8-3-2012 12:00 AM

Investigation of Wireless LAN for IEC 61850 based Smart Distribution Substations

Palak P. Parikh
The University of Western Ontario

Supervisor
Dr. Tarlochan S. Sidhu
The University of Western Ontario

Graduate Program in Electrical and Computer Engineering
A thesis submitted in partial fulfillment of the requirements for the degree in Doctor of Philosophy

Recommended Citation

Parikh, Palak P., "Investigation of Wireless LAN for IEC 61850 based Smart Distribution Substations" (2012). *Electronic Thesis and Dissertation Repository*. 869.
https://ir.lib.uwo.ca/etd/869

Investigation of Wireless LAN for IEC 61850 based Smart Distribution Substations

(Spine title: Investigating WLAN for IEC 61850 based Distribution Substation)

(Thesis Format: monograph)

by

Palak Parikh

Graduate Program in Engineering Science
Department of Electrical and Computer engineering

A thesis submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy

School of Graduate and Postdoctoral Studies
The University of Western Ontario
London, Ontario, Canada

THE UNIVERSITY OF WESTERN ONTARIO
SCHOOL OF GRADUATE AND POSTDOCTORAL STUDIES

CERTIFICATE OF EXAMINATION

Supervisor	Examiners
Dr. Tarlochan S. Sidhu	Dr. Jin Jiang
Co-Supervisor	
Dr. Abdullah Shami	Dr. Robert Sobot
	Dr. Madhumita Ray
	Dr. Kankar Bhattacharya

The thesis by

Palak Parikh

entitled:

Investigation of Wireless LAN for IEC 61850 based Smart Distribution Substations

is accepted in partial fulfilment of the
requirements for the degree of
Doctor of Philosophy

Date

Chair of the Thesis Examination Board

Abstract

The IEC 61850 standard is receiving acceptance worldwide to deploy Ethernet Local Area Networks (LANs) for electrical substations in a smart grid environment. With the recent growth in wireless communication technologies, wireless Ethernet or Wireless LAN (WLAN), standardized in IEEE 802.11, is gaining interest in the power industry for substation automation applications, especially at the distribution level. Low Voltage (LV) / Medium Voltage (MV) distribution substations have comparatively low time-critical performance requirements. At the same time, expensive but high data-rate fiber-based Ethernet networks may not be a feasible solution for the MV/LV distribution network. Extensive work is carried out to assess wireless LAN technologies for various IEC 61850 based smart distribution substation applications: control and monitoring; automation and metering; and over-current protection.

First, the investigation of wireless LANs for various smart distribution substation applications was initiated with radio noise-level measurements in total five (27.6 and 13.8 kV) substations owned by London Hydro and Hydro One in London, ON, Canada. The measured noise level from a spectrum analyzer was modeled using the Probability Distribution Function (PDF) tool in MATLAB, and parameters for these models in the 2.4 GHz band and 5.8 GHz band were obtained. Further, this measured noise models were used to simulate substation environment in OPNET (the industry-trusted communication networking simulation) tool. In addition, the efforts for developing dynamic models of WLAN-enabled IEC 61850 devices were initiated using Proto-C programming in OPNET tool. The IEC 61850 based devices, such as Protection and Control (P&C) Intelligent Electronic Devices (IEDs) and Merging Unit (MU) were developed based on the OSI-7 layer stack proposed in IEC 61850. The performance of various smart distribution substation applications was assessed in terms of average and maximum message transfer delays and throughput.

The work was extended by developing hardware prototypes of WLAN enabled IEC 61850 devices in the R&D laboratory at University of Western Ontario, Canada. P&C IED, MU, Processing IED, and Echo IED were developed using industrial embedded computers over the QNX Real Time Operating System (RTOS) platform. The functions were developed using hard real-time multithreads, timers, and so on to communicate IEC 61850 application messages for analyzing WLAN performance in terms of Round Trip Time (RTT) and throughput. The laboratory was set up with WLAN-enabled IEC 61850 devices, a commercially available WLAN Access Point (AP), noise sources, and spectrum and network analyzers. Performance of various smart distribution substation applications is examined within the developed laboratory.

Finally, the performance evaluation was carried out in real-world field testing at 13.8 and 27.6 kV distribution substations, by installing the devices in substation control room and switchyard. The RTT of IEC 61850 based messages and operating time of the overcurrent protection using WLAN based communication network were evaluated in the harsh environment of actual distribution substations. The important findings from the exhaustive investigation were discussed throughout this work.

Dedication

I dedicate this work to my parents and my husband.

Acknowledgment

It is with great pleasure and felicity that I would like to express thanks to all the people who have made this thesis possible.

I will always remain grateful to my Supervisor Dr. Tarlochan Sidhu, for his encouragement, and support from the initial to the final level of this work. Then, I am very much thankful to my co-supervisor Dr. Abdullah Shami, for his guidance and valuable feedback for making this work successful. Their continuous supports have helped me in successfully completing my doctoral degree.

I would like to thanks all my friends and colleagues of GE innovation Lab, for providing friendly and encouraging work atmosphere.

I wish to express my gratitude to Mr. Dan Mittelholtz, from Hydro one and Mr. Cole Tavener, from London Hydro, for their support and help during noise measurement experiments. I am thankful for the help provided by OPNET and QNX technical support team.

My life would not have been the same without my parents, sister and extended family that have remained close to me even if we were thousands of miles away. I am forever indebted to them for their love and absolute confidence in me. Finally, very special thanks to my husband, who gave me unconditional support and love through all this long process.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AP	Access Point
APDU	Application Protocol Data Unit
ASDU	Application Service Data Unit
BER	Bit Error Rate
BSS	Basic Service Set
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CT	Current Transformer
DAS	Distribution Automation System
DERs	Distributed Energy Resources
DGs	Distribution Generation
EPRI	Electrical Power Research Institute
EMI	Electro-Magnetic Interferences
GOOSE	Generic Object Oriented Substation Event
GSSE	Generic Substation Status Event
HMI	Human Machine Interface
IEC	International Electro technical Commission
IED	Intelligent Electronic Device
IEEE	The Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
MAC	Medium Access Control
MATLAB	MATrix LABoratory
MMS	Manufacturing Message Specification
MU	Merging Unit
NSIT	National Institute of Science and Technology
OSI	Open Systems Interconnection
P&C	Protection and Control
PSCAD	Power system Computer Aided Design
PSRC	Power System Relaying Committee
QoS	Quality of Service
RFI	Radio Frequency Interferences
RTP	Real Time Playback
RTT	Round Trip Time
SAS	Substation Automation System
SCL	Substation Configuration Language
SIR	Source Impedance Ratios
SNR	Signal to Noise Ratio
SV	Sampled Values
TC	Technical Committee
TCI	Tag Control Identifier
TCP	Transmission Control Protocol
TPID	Tag Protocol Identifier
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Network

Chapter 1

1. Introduction

1.1 IEC 61850 Based Smart Distribution Substations

First of all, this chapter provides background of distribution substations, and IEC 61850 standard suite, and communication technologies for distribution substation applications. Also, the comparison of requirements and aspects between: 1) distribution and transmission substations; 2) wireless and wired communication networks; 3) industrial wireless LAN and residential wireless LAN. Further, the comprehensive literature survey is presented for wireless applications in power substations, and possible implementation issues with wireless LAN while applying to power distribution substation. Finally, the motivation behind this research work and detail research methodology is discussed.

1.1.1 **Distribution Substation**

Power distribution system is an important part of electrical power systems in delivery of electricity to consumers. Development of Distribution systems poses new challenges in the changing world, where levels of electrification need to be increased and electricity served reliably for sustainable economic and social development. Technological development and adequate regulations are required at the distribution level to respond to new energy challenges and the restructured environment [2].

