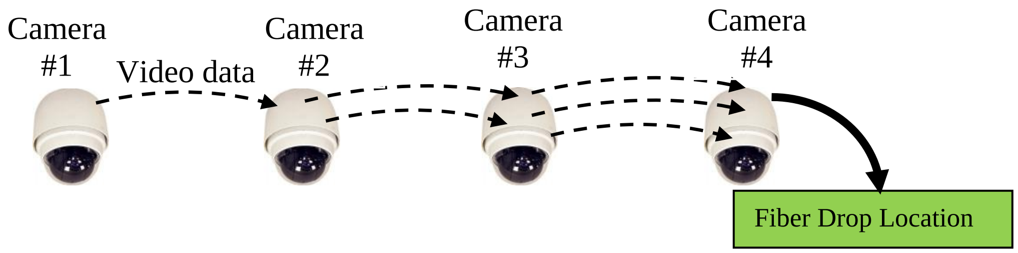


Figure 57 An Example of Data Transmission within One Mesh Cluster

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). This study assumes each camera requires 384 Kbps data rate, so the throughput requirements of the entire network is the 384Kbps times the total number of cameras. Although the infrastructure provides more bandwidth per device, this study used the actual demand rather than highest throughput possible for each WiFi and WiMAX network topology. Therefore, throughput-cost ratio was calculated by dividing the actual throughput requirements by total equipment cost. Table 20 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 20 Comparison of Four Network Architectures

Technology	Architecture	Average Throughput (Mbps)	Throughput Requirements (Mbps)	Total Cost ($)	Throughput/Cost (Bits/Dollar)
WiFi	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 20 indicated that the WiFi infrastructure and mesh network had the same throughput-cost ratio. Considering the number of fiber drops needed, a WiFi mesh solution has highest throughput-cost ratio for Greenville traffic camera systems, while the WiMAX mesh is next higher option. Because the WiMAX mesh was found has 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 author discussed in the case study section, compared to infrastructure option, the mesh option has less expandability for future ITS devices deployment.

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

CHAPTER EIGHT

8 CONCLUSIONS AND RECOMENDATIONS

The chapter first presents conclusions developed based upon the study results. Then, the second part of this chapter presents recommendations for utilizing the research results presented in the dissertation and future research needs.

The author also developed an implementation strategy, presented in Appendix D, to help state agencies to utilize the research results. The implementation strategy summarizes the most important characteristics in selecting the technology alternatives, the major steps used in designing the wireless sensor networks, the key factors need to be considered connecting sensors in the field or field to the TMC, and to identify possible sources of opportunities and concerns within the implementation process.

8.1 Conclusions

Wireless communication technologies have gained increasing attention in wide aspects of the transportation area. More states throughout the country are moving towards deploying large scale wireless communication-based ITS networks to improve traffic safety, efficiency and mobility for both daily and emergency situations. This dissertation conducted a systematic study of the performance, reliability and cost-effectiveness of three wireless technoglies; WiFi, WiMAX and DSRC, as communication platform for on-line traffic surveillance. The focus of this dissertation was on the communication between roadside traffic control devices, and between devices and TMCs.

Survey responses revealed that public agencies are using WiFi, cellular services provided by commercial carriers, state owned and operated microwave systems and 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 potential wireless technologies, such as WiFi and WiMAX. This is because of their broadband capabilities and potential cost-effectiveness. 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 network in seven metropolitan cities in South Carolina provided an excellent opportunity to present a process of planning a wireless traffic sensor network. The study interfaced potential wireless systems with the existing ITS backbone. This case study also addressed the use of WiFi and WiMAX technologies to adequately cover the region to support the required surveillance performance requirements. It also allowed for the comparison between WiFi and WiMAX architectures when dealing with a relatively sparse camera density.

8.1.1 WiFi Field Tests

The author 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 WiFi (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 become very unreliable as most packets are dropped. These findings imply that when traffic agencies implement wireless sensor network in the field, traffic sensors nodes should be deployed within a distance that can be supported at a chosen modulation rate to ensure reliable effective data transmission for traffic management applications. 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 rate as auto 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 and locations.

8.1.2 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 a WiMAX wireless supported traffic surveillance system. 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 solo powerconfiguration design.

8.1.3 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. Experimental results suggested that the 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 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.

8.1.4 Simulation 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 environmental onditions. The wireless sensor based traffic monitoring system was 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 indicated that within a wireless network, the number 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 should 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. 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 tunnel and bridge, traffic agencies might need to have a camera directly connected to TMC with a dedicated link to ensure the surveillance quality in adverse conditions.

Simulation analysis indicated that with a 5% error rate, the saturating throughput dropped below 64 Kbps, which is far lower than the typical traffic camera data 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.

8.1.5 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 WiFi infrastructure and mesh network had the same throughput to cost ratio. Considering the number of fiber drops needed, a WiFi 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.

8.2 Recommendations

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

8.2.1 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 environmental

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 higher bandwidths are required for large scale video surveillance.

- Performance-cost analysis provides a foundation for further investigation of the benefit-cost analysis of WiFi 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.

8.2.2 Recommendations for Future Research

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

- Future field study should be conducted to quantify the effects of modulation rate and transmission power on received signal power. 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 study should also be conducted to quantify the errors 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. Future research should also evaluate important parameters related to the surveillance video quality received from multiple video sources through a wireless network and the Internet.

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)

_____WiFi ____________________ ____________________

_____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	________________________	______________________
___WiFi	________________________	______________________
___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)
WiFi			
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

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-1below.

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.

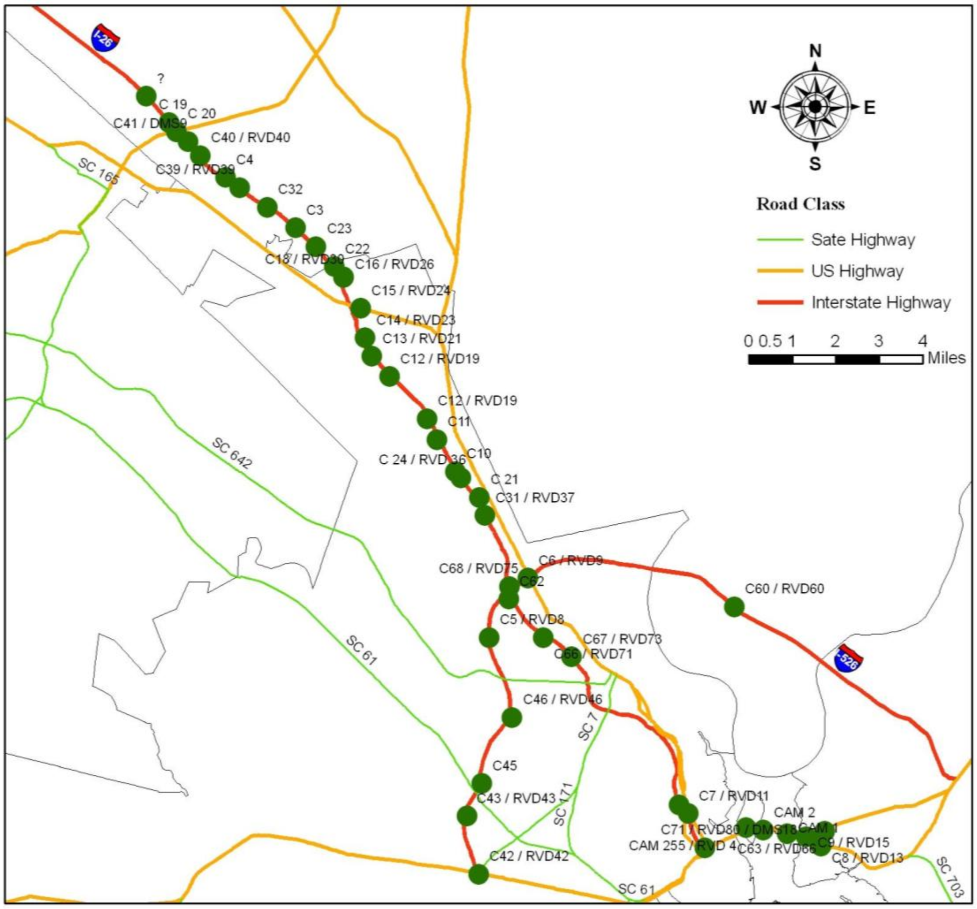


Figure C-1 Traffic Surveillance Devices in Columbia, South Carolina

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.

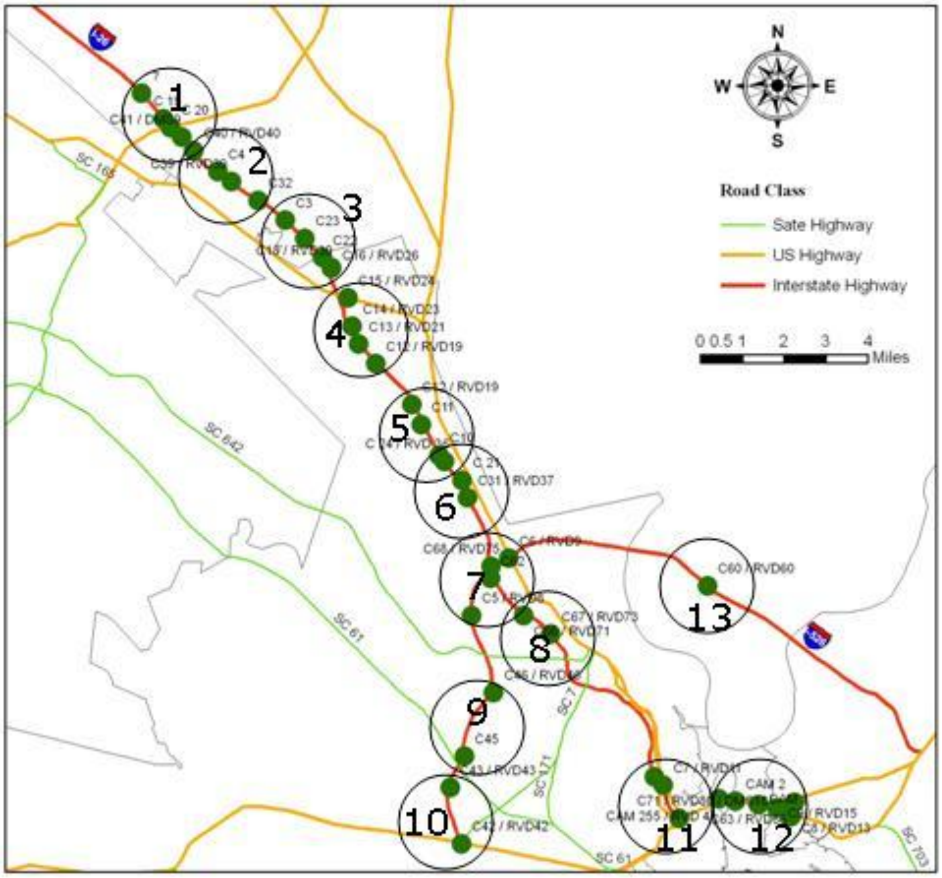


Figure C-2 Traffic Surveillance Devices in Columbia, South Carolina

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

WiFi Infrastructure Network

The WiFi infrastructure model is shown in Figure C-3 below, and divides the forty-two nodes into twenty-two clusters. Each cluster would have its own fiber optic access.

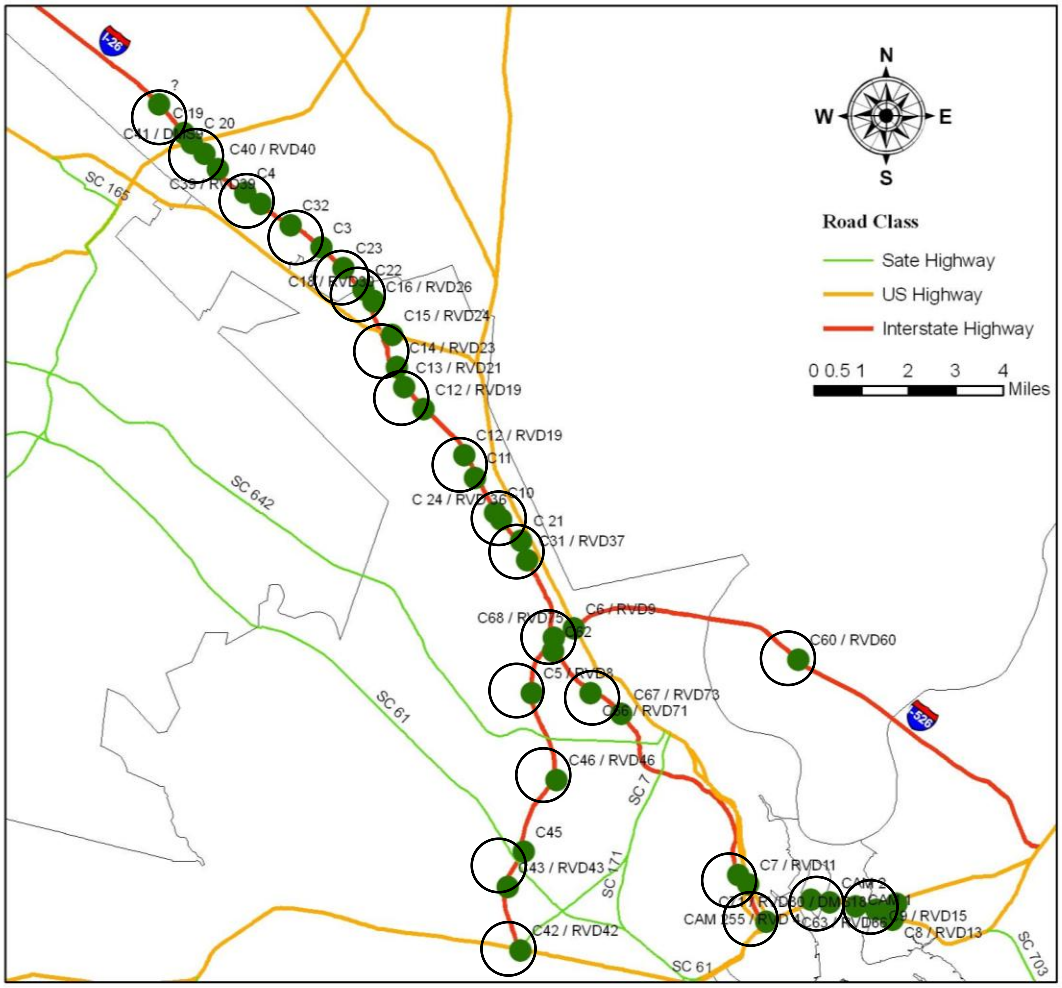


Figure C-3 WiFi Infrastructure Model of Columbia Site

<u>WiFi Mesh Network</u>

The WiFi mesh model is shown in Figure C-4 below, and 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.

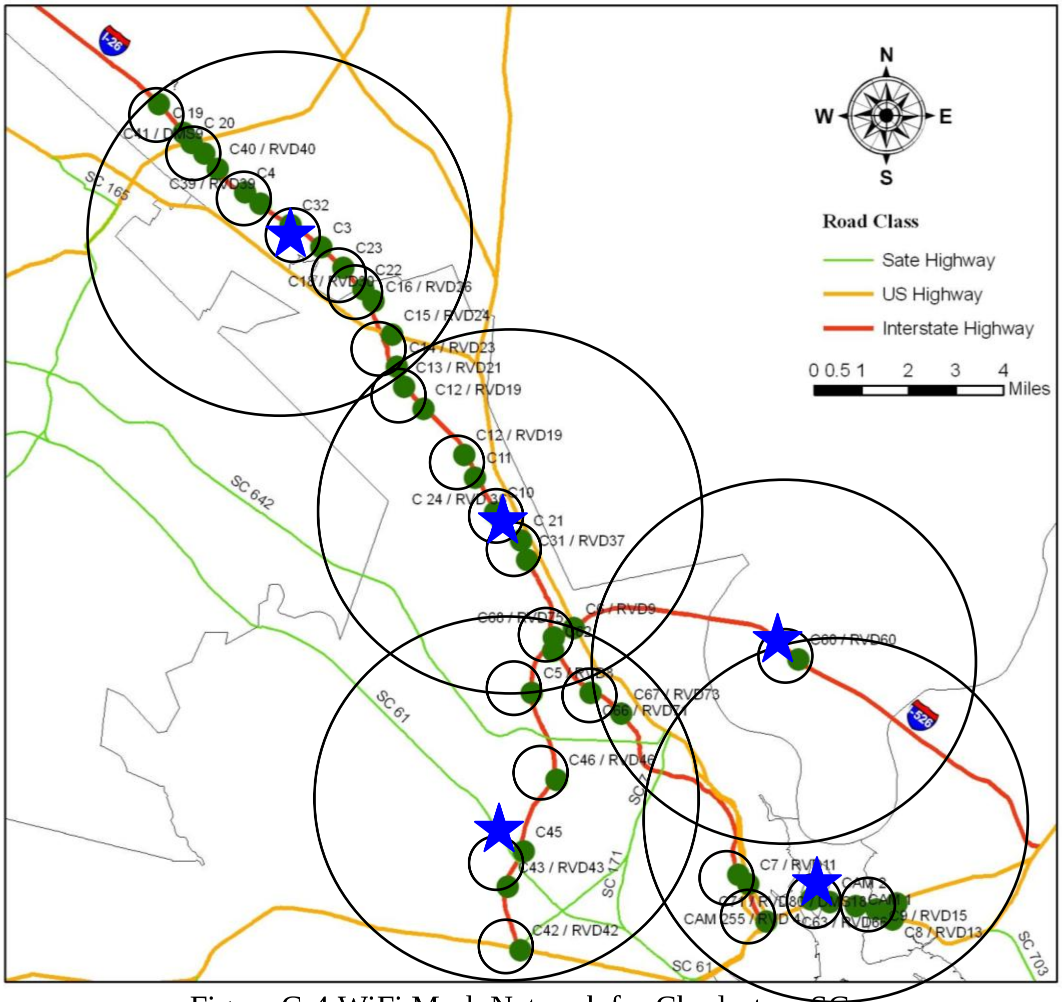


Figure C-4 WiFi Mesh Network for Charleston, SC

WiMAX Mesh Network

The WiMAX mesh model is shown in Figure C-5 below, and divides the twenty-two clusters in the same manner as the WiFi 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.

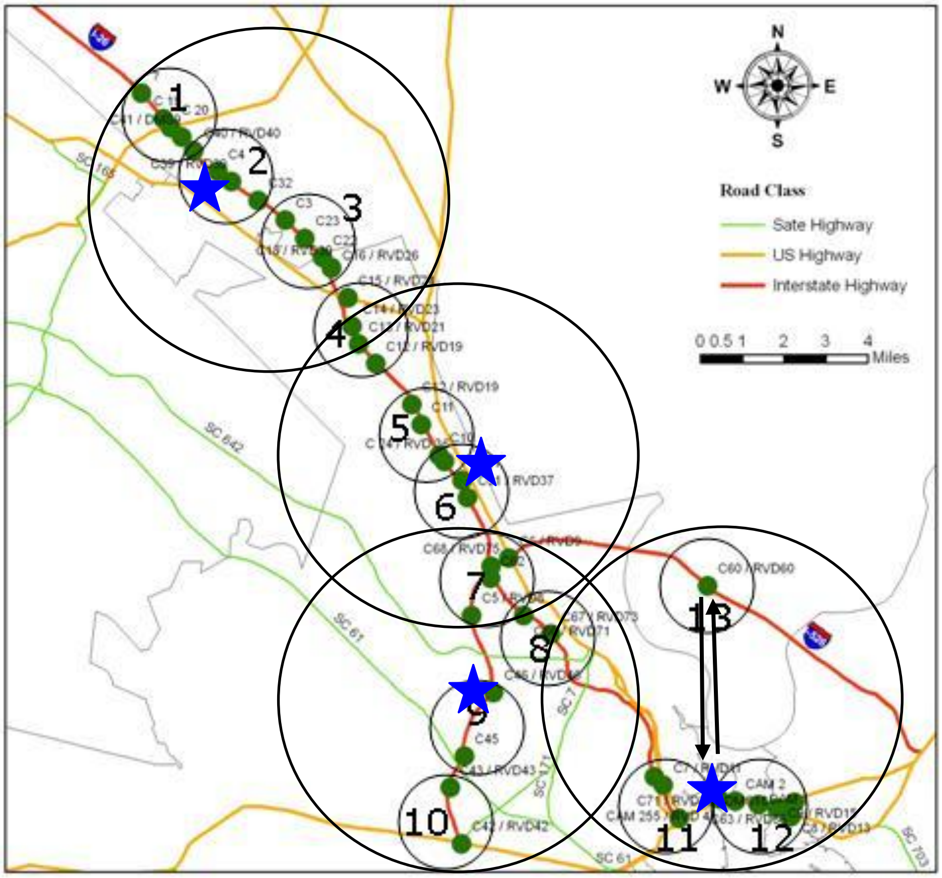


Figure C-5 WiMAX Mesh Network for Charleston, SC

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.

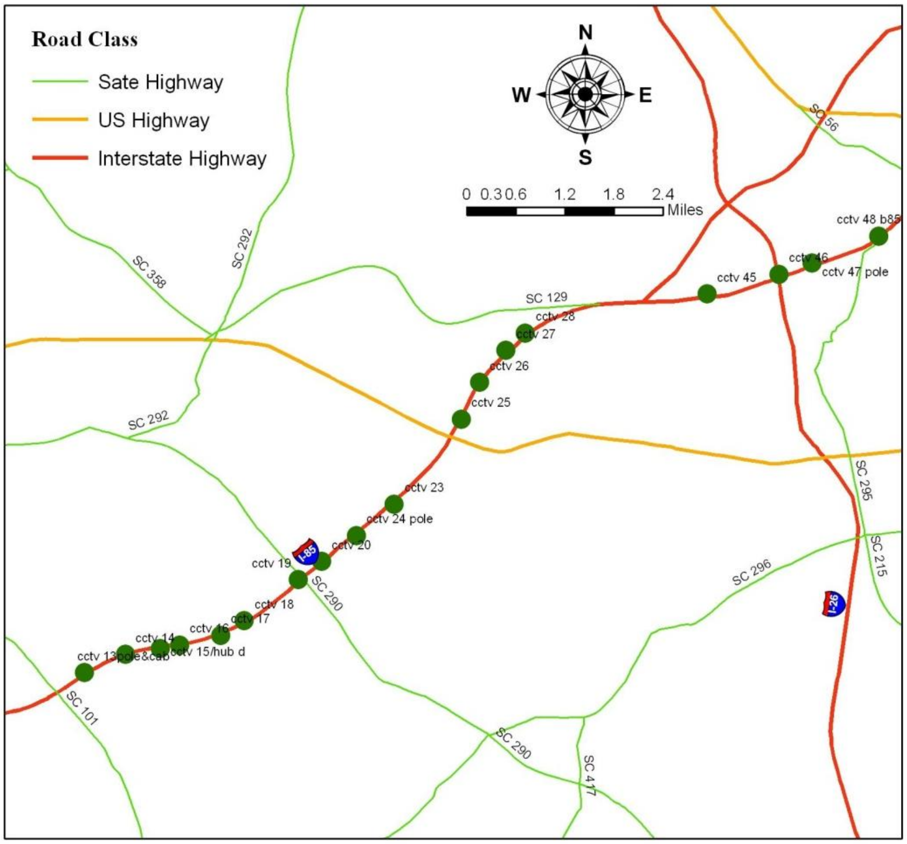


Figure C-6 Traffic Surveillance Devices in Spartanburg, South Carolina

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.

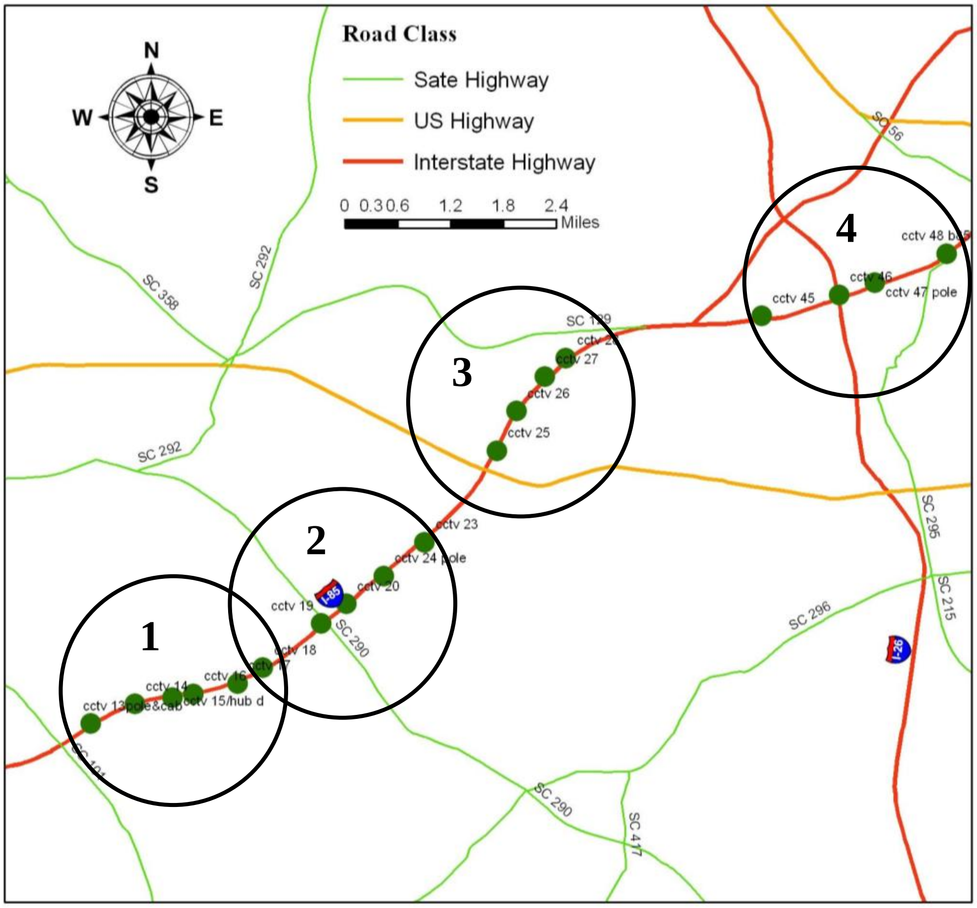


Figure C-7 WiMAX Infrastructure Network for Spartanburg, SC

WiFi Infrastructure Network

The WiFi infrastructure model is shown in Figure C-8 below, and divides the eighteen nodes into ten clusters. Each cluster would have its own fiber optic access.