Table 1-1: Comparison table of distribution and transmission system [3]

Characteristics	Distribution	Transmission
Topology	Radial	Network or Loop
Power	100 MVA and Below	Bulk (100-20,000 MVA)

Voltage	< 69 kV	> 120 kV class
Components	About 100 times in transmission	10 to 100 times less than in distribution
Capital Outlay	40%	20%
Load	Distributed	Concentrated (end points)
Unbalance	< 5% - 30%	< 5%
No. of Phases	Both 1 & 3 (2 have been used)	3 or more, or HVDC

Major challenges:

1. Efficiency: Energy losses on distribution network are relatively high, and affect efficiency tremendously. When some large scale DERs are to be integrated into grid, their locations may far from main system. Therefore, the energy losses on distribution line will be considerable if using traditional design and construction approaches.
2. Reliable power supply: The current power grid is largely based on technology created and developed more than a century ago. Current grid is no longer suited to the requirements of an information driven and security conscious society. As a result, the grid is more and more vulnerable to some natural disasters, accidents, and security threat.
3. Major changes are happening in power distribution systems by introduction of Distributed Energy Resources (DERs) [4]. These energy resources include Distributed Generation (DGs) both conventional (e.g. diesel generators) and renewable generators (e.g. wind generators, solar power generation), electrical storage, and Plug-in Hybrid Electric Vehicles (PHEVs). The conventional protection schemes for traditional distribution systems cannot be used in presence of DERs without modifications or upgrades. Present-day distribution systems have been mostly designed to operate in a radial fashion which can only deliver power from main distribution substations to loads. They have not been designed to handle generation resources scattered along the loads.
4. In any condition, distribution network voltage profile should be within the allowable range. There are several voltage/VAR control devices available commercially and installed widely in the distribution network. There is a need for

the optimal control of these devices to enhance the performance of voltage control devices. This can be achieved with the help of smart grid communication network to coordinate these voltage/VAR control devises.

5. Microgrid is costumer ends of future power systems that bring together loads and sources i.e. DERs operating as a single system. A microgrid is well suited for integrating renewable sources with the grid as well as being utilized to increase system reliability. In addition to this, there are challenges related to voltage control over the distribution network, as the amount of generation/consumption and location (e.g. PHEVs) of these DERs would continuously vary.

   The impact of all this challenges can be reduced with the use of proper and detail data exchange between distribution network substation and DERs and micro gird. The wireless communication network in distribution can be more promising solution for the data exchange in distribution network.

1.1.2 IEC 61850-Global Standard for Substation Automation and Protection

The electric power system becomes more complex, and hence efficient and reliable operation of that is more and more critical and important. This led to a drive for increased automation of the transmission and distribution substation. Automation in the distribution field allows utilities to implement flexible control of distribution systems, which can be used to enhance efficiency, reliability, and quality of electric service. Seamless information exchange among the substation protection and automation devices is the key for achieving the smart grid vision. Various communication technologies are explored to achieve the smart grid [1]. Smart distribution substation automation and protection can play an important role to realize the vision of future smart grid [2]-[5]. Currently, interoperability among the multi-vendor substation devices is one of the major concerns in substation automation communication [6].

Presently, worldwide research and development efforts are focused in the areas of communication technologies revolution and application of IEC 61850 protocol in the distribution automation to make distribution automation more intelligent, efficient and cost effective [3], [5]. The technical committee TC 57 of International Electro-technical Commission has published IEC 61850 global standard on "Communication Networks and Systems in Substation" in 2003 [7]. IEC 61850 standard has proposed Ethernet based communication networks to interconnect substation automation devices supplied by different manufactures within the substation in order to achieve interoperable Substation Automation Systems (SAS) [8]. IEC 61850, with the objective to solve the interoperation problem, now becomes the global communication standard for substation automation. It solves the interoperation problem by defining the protocol, data format and the language. National Institute of Standards and Technology (NIST) has recognized IEC 61850 standard for substation automation and protection applications to achieve the interoperability for the future smart grid [9], [10]. New concepts and solutions for distribution substation using IEC 61850 standard are discussed in references [11], [12].

1.1.3 Comparing Requirements and Aspects of Transmission and Distribution Substations

There is a significant difference in aspects and requirements of transmission and distribution substation. Table 1-2 compares various requirements and aspects for typical transmission and distribution substations. The data rate requirement of a distribution substation is quite less than a typical transmission substation due to multiple reasons, e.g. number of equipment in transmission is large, amount of data required for protection, control and monitoring applications is higher, etc. At the same time, distribution substation has lower time delay requirements compare to transmission, due to the fact that distribution level has low power level compare to transmission e.g. IEC 61850 has specified communication delay of the most time critical applications to be 10 ms for distribution substation, whereas, 3-4 ms for transmission substation [7]. The allowable cost of communication infrastructure installation is lower for distribution substation applications comparatively. Other aspects, such as area coverage required for a typical communication technology is approx. 25 to 150 meter for a typical distribution substation; whereas, 50-300 meter for a typical transmission substation. Some of the remote distribution substation may be unmanned, and there is no means of physical security available at the site to protect the communication infrastructure.

Table 1-2: Comparing aspects and requirements of transmission and distribution substation

Requirements Aspects	Transmission substation	Distribution substation
Data rate requirements	Higher	Lower
Communication delay requirements	Higher	Lower
Allowable cost of communication infrastructure	Higher	Lower
Coverage	Approx. 50 – 300 meter	Approx. 25-100 meter
Availability of man power presence	Yes	May not be

1.2 Significance of Selecting Wireless LAN (WLAN) Technology for Distribution Substation Applications

This section presents comparison of wireless and wired technologies, and discusses reason for potential use of wireless technologies in distribution substation. Moreover, the significance of selecting wireless LAN among other wireless technologies is also described below.

1.2.1 Comparison of Wired and Wireless Technologies

Potential use of wireless technologies and their benefits over wired technologies is described with applications in references [13]-[16].

1.2.1.1 Benefits of Wired Technologies

1. Higher data rates and bandwidth, up to 1-10 Gbps
2. Lower communication delay
3. More secured comparatively

1.2.1.2 Limitation of Wired Technologies

1. There is possibility of cutting or breaking of wire. In case of the underground wire or cable finding and repairing the break can be difficult, dangerous and time consuming.
2. Loose connection of wire leads to noisy or intermittent communication.
3. Possibilities of eavesdropping on metallic wires.
4. It is difficult to modified, upgrade or change the wired network due to its immobility feature.
5. Metallic wires are susceptible to ground potential rise in substations.

1.2.1.3 Benefits of Wireless Technology

1. Less expensive as compared to wired communication systems to deploy because no complex and expensive cables need to be designed for or installed.
2. Easy to install, because of wireless feature.
3. More portable, hence the equipment can easily be moved from one spot to another, either continuously or periodically.
4. Wireless equipment can automatically connect into an existing wireless network with only the appropriate security features enabled.
5. Less susceptible to ground potential rise because no cabling is needed.

1.2.1.4 Limitations of Wireless Technology

1. Impact of surrounding EMI/RFI
2. Lower data rates comparatively (54 – 160 Mbps)
3. Channels reliability/availability
4. Cyber security due to open air medium

1.2.2 **Comparison of Wireless LAN with Other Wireless Technologies**

The IEC 61850 standard proposes Ethernet based communication networks to integrate substation automation devices supplied by different manufactures within a substation. The wired Ethernet technologies are standardized in IEEE 802.3 series of standards;

whereas, wireless Ethernet (LAN) technologies are standardized in IEEE 802.11 series of standards [17]. Recent studies have shown the suitability of wireless LAN technologies for industrial environment, and demonstrated advantages to employ wireless LAN as an extension of industrial Ethernet for various industrial applications [18]. The comparison of wireless LAN with other wireless technology in terms of data rate, cost, complexity and power consumption with other technologies is shown in Figure 1-1. Data rate and range coverage of popular wireless technologies are presented in Table 1-3 [19], [20].

Table 1-3: Comparison of wireless technologies used in power industry

Wireless Technologies	**Data Rate**	**Approx. Coverage**
Wireless LAN	**1-54 Mbps**	**100-200 m**
WiMAX	70 Mbps	48 km
Cellular (3G/ 4G)	60-240 Kbps	10-50 km
ZigBee	20-250 Kbps	10-100 m
MobileFi	20 Mbps	Vehicular Std.
Digital Microwave	155 Mbps	60 km
Bluetooth	721 Kbps	100 m

Appendix-A discusses various applications of different wireless technologies in power utilities, except wireless LAN. The applications of wireless LAN are discussed in following chapter.

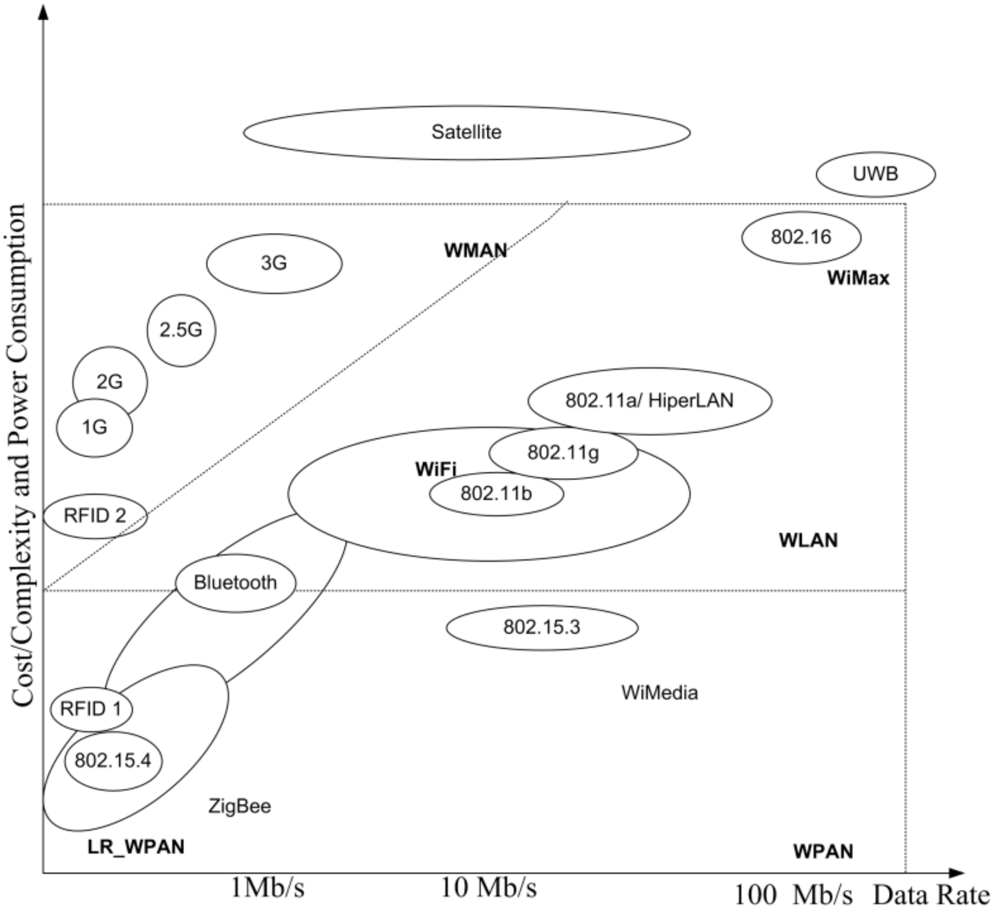


Figure 1-1 Overview of cost/complexity versus data rates of many wireless technologies [20], [21]

1.2.3 Industrial WLAN Applications and Comparison with Residential WLAN

Since the residential/business users of WLAN sometime have difficulties related to signal strength, security, etc., the first impression of applying WLAN for industrial use raises many concerns to power utilities. However, the industrial-grade WLAN technologies have already been in the use for other mission-critical industrial applications, e.g. mobile traffic control and road signs in transportation industries; mining automation; video surveillance in financial industries; tracking inventories and assets; pipeline monitoring, etc. [22]. Comparison between residential and industrial-grade WLANs is presented in Table 1-4. It can be inferred from the table that WLAN used in industry is much more robust, secure, and reliable as compared to residential WLAN. It is evident that industrial strength WLAN is more expensive and complex with respect to residential.

Table 1-4: Comparison of wireless technologies used in power industry

Features	Residential WLAN	Industrial Strength WLAN
High speed networks	YES	YES
Multiple WLAN interfaces to enhance reliability	NO	YES
Rugged outdoor design	NO	YES (IEEE 1613, IEC 61850-3, IP65/67 compliance)
Temperature	+10°C to +30°C	-40°C to +85°C
Security	WEP, WPA, WPA2 with IEEE 802.11i	IEEE 802.11i with AES; IEEE 802.1x RADIUS; SSH encryption; Port based access; May include vendor specific proprietary protocol
Registered MAC access and monitoring	Limited	YES (Enhanced)
Redundant power supply	NO	YES (additional power over Ethernet using IEEE 802.3af)
Robust directional or Omni-directional multiple antennas	NO	YES
Signal strength	Low	High (repeaters can be applied if required)
Cost	Low	High

1.3 Literature Survey - Application of Wireless Technologies in Power Substation

Wireless systems are used for decades for data communications in power utilities; microwave systems, spread spectrum radio, and multiple address radio are prime examples [23]. This section discusses various international technical reports and ongoing activities for deploying wireless technologies for different power utility applications. Moreover, the published case-studies and commercially available products are also presented below.

1.3.1 International Technical Reports and Ongoing Activities

In investigation report published by Electric Power Research Institute (EPRI) of USA, it was concluded that wireless technology will almost certainly be incorporated into future, high speed control system networks and substation applications [23]. Technical reports from IEEE P1777 committee [13] and EPRI [24] have investigated wireless technologies for power utilities, and presented the potential of these technologies for future substation protection, control and monitoring applications. Technical reports from IEEE PSRC and CIGRE have presented protection and control applications, e.g. enhanced transformer differential protection, breaker failure, and fast bus overcurrent trip, over wireless medium [25], [26].

1.3.2 Published Case-Studies

In reference [27], authors have investigated wireless LAN (Wi-Fi) with 11 Mbps data rate using laboratory set-up, and demonstrated the successful use of wireless LAN for line differential protection applications. Reference [28] demonstrates the wireless applications for differential protection and monitoring of air-core inductors even at 150kbps for protection within the substation. Pilot protection of distribution system with the help of digital radio technologies was analyzed by GE Digital Energy in reference [29]. The results documented in this reference shows that digital radio successfully sends the IEC 61850 GOOSE message within 10-15 ms of the time as a transfer trip signal. ABB Power Technology proposed wireless communication for medium voltage protection and control scheme. This paper proposes "e-breaker concept" to control the medium voltage breaker based on wireless communication systems [30]. Wireless applications for smart grid applications are also demonstrated in references [30]-[33].

1.3.3 Commercial Availability of Wireless Products for Distribution Substations

There are several manufacturers offer the different products based on traditional low data rate wireless technologies, for example, General Electric (GE) has products for the wireless communication between distribution automation substation and remote distributed energy resources (DER) [34], [35]. Further, Schweitzer Engineering Laboratory (SEL) has developed SEL-3022 wireless encrypting transceiver for advanced reclosure control applications in remotely located distribution substation [36]. Beckwith has products based on wireless LAN (IEEE 802.11) to localize the SCADA applications such as monitoring and control of transformer on-load tap changer (LTC) [37]. Product developers for power utilities have already initiated developing robust wireless LAN substation automation devices [38]-[41].