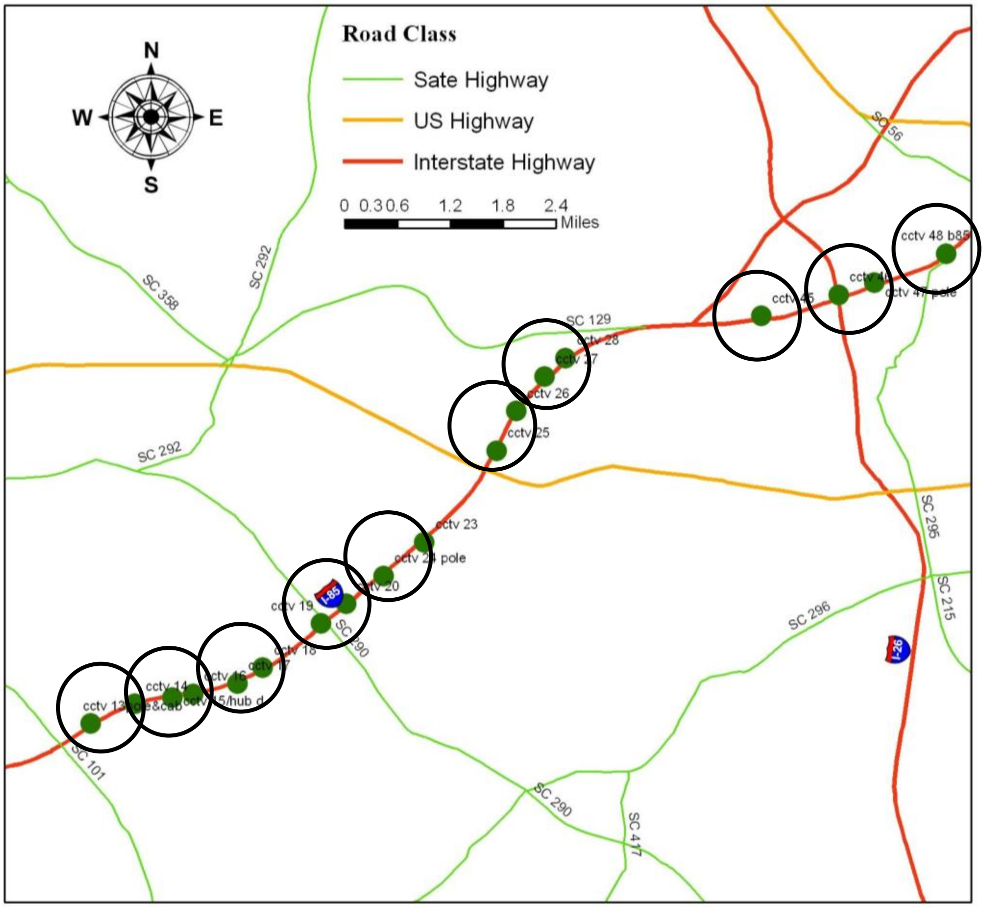


Figure C-8 WiFi Infrastructure Network for Spartanburg, SC

WiFi Mesh Network

The WiFi mesh model is shown in Figure C-9 below, and 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.

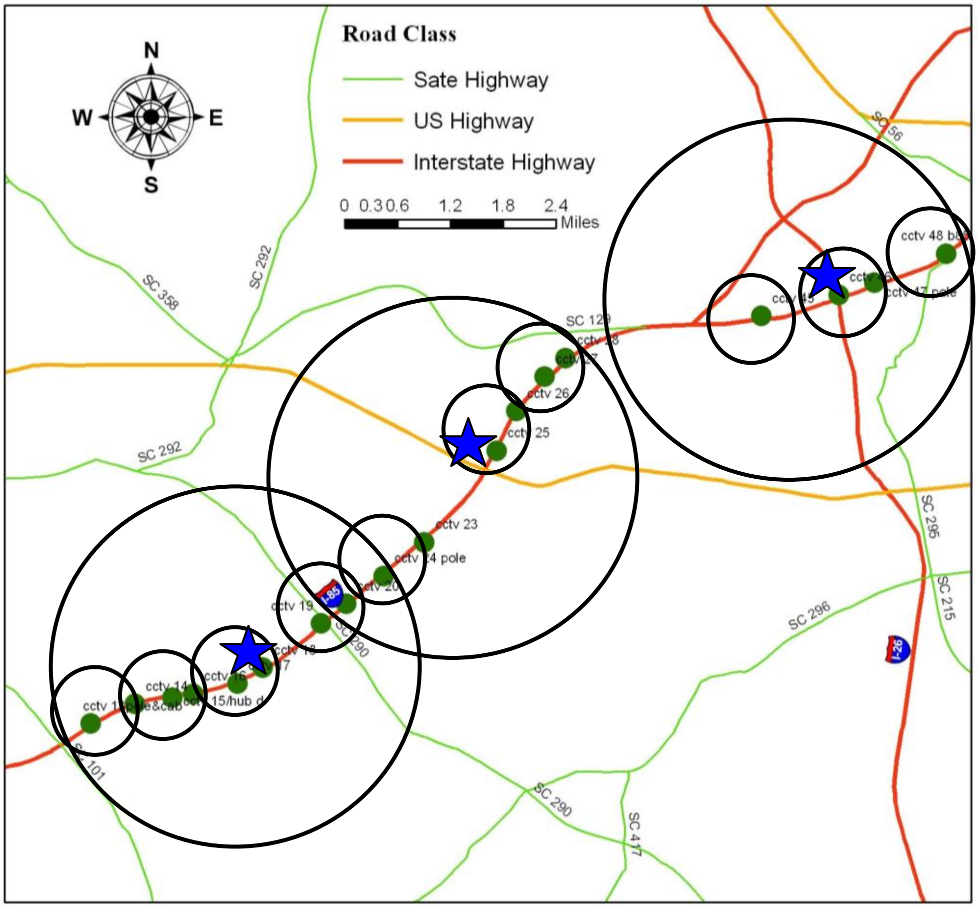


Figure C-9 WiFi Mesh Network for Spartanburg, SC

<u>WiMAX Mesh Network</u>

The WiMAX mesh model is shown in Figure C-10 below, and divides the ten clusters in the same manner as the WiFi 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.

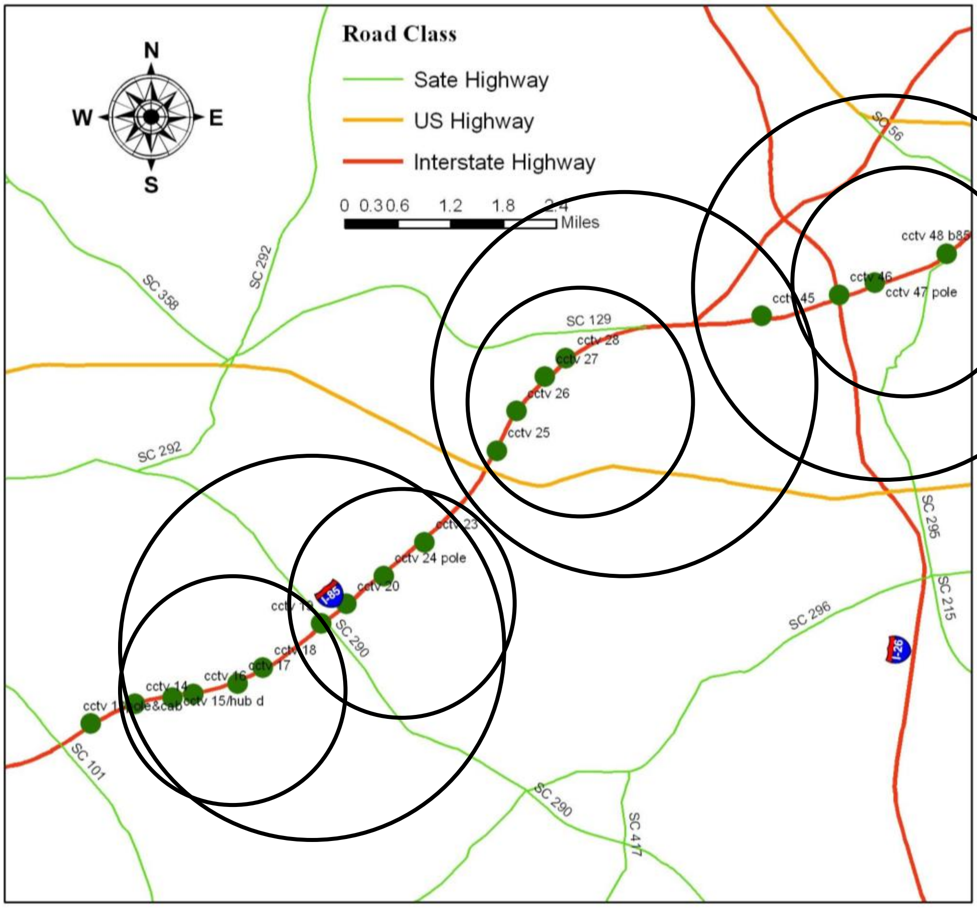


Figure C-10 WiMAX Mesh Network for Spartanburg, SC

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.

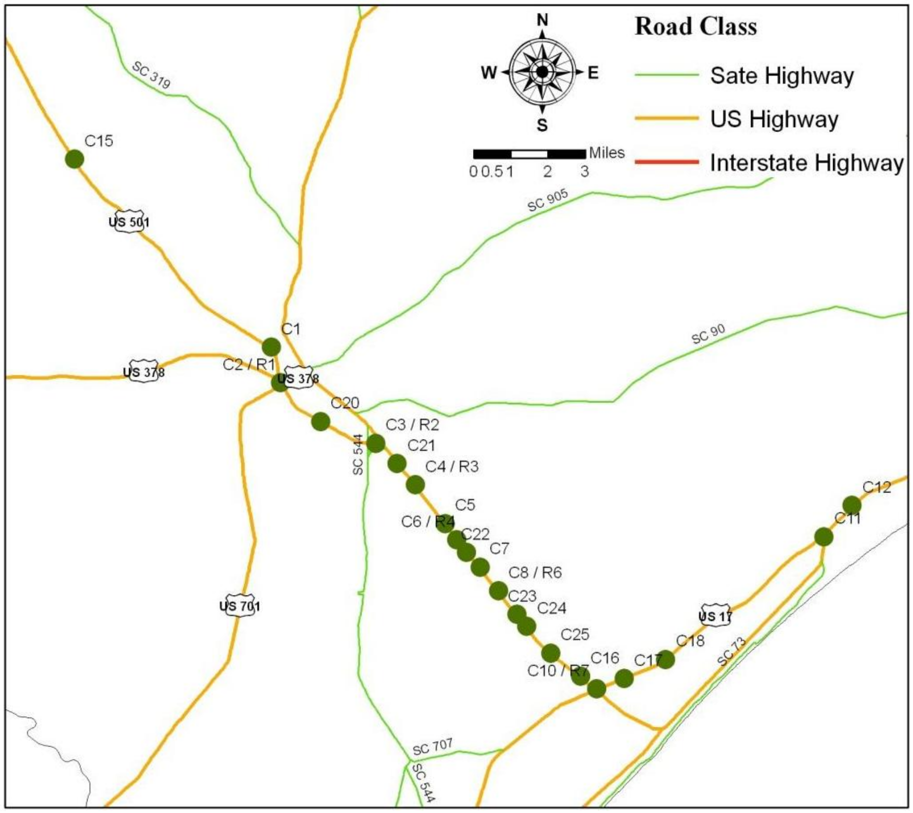


Figure C-11 Traffic Surveillance Devices in Myrtle Beach, South Carolina

<u>WiMAX Infrastructure Models</u>

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.