1.4 Literature Survey - Technical Issues while Deploying Wireless LAN

1.4.1 Radio Noise Profile Measurement and Modeling

The radio noise sources in a power substation environment can be classified in two different types: 1) Electro-Magnetic Interferences (EMI) from gap or insulation breakdown due to switching operation of SF6 circuit breaker or disconnector, lightning discharge, corona discharge, etc.; 2) Interferences from other radio devices installed within substation or in vicinity of a substation. The EMI/RF interferences from deliberate or inadvertent external EMI sources can slow down these transmissions of data by causing the wireless systems to re-transmit messages [24], [13]. In 1971, the joint study by CIGRE/IEEE on “Extra High Voltage Transmission Line Radio Noise” suggests the dependency of radio noise on weather or climatic condition [42]. The extensive work has been carried out to measure transient EMI in 115kV, 230 kV, 345 kV, and 500kV [43]. It was concluded that the measured transient EMI is significant in the frequency range of 1 kHz to 20 MHz. This transient EMI decays drastically and is almost negligible above 100

MHz. Measurement of EMI and experiment of applying wireless based digital data acquisition system in substation have been discussed in references [44], [45] It is concluded that wireless based data acquisition system has potential to be applied in an EMI environment of power substation. Power System Engineering Research Center (PSERC) has carried out study on measuring Electro-Magnetic Interferences (EMIs) in 34.5kV, 138kV, and 345kV substations in frequency bands of 900 MHz and 2.4 GHz [46]. Moreover, it was concluded that the instantaneous ingoing/outgoing voltage values, power factors, ambient temperatures as well as transformer temperatures does not have any obvious effect on radio noise profile in substation [47]. However, this report does not report measurement of EMI during substation switching events. Q. Shan et. al. in references [48], [49], presented measurement of impulsive noise in 400 kV Air Insulated Substation (AIS). The noise modeling in terms of distribution function is presented in these technical papers. Moreover, reference [48], [50] have demonstrated the degradation in the performance of WLAN in the presence of impulsive noise using the experimental lab set-up. The efforts have been put to study radio noise profile in power substation within the range of wireless LAN in report [51], and for Wireless Sensor Network (WSN) in [52]. However, there was no significant EMI measured. In summary, there is no literature available on measurement of noise profile in distribution substation, especially during switching. Moreover, the study of noise measurements in literature does not include Radio Frequency Interferences (RFI) from other wireless LAN devices surround distribution substations. Therefore, there is need for radio noise profile study in distribution substation, and model the measured radio noise in order to use it for performance related studies. In addition, it is important to measure interfaces from other wireless LAN based radio devices installed in vicinity of a distribution substation.

1.4.2 Dynamic Models of IEC 61850 Devices and Substation Noise

The IEC 61850 part-5 [53] suggests to evaluate the dynamic performance of IEC 61850 based substation LAN in order to study end-to-end communication delays in various worst case scenarios [54]. There are communication network modeling tools available with some standardized models, e.g. OPNET [55], NS-2[56] , etc. Literature is available on modeling Ethernet based WLAN in various simulation environment [57]-[61]. However, these works in literature do not include models of IEC 61850 protocol/communication stack. There is no platform available to analyze communication network performance of IEC 61850 based smart substation automation applications. Therefore, the effort is made to develop dynamic models of IEC 61850 devices based on IEEE 802.3 (wired LAN) standard [62] using OPNET tool [55]. However, there is no literature available on dynamic models of IEC 61850 devices based on IEEE 802.11 (wireless LAN). Moreover, the second challenge specific to wireless technology is to develop models of EMI present in distribution substations. Reference [63] presents channel model simulation for underwater acoustic sensor network using OPNET; however, there is no model available in OPNET for the radio noise available in distribution substation environment. Therefore, there is a need for the development of dynamic models for IEC 61850 based devices, e.g. Intelligent Electronic Device (IED), and Merging Unit (MU); as well as, substation noise models in order to simulate distribution substation environment.

1.4.3 Performance Evaluation

IEC 61850-5 standard [53] specifies the allowable average transmission delay requirements, e.g. in case of time critical applications, it is 10 ms for distribution substation, and 3ms for transmission substation. This time delay requirements has to be achieved for all the time critical messages e.g. GOOSE and sampled values, independent from the network traffic load on the process bus communication network. However, the overall system performance and its extensibility can’t be easily solved using this standard although it does classify the message performance class. Therefore, the performance of wired Ethernet network for IEC 61850 based substation automation system is evaluated in various references [62], [64]-[67] using OPNET tool. However, until now none of the literature presents the performance evaluation of latest wireless LAN technologies for IEC 61850 based substation automation applications. Therefore, it is important to assess 802.11 based network performance for IEC 61850 based substation automation systems.

1.4.4 Hardware Setup and Field Testing

In order to access the performance of a technology for a particular application, it is important to develop proto-type devices and carry out real field testing. Some efforts are put in order to setup wireless devices and test a specific application in a substation and/or laboratory [27], [28], [48]. However, there is no work presented in literature to develop IEC 61850 based wireless LAN devices for distribution substation, and, test them in distribution substation for various range of IEC 61850 applications.

1.4.5 Security /Reliability of the wireless communication

For data transmission of wireless signals air is medium. Therefore, threat of data security is more with wireless technologies as compared to wired technology [24]. Wireless signals are weak and faded, which may cause failure of transmission whenever an end device is moved toward the edge or beyond the normal signal range, or if unusual atmospheric or other environmental conditions cause the actual range to become less than the normal range. Also, wireless devices are battery operated and batteries can run out of energy before they are supposed to, or can fail without warning. This results in to unreliability of wireless device [25], [14].

1.5 Motivation for the Research Work

Current implementations of communication networks for substation automation system are based on wired technology due to high data rates and less susceptibility to EMI/RF interferences. However, over a past few years advancement in wireless communication system offers the benefits of higher data rate, low cost of installations, more probabilities and flexibility of data acquisition, which are not offered by wired technologies for substation automation purpose. Above literature survey suggests the potential of wireless communication application in the power application. Further, literature highlights the limitation of wireless technology, which restrains its use for time critical applications in electric substation environment. There were some challenges faced by wireless LAN technologies, such as lower data rate, effects of noise interferences, and congestion of unlicensed frequencies. In spite of these challenges, with the recent advancements in wireless LAN technologies, the use of wireless technologies in IEC 61850 based substation automation system need to be assessed with respect to communication performance requirement for protection and control applications.

1.6 Research Methodology

1.6.1 Scope of the research

This research work assesses the wireless LAN (IEEE 802.11) technology performance for IEC 61850 based substation distribution automation system. The main tasks of this project are listed below:

- Noise profile measurement in distribution substations, and modeling using MATLAB tool.
- Developments of WLAN based dynamic models of protection and control (P&C) intelligent electronic devices (IEDs), merging unit (MU), etc. in compliance with IEC 61850 using OPNET simulation tool.
- Performance analysis of IEC 61850 based distribution substation automation systems considering various parameters, such as data rates of the WLAN technologies, sampling frequency, signal to noise ration in the substation, bit error rate, etc.
- Hardware Lab Set-up and field testing.

1.6.2 Research Methodology

The methodology of the research work is summarized as follows:

I. EMI/RFI measurement in distribution substation and noise modelling: The noise level measurements at 27.6 and 13.8 kV London Hydro Inc. distribution substations are carried out using the commercial spectrum analyzer. The measured substation noise profile is modeled using various distribution functions in the MATLAB tool.

II. Modeling of IEC 61850 automation devices with WLAN interface using OPNET: Detailed dynamic modeling of wireless enabled IEC 61850 based substation automation system devices, i.e. intelligent electronic device and merging unit, and incorporation of measured substation noise interference models are carried out with the help of industry-trusted dynamic simulation tool, OPNET. Using these proposed dynamic models of wireless IED and MU, WLAN for the IEC 61850 based distribution automation and protection is simulated for a typical 27.6/13.8 kV distribution substation. The performance evaluation of smart distribution substation applications related to protection, control and monitoring is examined considering effect of Quality of Service (QoS) parameters, various wireless LAN data rates, sampling frequencies of sampled value messages, and substation noise levels. Also, the evaluation of WLAN based communication network for IEC 61850 based distribution automation system (DAS) with DER are analyzed in OPNET. Similar kind of analysis is also carried out for the WLAN based communication network of micro grid network.

III. Laboratory Set-Up: The development of wireless enabled IEC 61850 based substation devices, such as wireless IED and MU, using industrial embedded systems with hard-real time platform are setup in the laboratory. In order to assess wireless LAN performance, the further laboratory setup includes commercial wireless Access Point (AP), traffic generator, noise sources, network analyzer, and spectrum analyzer. The examination results from the developed hardware laboratory are discussed in detail.

IV. Field Testing: Field measurement experiments in London Hydro Inc. and Hydro One Inc. distribution substation is carried out. RTT delay of time critical messages using different WLAN technology are measured during field test. Over current relay performance over the WLAN communication network is also analyzed in this study.

1.7 Thesis Outline

This thesis is organized in eight chapters and four appendixes.

Chapter 1 provides introduction about the research subject, along with literature survey, motivation behind this research and research methodology. In the second chapter, brief introduction about the IEC 61850 the standard for substation automation, IEEE 802.11 Wireless LAN standard are presented. Also, various applications of the wireless LAN in the smart distribution substation are explained in the detail.

Chapter 2 presents salient features of IEC 61850 (standard suite for substation automation systems), as well as IEEE 802.11 (standard suite for WLAN technologies). Furthermore, the key smart distribution substation applications which can be realized using WLAN technologies are also discussed in this chapter.

Chapter 3 includes noise analysis from the real world distribution substation measurement took during normal and fault condition. This chapter describes the basics about the instruments used during the substation noise measurement, and gives the detail idea about the test measurement setup at the test site.

Chapter 4 covers the introduction of the OPNET simulation tool used for the modeling and analysis of Wireless LAN based substation communication network. It also describes the various models, like WLAN IED, WLAN merging unit, noise model developed for the distribution network communication network analysis. Various IEEE 802.11 standard features develop and include in the model, like packet format, WLAN pipeline stages, quality of service implementation are discussed in the detail.

In chapter 5, performance analysis of WLAN based communication network for various sceneries are presented. Communication network analysis in terms of delay, throughput, and various data rate for IEC 61850 based distribution substation automation system is presented. It also includes WLAN communication network analysis between DAS and DERs networks as well as various Microgrid applications are also presented.

Chapter 6 discusses the hardware prototypes development of WLAN enabled IEC 61850 devices, and a laboratory setup for the further performance investigation. Results and analysis of the developed hardware setup in the laboratory environment are presented.

Field testing of these developed WLAN enabled IEC 61850 devices (deployed at 13.8 kV and 27.6 kV distribution substation owned by London Hydro Inc, and Hydro One Inc.) is presented in chapter 7. The results are analyzed and important concludes are discussed in detail.

The thesis is summarized and concluded in Chapter 8.

1.8 Summary

A brief introduction about the basics of distribution substation and WLAN communication network are provided in this chapter. Challenges and proposed solution were discussed in detail. The research motivation, methodology and a detailed outline of the organization of the thesis are also given in this chapter. Basics of IEC 61850, WLAN and potential applications of WLAN in IEC 61850 based distribution substation will be discussed the following chapter.

Chapter 2

2. Potential Applications of WLAN in IEC 61850 based Smart Distribution Substation

This chapter includes the basic features of IEC 61850 standard and IEEE 802.11 wireless LAN standard. Thereafter, potential of implementing wireless LAN based communication network for various application in smart distribution network, including within substation, between substation and distribution generation resources, and within Microgrid are discussed in detail.

2.1 IEC 61850 – A standard for Substation Automation

IEC 61850 standard defines the communication protocol and logical node functions to facilitate the universal modeling of the SAS devices. The high-speed digital communication allows replacing the traditional electrical wiring using virtual wiring, which could save a lot of time and cost for substation automation system. Different from that of earlier standards, the technical approaches make IEC 61850 open and future-proof.

2.1.1 IEC 61850 Architecture

It can be inferred from the Figure 2-1 that station bus facilitates the communication between the station level and bay level. For this communication application interfaces applied between them are shown in figure i.e.IF1, IF3, IF6, IF8 and IF9. Similarly, process bus is used for data exchange purpose between bay level and process level. Interface IF4 and IF5 supports this communication. The functions of interface numbers used in Figure 2-1 are explained in Table 2-1.

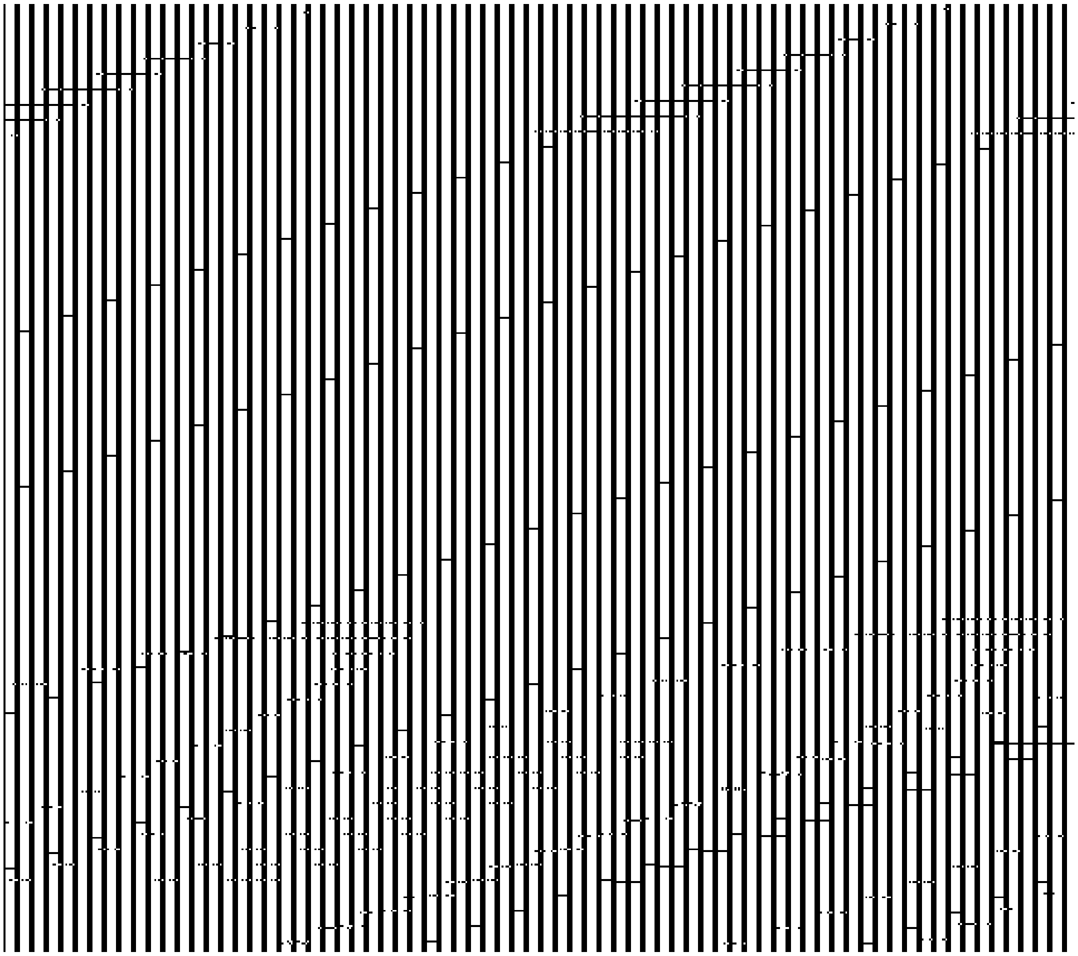


Figure 2-1 IEC 61850 architecture

Table 2-1 Interface types & their function

Sr. No.	Interface Types	Function
1	IF 1	Protection-data exchange between bay and station level
2	IF 2	Protection-data exchange between bay level and remote protection (beyond the scope of IEC 61850 standard)
3	IF 3	Data exchange within bay level
4	IF 4	CT and VT instantaneous data exchange (especially samples) between process and bay level
5	IF 5	Control-data exchange between process and bay level
6	IF 6	Control-data exchange between bay and station level
7	IF 7	Data exchange between substation (level) and a remote engineer's workplace
8	IF 8	Direct data exchange between the bays especially for fast functions such as interlocking