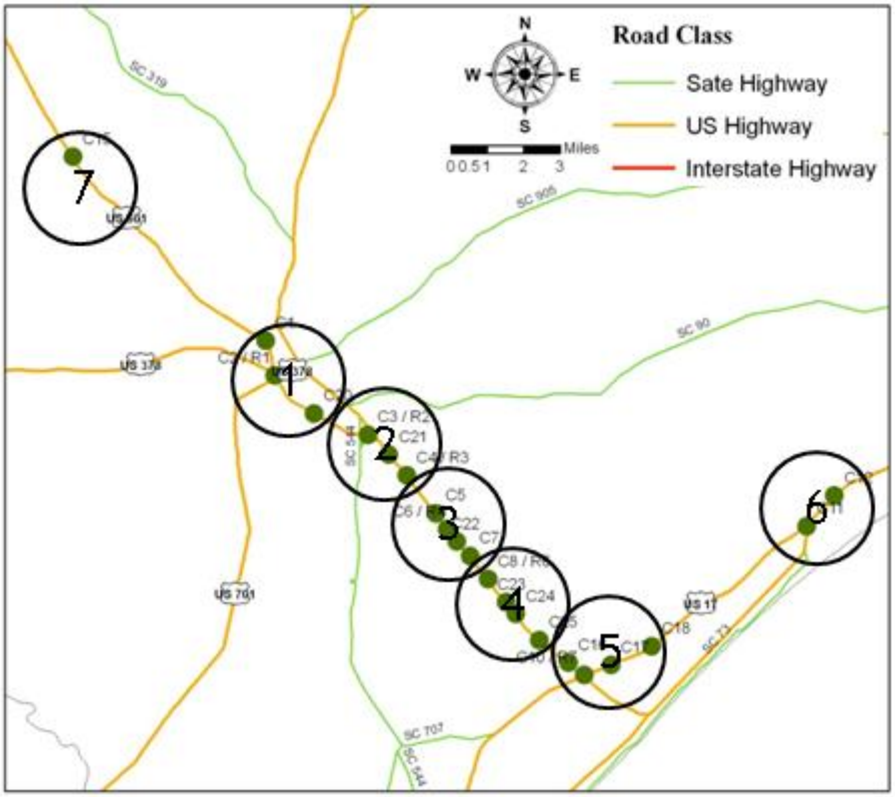


Figure C-12 WiMAX Infrastructure Model for Myrtle Beach, SC

<u>WiFi Infrastructure Network</u>

The WiFi infrastructure model is shown in Figure C-13 below, and divides the 20 nodes into twelve clusters. Each cluster would have its own fiber optic access.

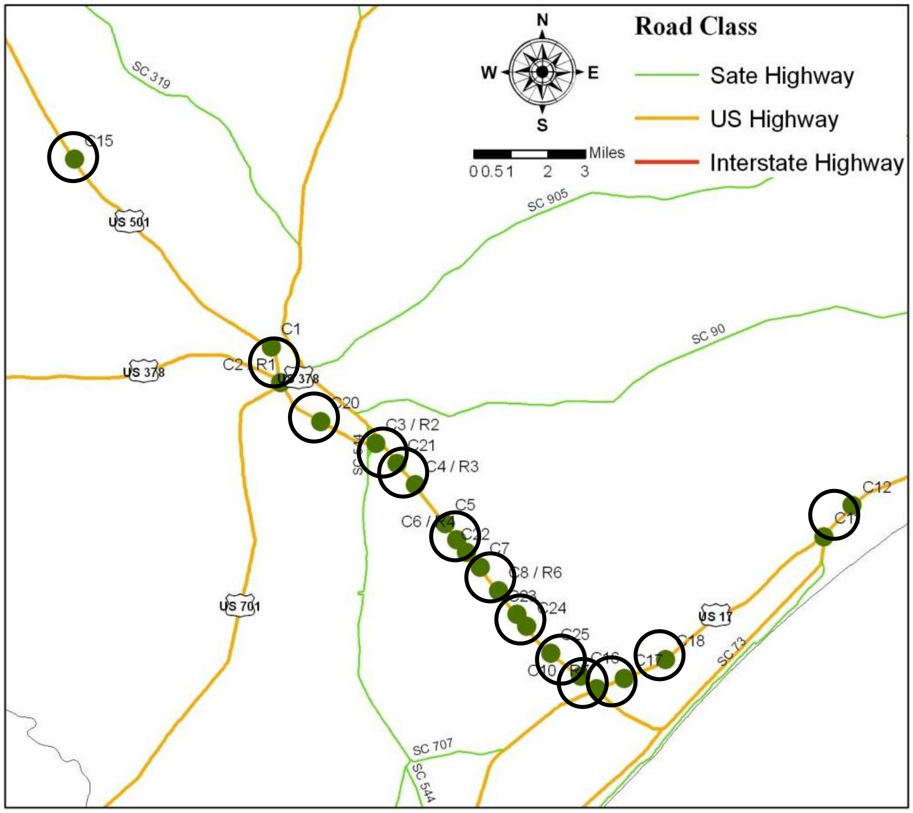


Figure C-13 WiFi Infrastructure Model for Myrtle Beach, SC

<u>WiFi Mesh Network</u>

The WiFi mesh model is shown in Figure C-14 below, and 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.

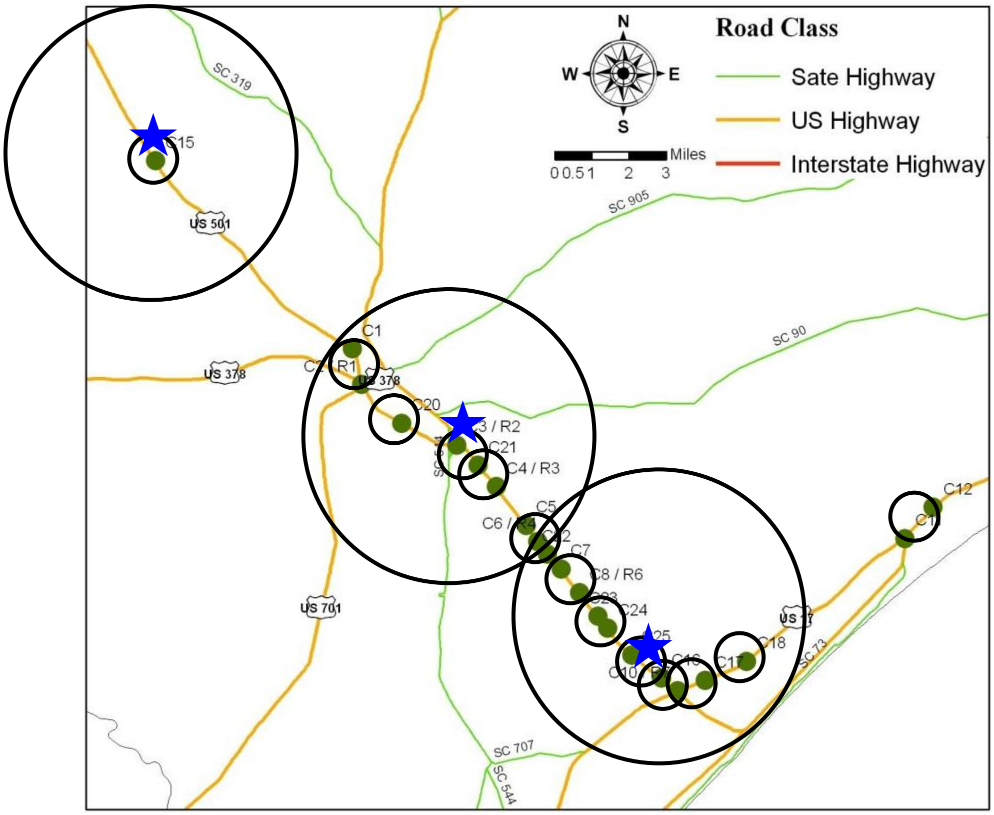


Figure C-14 WiFi Mesh Network Model for Myrtle Beach, SC

<u>WiMAX Mesh Network</u>

The WiMAX mesh model is shown in Figure C-15 below, and divides the six clusters in the same manner as the WiFi 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.

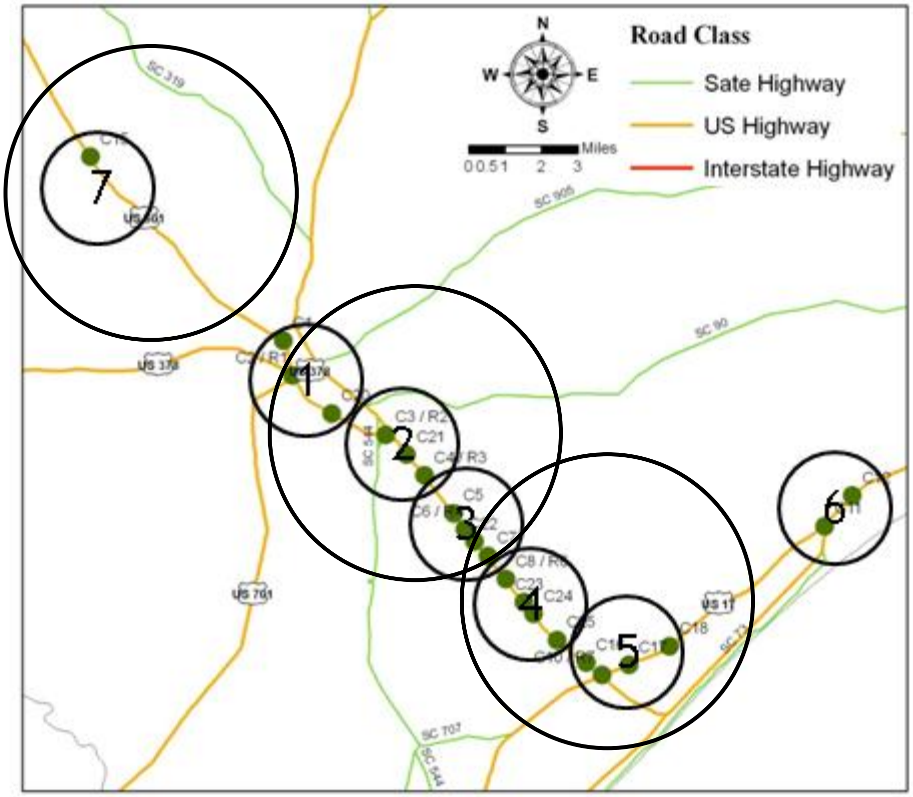


Figure C-15 WiMAX Mesh Network Model for Myrtle Beach, SC

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.

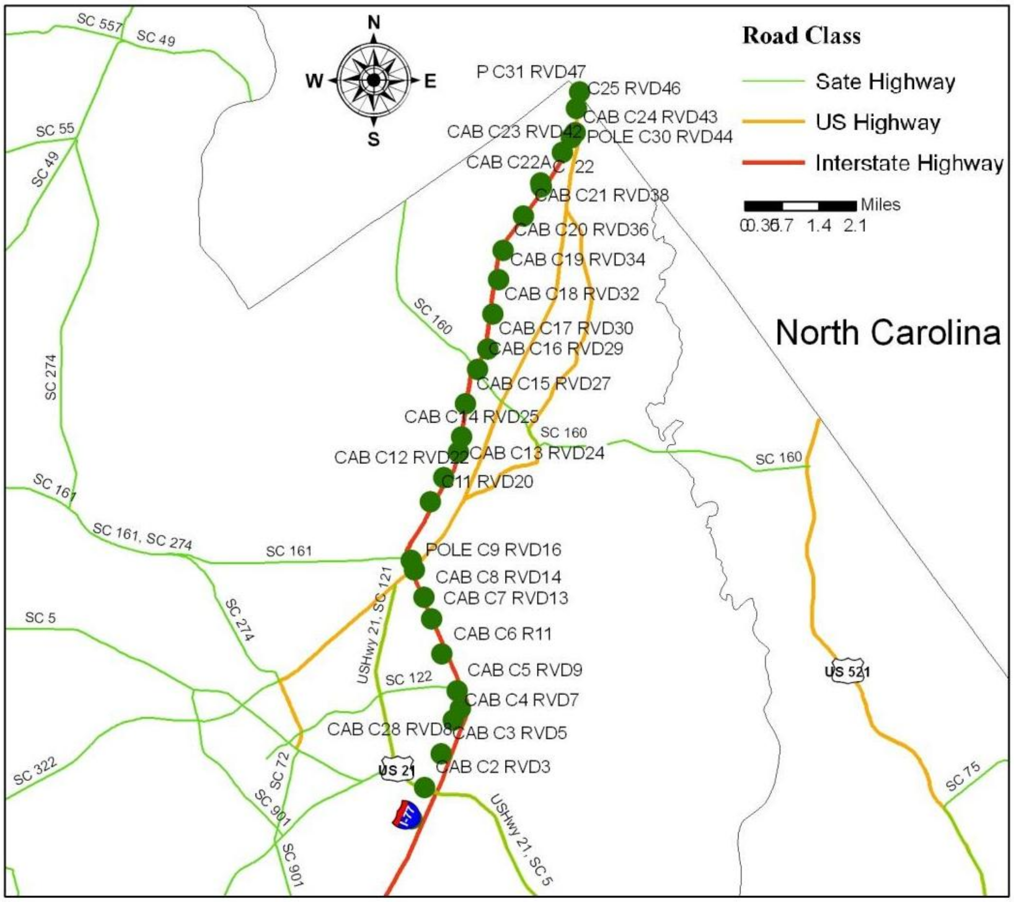


Figure C-16 Traffic Surveillance Devices in Rock Hill, SC

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.