9	IF 9	Data exchange within station level
10	IF 10	Control-data exchange between substation (devices) and a remote control centre (beyond the scope of IEC 61850 standard)

The seven types of messages are mapped into different communication stacks. As shown in Figure 2-2, the raw data samples (type 4) and GOOSE messages (type1, 1A) are time critical and are, therefore, directly mapped to low–level Ethernet link layer. This gives the advantage of improved performance for real time messages by shortening the Ethernet frame (no upper layer protocol overhead) and reducing the processing time. The medium speed message (type 2), the command message with access control (type 7), the low speed message (type 3) and the file transfer functions (type 5) are mapped to MMS protocol suits which has a TCP/IP stack above the Ethernet layer. The time synchronization messages (type 6) are broadcasted to all IEDs in substation using UDP/IP.

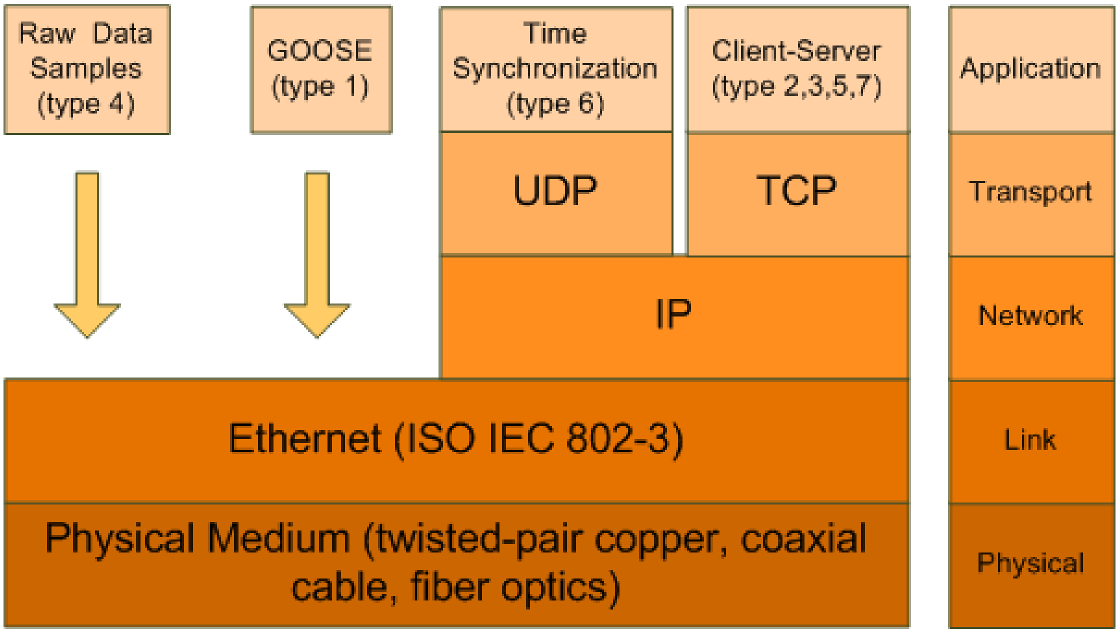


Figure 2-2 IEC 61850 Message Communication Stack

Table 2-2 shows the relation between message types and interfaces with respect to different communication stack as discussed in Figure 2-2.

Table 2-2 Message types and their interface support

Sr. No.	Message Type	Communication Protocol	Interfaces Support
1	Type 1 1a – Trip 1b – Others Message	Direct on Ethernet Link Layer	IF 3,5,8
2	Type 2 Medium Speed Message	Client Server (TCP/IP)	IF 3,8,9
3	Type 3 Low Speed Message	Client Server (TCP/IP)	IF 1,3,4,5,6,8,9
4	Type 4 Raw Data Message	Direct on Ethernet Link Layer	IF 4
5	Type 5 File Transfer	Client Server (TCP/IP)	IF 1,3,4,6
6	Type 6 Time Synchronisation Message	UDP/IP	IF 1,3,4,5,6,8,9
7	Type 7 Command Message with Access Control Message	Client Server (TCP/IP)	IF 1,6,7

2.1.2 Communication Performance Requirements

As per IEC 61850, the transfer time is the time counts from the moment the sender (IED) puts the data content on top of its transmission stack up to the moment the receiver (IED) extracts the data from its transmission stack.

PICOMs refer to information transfer based on single dedicated functionality, and include source and sink. The messages types are based on a grouping of the performance related PICOM attributes, and therefore, define the performance requirements to be supported. The performance requirements are independent of the size of the substation, and are defined according to functionality.

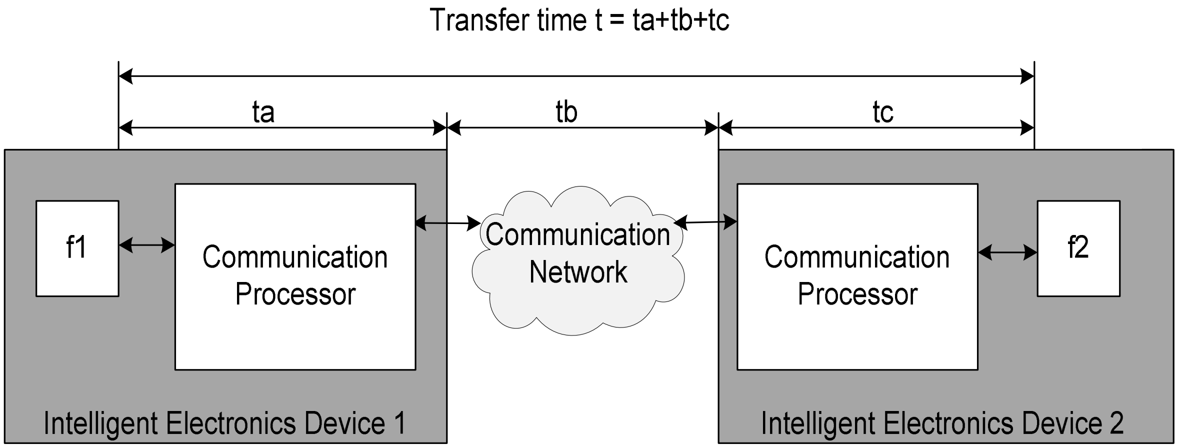


Figure 2-3 IEC 61850 Message Communication Stack

The modeling of IED shall be based on the communication stack specified in IEC 61850. According to IEC 61850-5 and IEC 61850-8, messages are classified into 7 categories based on the performance requirements. Table 2-3 summarizes these messages and transfer time requirements based on IEC 61850 standard.