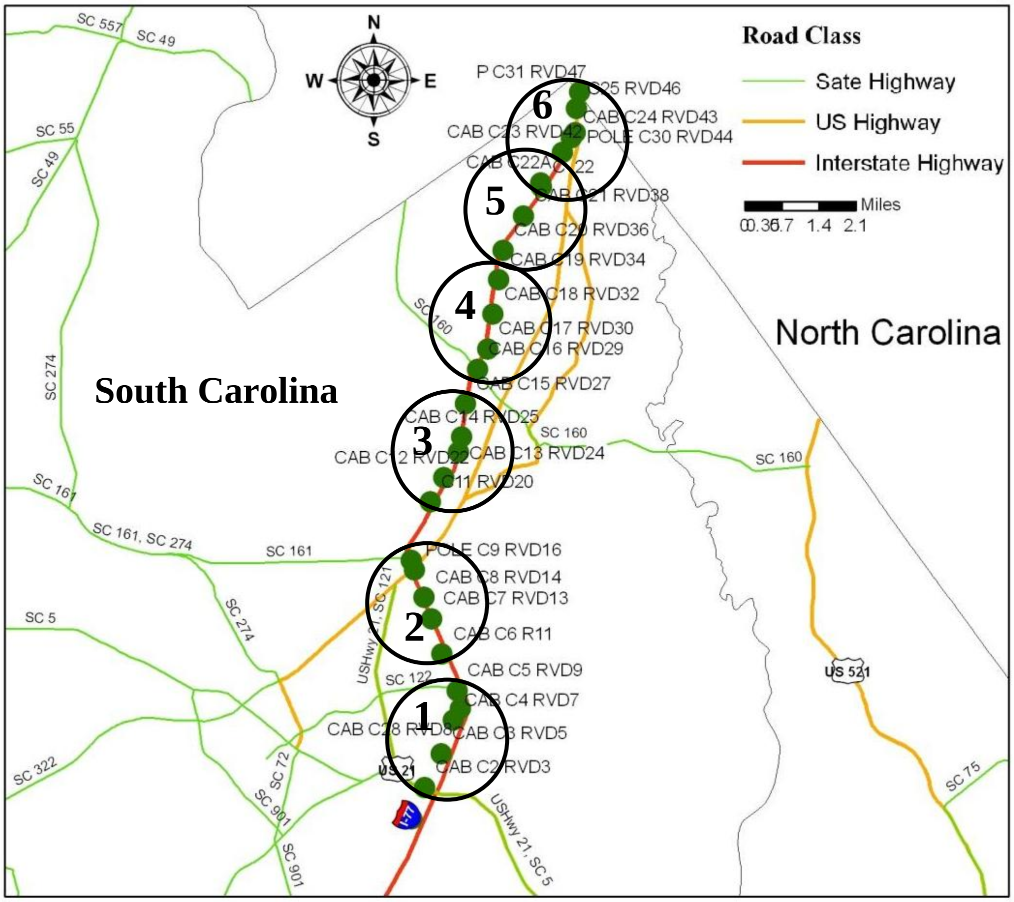


Figure C-17 WiMAX Infrastructure Network Model for Rock Hill, SC

WiFi Infrastructure Network

The WiFi infrastructure model is shown in Figure C-18 below, and divides the twenty-six nodes into twelve clusters. Each cluster would have its own fiber optic access.

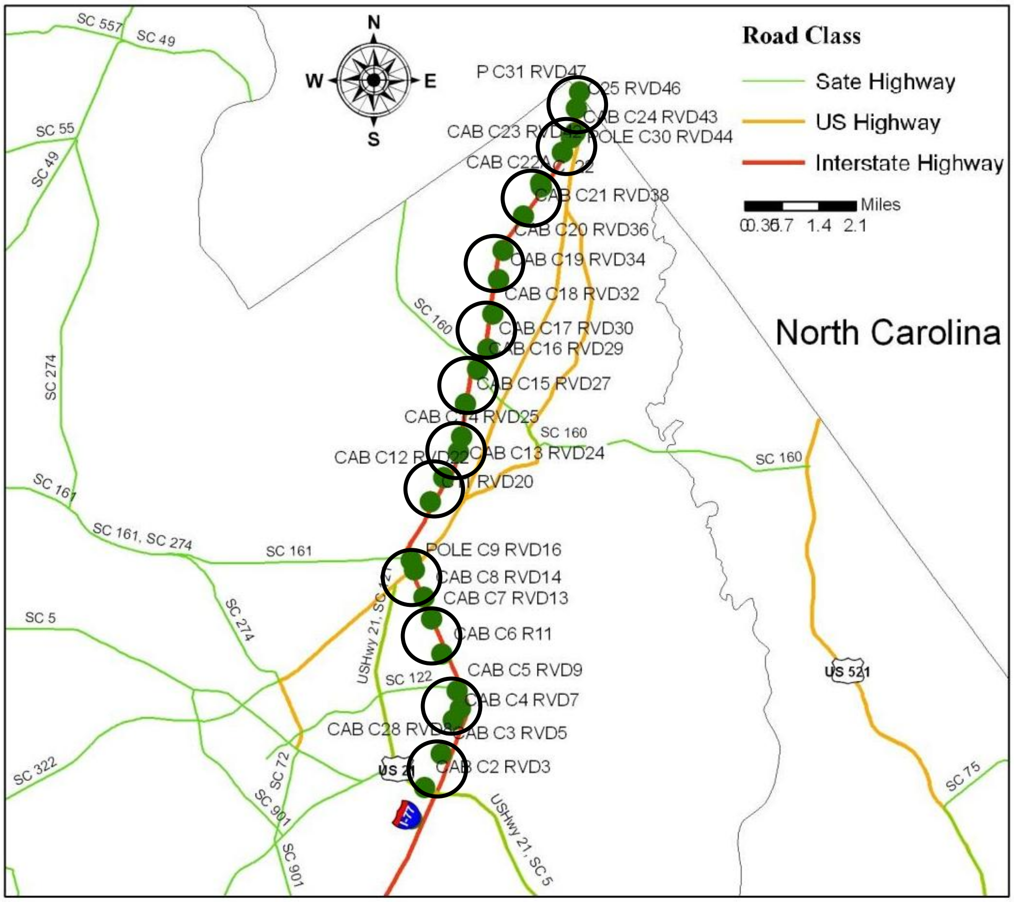


Figure C-18 WiFi Infrastructure Network Model for Rock Hill, SC

<u>WiFi Mesh Network</u>

The WiFi mesh model is shown in Figure C-19 below, and 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.

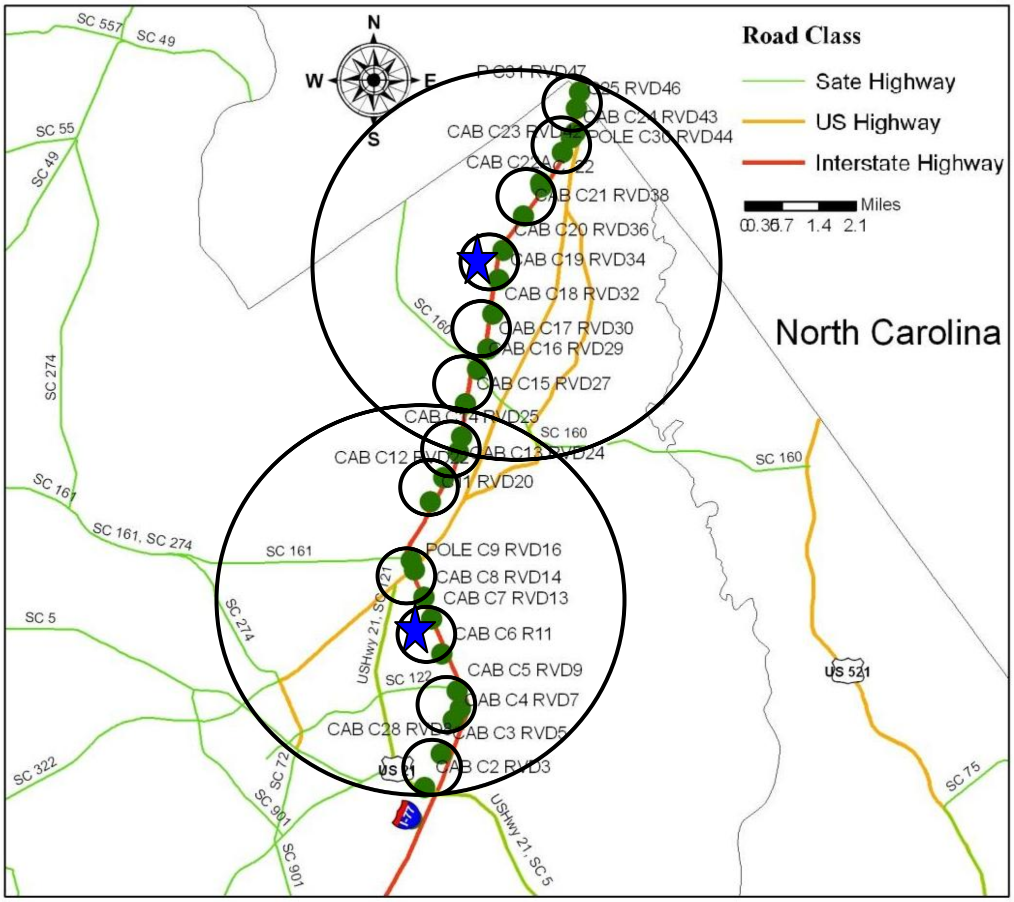


Figure C-19 WiFi Mesh Network Model for Rock Hill, SC

WiMAX Mesh Network

The WiMAX mesh model is shown in Figure C-20 below, and divides the six clusters in the same manner as the WiFi 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.

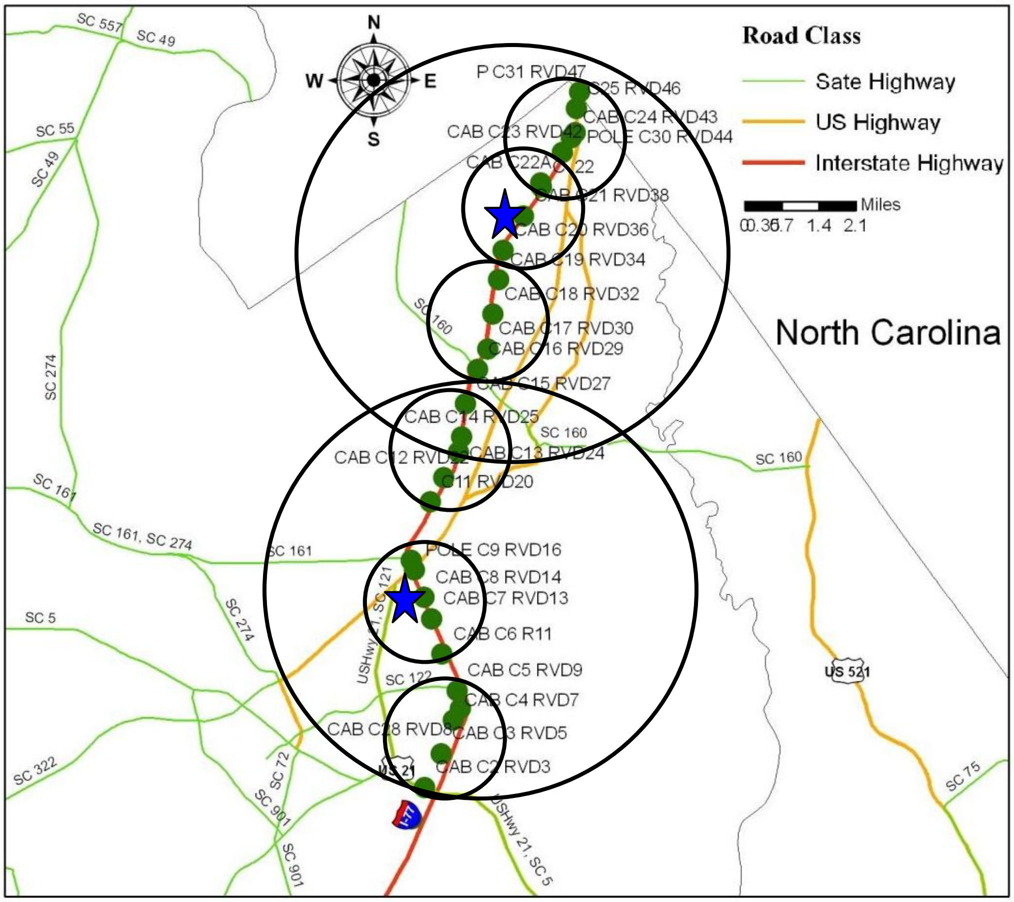


Figure C-20 WiMAX Mesh Network Model for Rock Hill, SC

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.

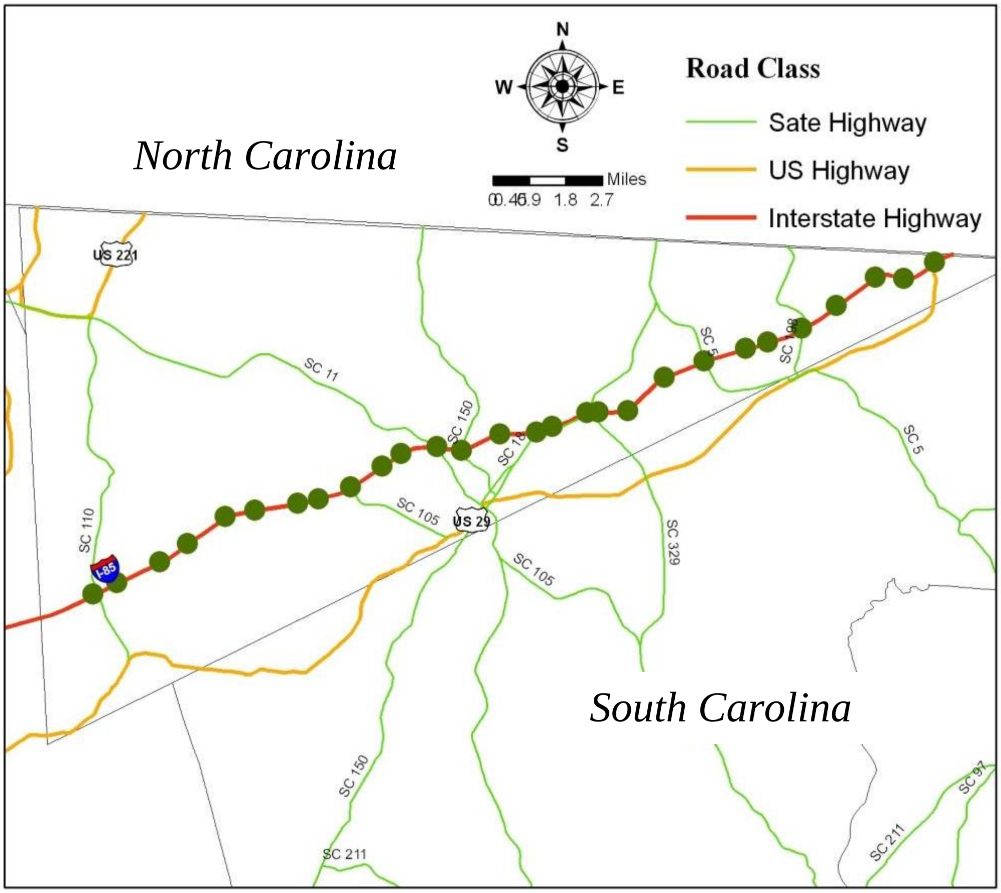


Figure C-21 Traffic Surveillance Devices in Gaffney, SC

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.

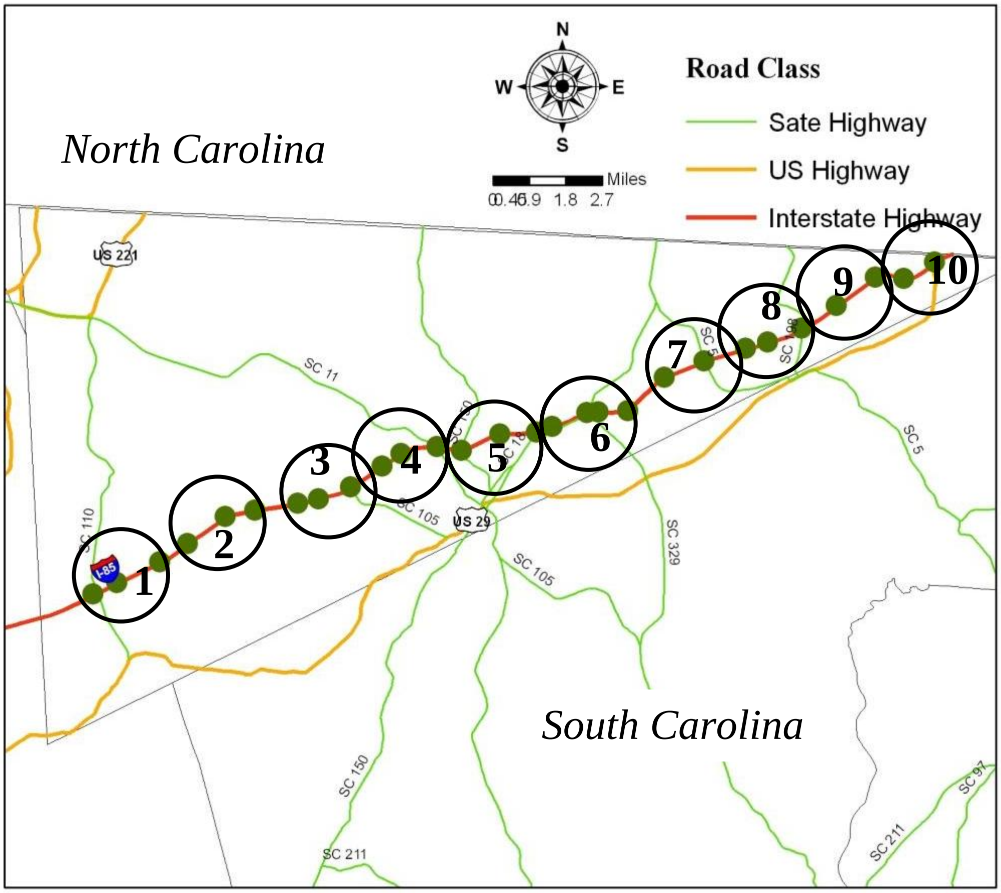


Figure C-22 WiMAX Infrastructure Model for Gaffney, SC

WiFi Infrastructure Network

The WiFi infrastructure model is shown in Figure C-23 below, and divides the 28 nodes into eighteen clusters. Each cluster would have its own fiber optic access.

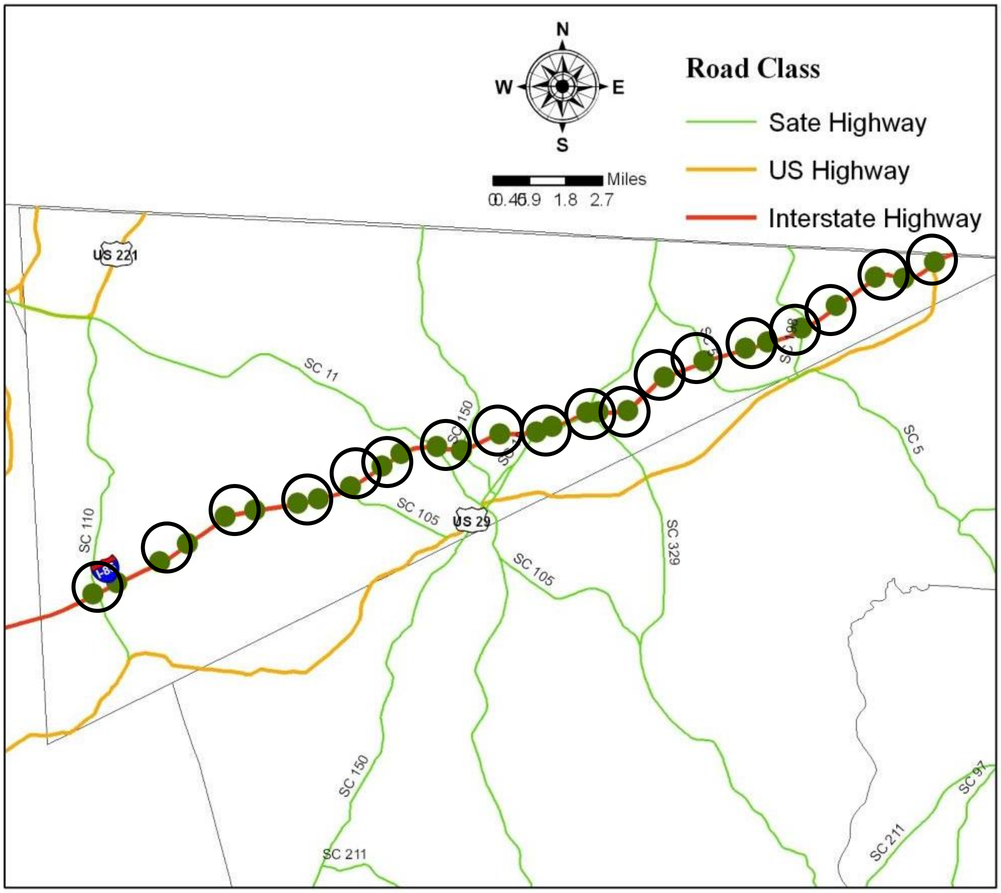


Figure C-23 WiFi Infrastructure Model for Gaffney, SC

WiFi Mesh Network

The WiFi mesh model is shown in Figure C-24 below, and 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.

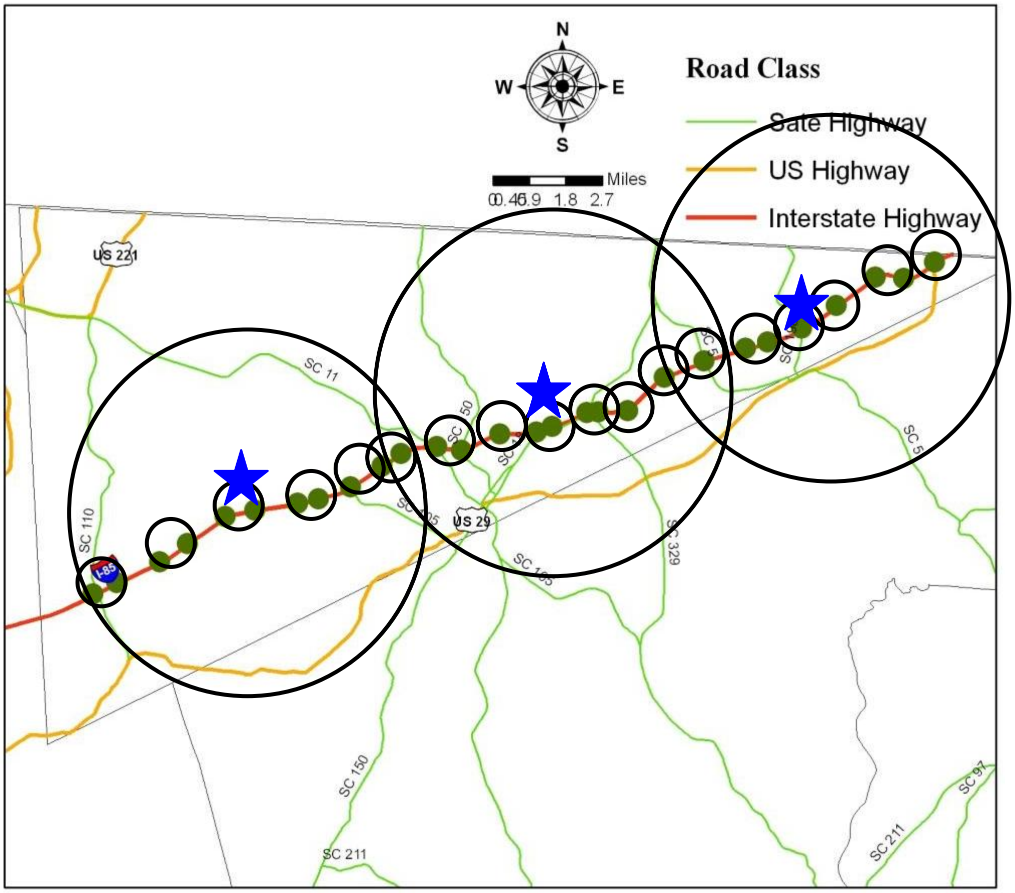


Figure C-24 WiFi Mesh Model for Gaffney, SC

<u>WiMAX Mesh Network</u>

The WiMAX mesh model is shown in Figure C-25 below, and divides the ten clusters in the same manner as the WiFi 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.