Table 2-3 Message and transfer time requirement

Sr. No.	Message Type	Application (In PICOM)	Transfer Time Limit (ms)
1	Type 1 1a – Trip 1b – Others Message	Trigger	10-100
		Complex block or release	10-100
		Fast broadcast Message	1
		Process State Changed	1-10
		Trip	1

2	Type 2 Medium Speed Message	Process value in r.m.s	50-1000
		Request for syn. check interlocking	10-100
		Process State	1-100
		Calculated State	1-100
		External Condition	1-100
3	Type 3 Low Speed Message	Measured value	100-1000
		Meter value	100-1000
		Non – electrical Process value	1000-5000
		Fault value	1000-5000
4	Type 4 Raw Data Message	Process value (Sample voltage & Current)	0.1-10
5	Type 5 File Transfer	Report e.g. Energy list	1000-5000
		Mixed fault info.	1000-5000
		Mixed fault data	5000
		Event/Alarm List	100-1000
		ID data, Setting	1000-5000
		Diagnostic data	5000
6	Type 6 Time Synchronisation Message	Synchronise of pulse	0.1-10
7	Type 7 Command Message with Access Control Message	Command (From local to remote HMI)	1-1000

2.1.2.1 Benefits of IEC 61850 Based Implementation:

- Interoperability: Different vendors are allowed to provide complete integration of bay functions within one or two IEDs.
- Free Configuration: Any possible number of substation protection and control functions can be integrated at the bay level IED.

- Simple Architecture: As the plenty of point-to-point copper wires are reduced to just simple communication links. Further, functional hierarchy architecture provides better communication performance for time critical applications.
- Overall Cost Saving: The high-speed digital communication at process level allows replacement of the traditional electrical wiring using virtual wiring, which could save a lot of time and cost for substation automation system.

2.1.3 IEC 61850-7-420 Standard

Utility and DER manufacturers recognized the growing need to have one international standard that defines the communication and control interfaces for all DER devices. As an extension of IEC 61850, the standard IEC 61850-7-420 is published in2009. The standard IEC 61850-7-420 comprises the information model to communicate with and within any distributed energy resources like wind farm, photovoltaic systems, fuel cell systems, combined heat and power, etc. These systems are integrated into the utility information and automation systems so that they are closely related to the standard series IEC 61850.

2.1.3.1 Benefits of using IEC 61850-7-420

- Interoperability of communication between IEC 61850 based DAS and DERs
- No conversion of proprietary protocols, therefore no loss of information.
- Standardized and consistent data models for all DERs
- Seamless integration into the station automation and the power control system
- Saving time and cost in implementation, maintenance, enhancement

2.2 EMI Requirements

Various electromagnetic interference such as, lightening and switching surges, electrostatic discharges, strokes in SF6 circuit breaker, etc. are commonly encountered in the substation. Hence, general EMI immunity requirements used for industry are not sufficient for substations. IEC 61850-3 Communications Networks and Systems in Substations – Part 3: General Requirements. Section 5.7 of the standard outlines the EMI immunity requirements for communications equipment installed in substations. For more details the IEC 61850 refers the requirements and testing procedures given in the parts of the IEC 6100 series (IEC 61000-6-5 and IEC 61000-4-x) or IEEE C37390.2. The IEC 61000-6-5: "Generic Standards – Immunity for power station and substation environments" outlines the EMI immunity requirements. The details of these requirements and type test procedures are given in the parts of the IEC 61000-4-x series. IEEE C37.90.x defines a variety of type withstands tests designed to simulate EMI phenomena such as inductive load switching, lightening strikes, electrostatic discharges from human contact, radio frequency interference due to personnel using portable radio handsets, ground potential rise resulting from high current fault conditions within the substation and a variety of other EMI phenomena commonly encountered in the substation. All the SAS devices such as IEDs, MUs, Ethernet switches, and other communication devices shall be designed and tested to withstand the various types of induced conducted and radiated electromagnetic disturbances that occur in substations.

2.3 Wireless LAN Technologies

IEEE 802.11 standard is known as standard for wireless local area network. It is divided in to various sub groups. Brief idea about the standards development growth is explained in the following subsection.

2.3.1 WLAN Standards

Major parts of IEEE 802.11 standards are explained below. Figure 2-4 shows the standard development growths, and data rate offered by different wireless LAN technologies.

1. IEEE 802.11: IEEE 802.11 defines the standard for wireless Local Area Networks (LANs) encompassing three incompatible (non-interoperable) technologies:

Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Infrared (IR) at 1 & 2Mbps data rates.

2. IEEE 802.11a: This standard provides data rate up to 54Mbps, but the devices that use it are more expensive than both 802.11b and 802.11g standard devices. 802.11a uses the relatively uncluttered 5 GHz frequency band, and has a range of around 25-75 feet (7.6 to 23m, approx). 802.11a's limitation is that it's not compatible with any other standard. Hence, it is rarely implemented.
3. IEEE 802.11b: IEEE 802.11b is also known as “WiFi”. Currently, WiFi is the most popular wireless standard out there; it has the advantage of being the cheapest of these three standards. 802.11b runs at 11Mbps, and uses the more crowded 2.4 Ghz band, with a range of 100-150 feet (30.5m to 45.7m, approx) [68].
4. IEEE 802.11g is the updated version of WiFi standard and can provide data rate up to 54Mbps [69]. It uses the same 2.4 GHz band, with the same range of 100-150 feet, and is backward compatible with 802.11b standard.

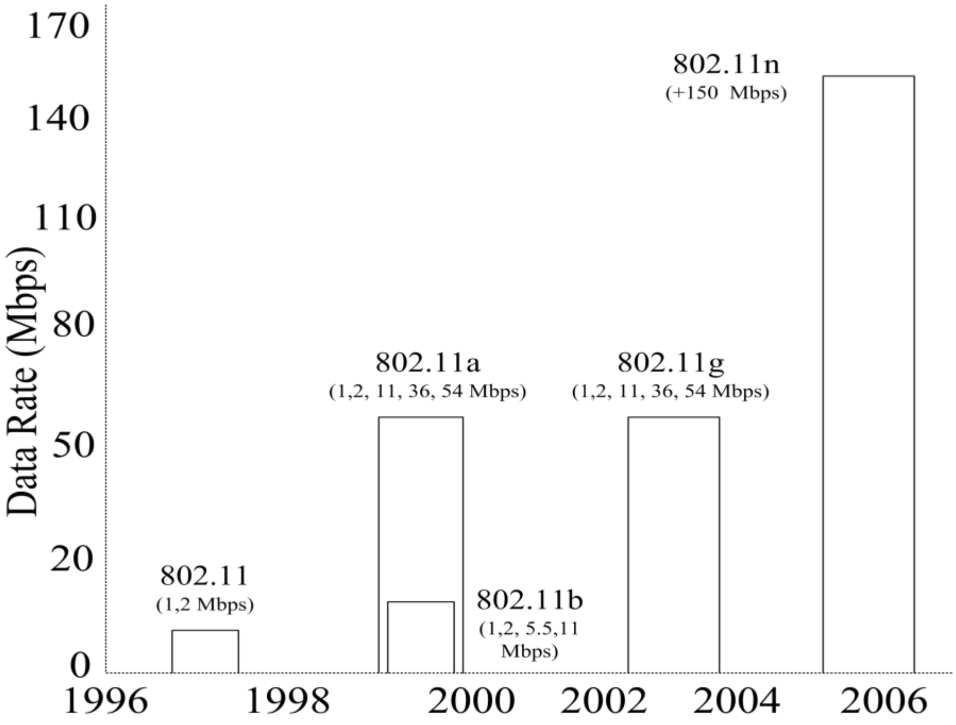


Figure 2-4 WLAN technology growth

5. IEEE 802.11n: The IEEE 802.11n standard is intended to increase data rates further, up to 300 Mbps. Performance is enhanced through the use of multiple antennas (MIMO-OFDM). It can be operate in both the ISM and U-NII frequency bands.
6. IEEE 802.11i: Earlier version of IEEE 802.1i uses Wired Equivalent Privacy (WEP) specification which had very high security impuissance (flaws). Wi-Fi alliance introduces Wi-Fi Protected Access (WPA) in 2002, as a intermediate solution to the WEP insecurity problems. It offers improved security features on WEP by the use of Temporal Key Integrity Protocol (TKIP). It also improves data integrity with the implementation of more robust hashing mechanism, the Michael Message Integrity Check (MMIC). Still, both WEP and WPA uses the RC4 encryption algorithms, which causes the data confidentiality issue. In June 2004, IEEE 802.11i amended the standard which is also known as WPA2 and Robust Security Network (RSN), which later also incorporated in IEEE 802.11, 2007 [70]. The 802.11i replaced the RC4 encryption algorithm with Advanced Encryption Standard (AES). It provides two different modes of security; Personal Mode and Enterprise Mode. WPA2 Enterprise mode provides RSN which depends upon IEEE 802.1X, the 4-way Handshake, and the Group Key Handshake and change cryptographic keys.