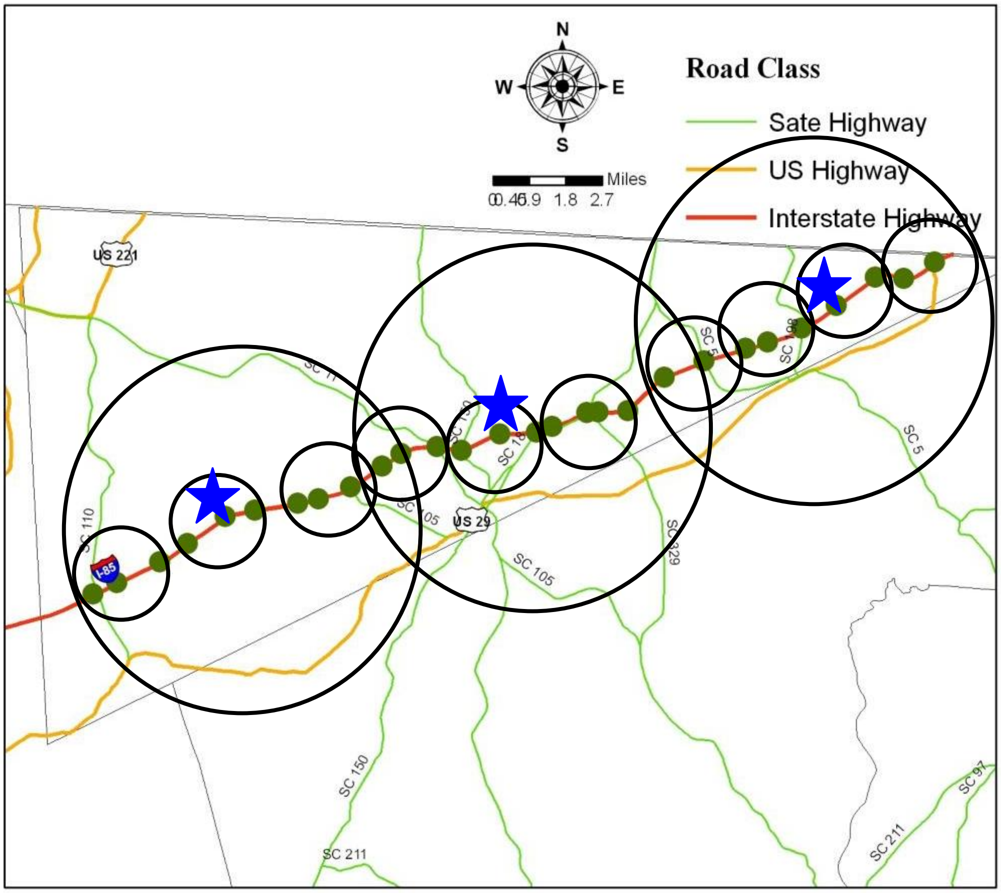


Figure C-25 WiMAX Mesh Model for Gaffney, SC

Appendix D

9 IMPLEMENTATION STRATEGY

The design, deployment and implementation of wireless communication infrastructure for ITS will require substantial planning and development. As shown in the Figure D-1, the implementation process starts with network design which includes 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.

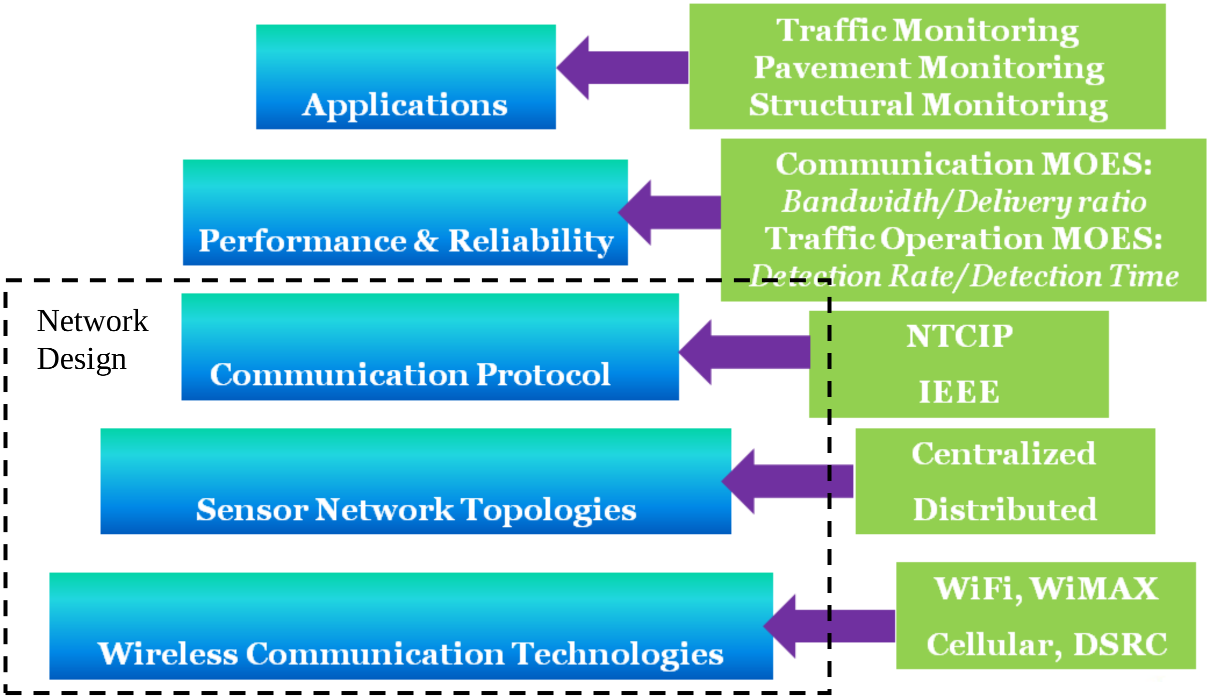


Figure D-1 High Level Implementation Process

9.1 Network Design

Planning an ITS network begins with determining the requirements that the various sensors, cameras, and other ITS components will necessitate. This part discusses technology/topology/protocol selection, network design process, and equipments selection.

9.1.1 Wireless Communication Technologies

In Table D-1, every column contains pertinent characteristics for a network important for selecting wireless options to be used in a ITS environment. For the three wireless technologies considered in this study, WiFi, WiMAX and DSRC, Table 7 in Chapter 5 summarized certain technical specifications that determine the applications it can reasonably support.

Table D-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

9.1.2 Sensor 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 D-2. Centralized network requires point-to-point connection between 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. On the other side, in the mesh network, one example of the distributed, sensors can still communicate with others even one connection failed. This topology provides more flexibility to relay traffic information especially in emergency situations, however requires more complex deployment. Detailed discussion about these two topologies can be found in Chapter 5.

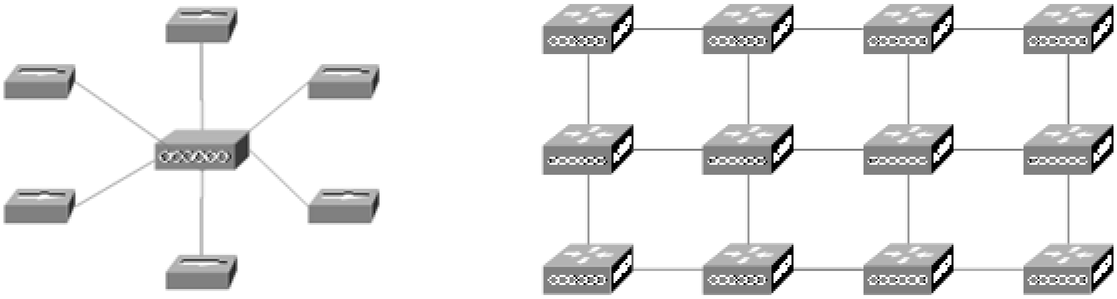


Figure D-2 Centralized and Distributed

9.1.3 Communication Protocol

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, with funding from the FHWA. 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. Detailed discussion about the TCP and UDP can be found in Chapter 6.

9.1.4 Network Design Process

After knowing the technology, topology and protocol, the design process is as shown in Figure D-3. 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, 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. If the clustering process leads to no solution, either 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 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. Examples of network design can be found in Chapter 5.

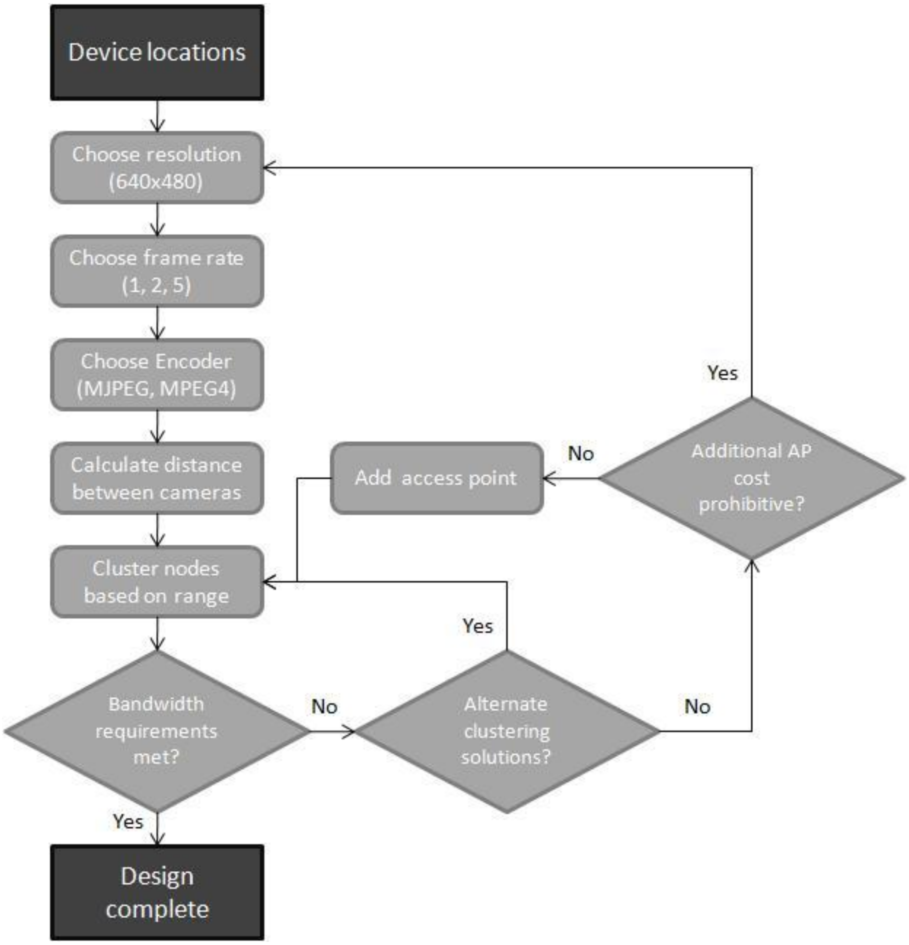

Device locations
Choose resolution (640x480)
Choose frame rate (1, 2, 5)
Choose Encoder (MJPEG, MPEG4)
Calculate distance between cameras
Cluster nodes based on range
Bandwidth requirements met?
No
Alternate clustering solutions?
Yes
No
Additional AP cost prohibitive?
No
Add access point
Yes
Yes
Design complete

Figure D-3 Flowchart for preliminary network design

9.2 Performance and Reliability

This study analyzed the performance and reliability of the communication between field devices, as well as between field devices to the TMC. The following content is divided into two parts, filed test and video surveillance test.

9.2.1 Field Test

There are many factors that can affect the communication performance and reliability in the field. The following are the key factors this study recommends traffic agencies to consider deploying the network.

Distances

The traffic sensors need to be placed within the wireless communication coverage range, which varies with technologies. If longer distance is required, communication relays are needed to relay the traffic information from one sensor to the other. However, deployment cost increase when more relays used. Moreover, field test results indicate that the more relays needed, the higher chance that data packet got lost during the transmission. In a distributed network, the performance of the network limited by the furthest sensor because it required the most number of relays to transmit the information back to local controller or a TMC. Therefore, the relay is better to be deployed at the maximum communication range to decrease the number needed. However, the field results also showed that throughput decreases when the distance between sensors (relays) increases. There is a trade-off between performance and the deployment cost.

When using different communication technologies and topologies, the communication range is different. Performance-cost analysis indicated that the WiFi infrastructure and mesh network had the same throughput-cost ratio. Considering the number of fiber drops needed, a WiFi mesh solution has highest throughput-cost ratio, while the WiMAX mesh is next higher option. Because the WiMAX mesh was found has 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 author discussed in the case study section, compared to infrastructure option, the mesh option has less expandability for future ITS devices deployment.

This study 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 located on a same pole sending information simultaneously and sharing the bandwidth, WiMAX infrastructure can provide the most bandwidth upgrade space.

Environmental Factors

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 highway terrain significant decrease the communication performance. Traffic agencies should either place the sensor closer to each other over the highway terrain peak or use the amplifier to amplify the signal.

For the highway segments that have intensive foliage coverage, amplifier also can be used to amplify the signal. Amplifier normally is installed on the sensor side. The one used in this study is a HyperAmp 2401GI-500 amplifier can increase the signal strength 500 mW (L-com 2009). For instance, if the sensor initially sends the information with 70 mW power, the total power with amplifier is 570 mW.

Technical Factors

There are two key technical factors, modulation rate and transmission power, needed to be considered when deploying a sensor network in the field. Modulation rate is the speed at which data is transmitted in a carrier, which can be achieved through different modulation scheme. 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. Moreover, 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 of the modulation rates, the drop occurs between 300 ft to 400 ft. Transmission power also limits the coverage range of the wireless communication range between two sensors. Higher power can supports longer communication range.

Moreover, there are many equipment products available to be chosen for either Wi-Fi or WiMAX network. The case study presented in Chapter one used the specifications of the Cisco product. Each product has different performance specification and cost. Traffic agencies should choose them according to their own needs and budgets wisely. WiMAX field study results indicate at the same location, the performance provided by different devices is significantly different. Detailed information can be found in Chapter 5 and 7.

Field Test Procedures

Before deploying the wireless sensor network in the field, SCDOT needs to conduct the 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. Moreover, at certain locations, the effects of the foliage coverage and highway terrain need to be quantified. Table D-2 demonstrated the field test procedure used and proposed in this study.

Table D-2 Field Test Procedure

Steps	Details
1. Select the test location	Select the locations that the sensors will be placed. Select the locations has the highway terrain characteristics and foliage coverage.
2. Determine Distance	Start with shorter distance, eg. 200 ft
3. Place sensors (routers)	Routers can be used as sensors, and better to be place at certain height above the ground. At least two router is needed, one as transmitter, the other as receiver.
4. Determine Modulation Rates	Each technology can support several rates. Start from the lower rates. Set up the rate at the transmitter side
5. Select Transmission Powers	Start from higher power Set up the power at the transmitter side
6. Identify MOEs	Communication Performance: throughput, delivery ratio, latency Traffic Operation Performance: Incident detection time Incident detection rate, false alarm rate

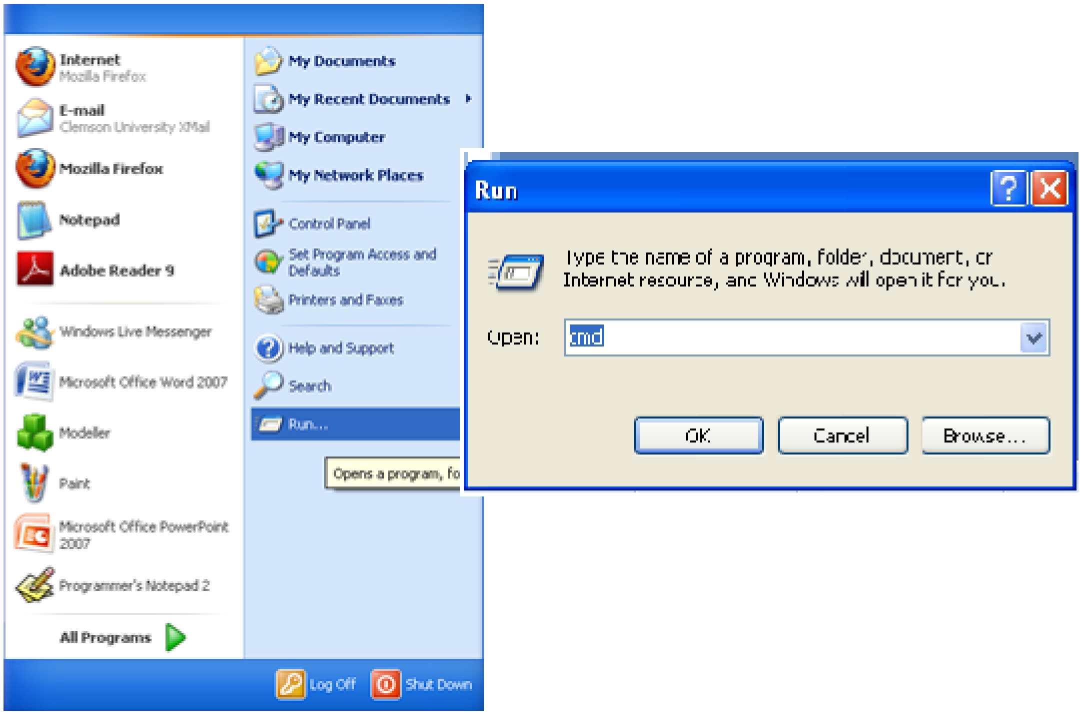
Steps	Details
7. Test the Performance	Set up the iperf server at the transmitter side Set up the iperf client at the receiver side Run iperf to start data transmission Run wireshark to record signal strength Change the distance, modulation rate or transmission power, then repeat step 1-6

The detailed process of setting up Iperf is shown as follows.

Step 1: Download iperf.exe file from http://www.noc.ucf.edu/Tools/Iperf/

Step 2: Install iperf on both receiver and transmitter, save the iperf fold under the C drive.

Step 3: Click "Start- Run", and type "cmd" in the pop-up window, and then click 'OK', as shown in Figure D-4.

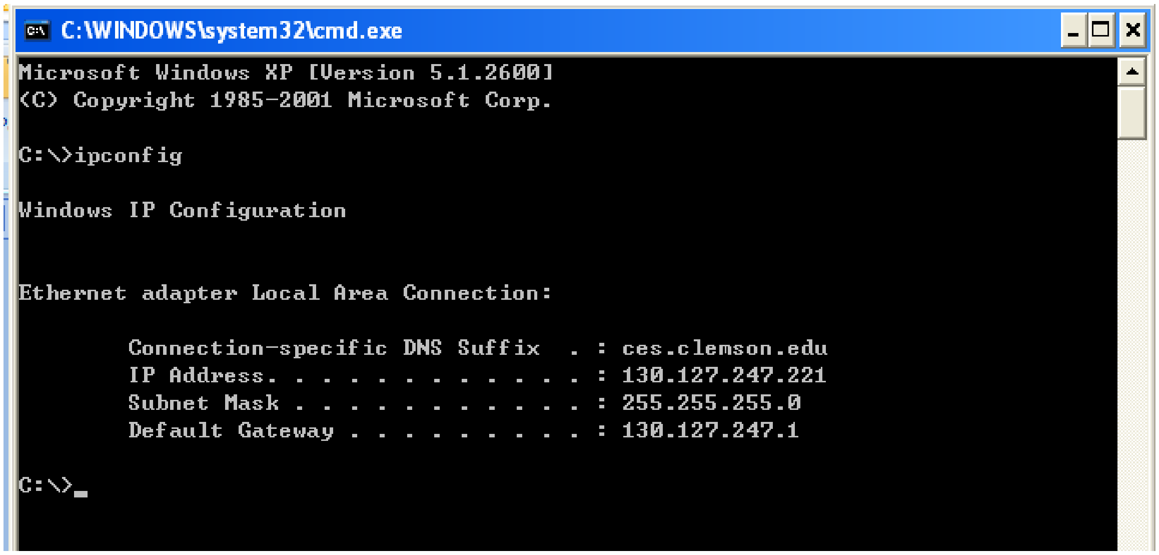


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

Figure D-4 Step 3

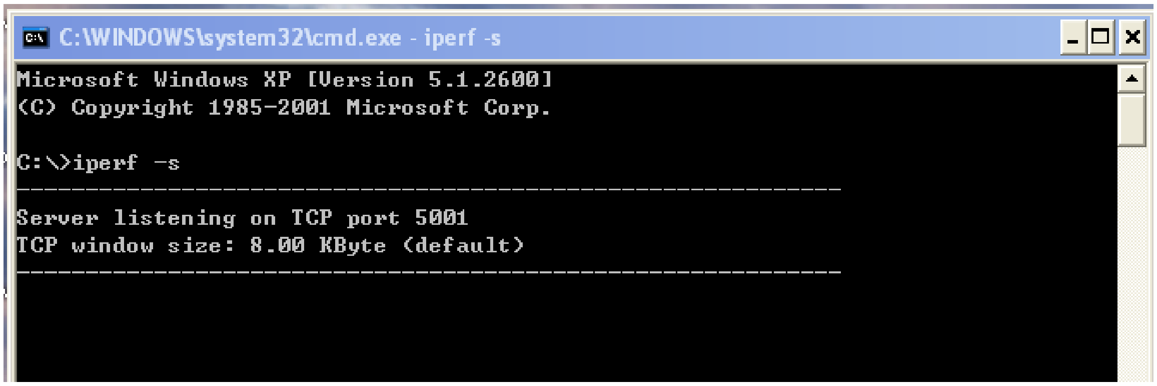
Step 4: Get the ip address on the server side: Type “ipconfig” and then click “enter”, shown in Figure D-5



```
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 D-5: Get the Ip Address of the Server

Step 5: Set-up server: type “iperf –s” and then click “enter”, shown in Figure D-6. 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 D-6: Set Up the Server

Step 5: Set-up the client: type “iperf –c 130. 127.247.221 and then click “enter”. Then the server and client are connected.

Step 6: If want to test UDP protocol, type “iperf –u –s” on the server side.

If want to test different bandwidth, type “iperf -c 130.127.247.221 –b 2m” to. This example sets up a bandwidth 2Mbps connection.

If want to set up the test duration, type “iperf –c 130.127.247.221 –b 2m –t 60”. This example sets up the one test duration as 60 seconds.

9.2.2 From Field to TMC

When connecting the field devices with TMC wirelessly, there are certain factors need to be considered as well, such as distance, foliage coverage, highway terrain. Detailed impacts of these factors can be found in section 2.1 to 2.4. 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 two factors needed to be considered to ensure the performance of real-time video surveillance, 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 value greater than 1 second likely delay the video transmission so human eyes can observes 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 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 devices, such as several office receiving video from the same traffic camera simultaneously, the performance could be significantly decreased compared to one user. Some time, one user can receive smooth video but the others may suffer slow-down or disconnection. Pre-evaluation test is needed to identify the number of users the system can support.

9.3 Applications

Wireless sensor network has wide application range, not only in the transportation field, but also in other areas. Besides of traffic management and operation, it can also be used in transportation infrastructure monitoring, structural health monitoring, pavement monitoring, etc. Agencies can collaborate with each other and share the same wireless network for different needs.

Normally, SCDOT starts a project from the application requirements, which is the top of the process as shown in Figure D-1. For instance, SCDOT wants to deploy wireless traffic network surveillance. National ITS architecture provides a market package ATM s01 which defined the communication and data flow needed between various subsystems and terminators. Based on the data flow requirements, SCDOT starts the network design process, and then evaluate the performance and reliability to satisfy the needs. Then, the implementation plan is from bottom-up, which was previously elaborated in this section.

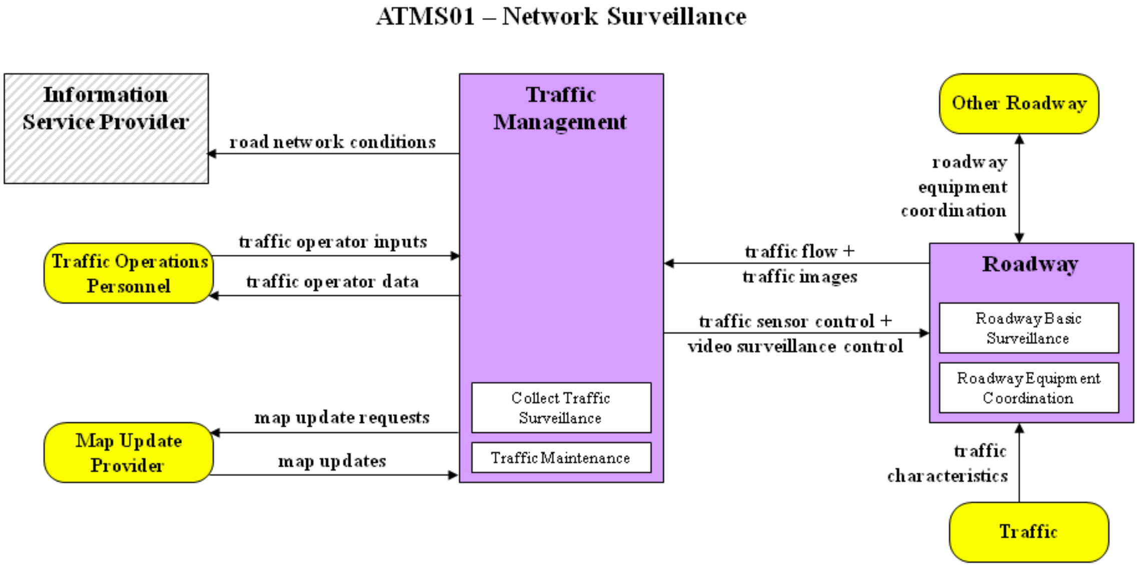

ATMS01 – Network Surveillance
Information Service Provider
road network conditions
Traffic Management
Other Roadway
roadway equipment coordination
Traffic Operations Personnel
traffic operator inputs
traffic operator data
traffic flow + traffic images
Roadway
traffic sensor control + video surveillance control
Roadway Basic Surveillance
Roadway Equipment Coordination
Collect Traffic Surveillance
Traffic Maintenance
Map Update Provider
map update requests
map updates
traffic characteristics
Traffic

Figure D-7 Network Surveillance Market Package (ITS Architecture 2009)

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 Systems1. (2009) <http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5279/ps5285/product_data_sheet09186a008018495c.html>

Cisco Systems2. (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 Section 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. dissertation, 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 WiFi: 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.

Zhou1, 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.

Zhou2, 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.

Zhou3, 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, No.2129, 2009, pp.121-128.

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.