   The enhancements provided by 802.11i finally deliver the level of data confidentiality, integrity and user authentication demanded by the industry, which facilitates the WLAN deployment to meet security standard of the industries [71]. In addition to the data confidentiality and authentication featured offer by the IEEE 802.11i, depending on the need of the system environment in which WLAN is deployed, additional security features like wireless intrusion detection and preventions mechanism, can be set up to achieve higher level of security.

2.3.2 Network Wireless topologies

2.3.2.1 Ad-hoc Network

Ad-hoc network is one of the networking topologies provided in the 802.11 standard. It consists of at least two wireless stations where no access point is involved in their communication. Ad-hoc mode WLANs are normally less expensive to run, as no APs are needed for the communication. However, this topology cannot scale for larger networks. Further, there are communication node association related issues with this topology. Hence, it has rare application for substation automation.

2.3.2.2 Access Point Network

Access Point mode is another networking topology in the 802.11 standard, in addition to ad-hoc mode. It consists of a number of wireless stations and access points. This network topology can scale to form large-scale networks with arbitrary coverage and complexity. Usually, an AP connects into to a wired network, and provides a bridge for data communication between wireless and wired devices.

It is generally advisable to use Access Points as compared to Ad-Hoc Networks for substation automation applications. This is because they provide a variety of benefits - they increase the range, provide better security, help in saving power, provide quality of service (QoS), allow roaming, etc.

2.3.3 Spread Spectrum Encoding Technologies

The Spread spectrum technique was developed initially for military and intelligence requirements. The basic idea is to spread the information signal over a broad bandwidth to make jamming and interception more difficult. Generally, but not always, the spreading code is generated by a pseudo noise, or pseudorandom number generator. By using this technique, one can get immunity from various kinds of noise and multi path distortion, it is also useful for hiding and encrypting signals, and hence multiple users can solely use the same bandwidth with very little interferences.

2.3.3.1 Frequency hopping techniques (FHSS)

In FHSS, the signal is broadcast over a seemingly random series of radio frequencies, and hoping from frequency to frequency is carried out at fixed intervals. There are two types of frequency hoppers: fast hoppers and slow hoppers. In slow hoppers the frequency is changed once per bit or once per “n” bits. While in fast frequency hopper the frequency may be hopped multiple times during the period of a single data bit transmission.

2.3.3.2 Direct Sequence Spread Spectrum (DSSS)

In this technique, each bit in the original signal is represented by multiple bits in the transmitted signal, using a spreading code. The spreading code spreads the signal across a wider frequency band in direct proportion to the number of bits used. Therefore, 10-bit spreading code spreads signal across a frequency band that is 10 times greater than a 1-bit spreading code.

In general, Frequency hopping averages the interferences, using a form of nonlinear modulation. Therefore, devices using FHSS need less power and are cheaper. While, direct sequence spread spectrum is a linear process, it consumes more power. But, the performance of DSSS is usually better and more reliable compare to FHSS.

2.3.3.3 Orthogonal Frequency Division Multiplexing (OFDM)

It is also called multicarrier modulation. It divides a digital single across a very large number of separate signal carrier frequencies that are transmitted simultaneously. OFDM uses an inverse fast Fourier transformation to determine the orthogonal frequencies, then spreads each bit simultaneously over each frequency, and finally “de-spreads” the received information using the fast Fourier transformation to regenerate the bit. OFDM can be considered as a spread spectrum technology, since it transmits in parallel over multiple frequencies.

Table 2-4 Comparison of RF modulation technologies [25]

	FHSS	DSSS	OFDM
Basic spreading strategy	Interference avoidance	Interference minimization	Data rate maximization
Spectrum Utilization	Lowest	Median	Highest
Range	Lowest	Median	Highest
Multipath fading rejection	Median	Lowest	Highest
System Complexity	Lowest	Median	Highest
Maximum data rate	Limited by FCC rules	Median	Highest
Latency	Highest	Median	Median
Power Consumption	Lowest	Median	Highest
In-band interference behavior	Dynamic data frame dropout on occupied channels	Graceful degradation until jamming margin is exceeded followed by total link failure	Adaptive data rate reduction
Loss of synchronization (penalty)	Highest (seconds)	Lowest	Low
Out of band interference rejection	Lowest	Highest	Medium to High

NIST has recognized IEC 61850 standard for substation automation and protection applications in smart grid environment. Wireless LAN technologies are also known as wireless Ethernet; and therefore, it can be considered for various smart grid applications, such as distribution substation automation and protection, and monitoring and control of distributed energy resources, especially for remotely located small substation and DERs, where data rate requirements and radio interferences are comparatively less.

2.4 Smart Distribution Substation Control and Monitoring Application using WLAN

2.4.1 Fast Distribution Bus Protection Scheme

A dedicated bus protection may not be economical for medium/low voltage distribution substation. Therefore, conventional method to protect distribution bus is using overcurrent relays, where the loads on the bus are fed radially (unidirectional power flow). Normally, the upstream protection IED (IED-1) is delayed by downstream feeder IEDs by coordination interval, i.e. approx. 400 to 500 ms or more [72]. This coordination interval is inserted in order to allow downstream feeder IED before bus IED in case of a feeder fault. However, if there is a fault on bus, bus overcurrent protection is delayed by this coordination delay (400 ms to 500 ms). This time delay can be drastically reduced by deploying low cost WLAN communication as explained below:

In this scheme, peer-to-peer IEC 61850 GOOSE message can be used to send signal from feeder protection IEDs to bus overcurrent IED. This scheme only requires non-directional overcurrent protective elements, with low-cost communication channel (i.e. wireless LAN). In case of a fault on feeder, two IEDs will detect a fault: 1) corresponding feeder IED, and 2) upstream bus IED. The feeder IED will immediately send BLOCK command using IEC 61850 GOOSE message, and feeder IED will isolate the fault. On the other hand, if there is a fault on the distribution substation bus, none of the feeder IEDs will detect a fault, and this way, bus IED will not receive any BLOCK message, and will operate normally after a delay of approx. 60 ms [73] (normally fault is detected in 4 ms, and average WLAN communication delay is approx. 5-10 ms). This way coordination delay can be reduced from 400-500 ms to 60 ms. This scheme improves the life of components installed on upstream of distribution bus, i.e. distribution transformer, since the time of fault current passing through these components reduces.

Furthermore, this scheme further can be enhanced to simultaneous faults. For example, if there is a simultaneous fault on bus and a feeder, this scheme can utilize IEC 61850

GOOSE message communication to not only send BLOCK command, but also incorporates information like, types of faults. This way, if feeder IED detects L-G fault, however, bus IED detects multiple phase faults, bus IED can immediately override BLOCK command, and operates.

The concept of fast distribution bus protection scheme is shown in Figure 2-5.

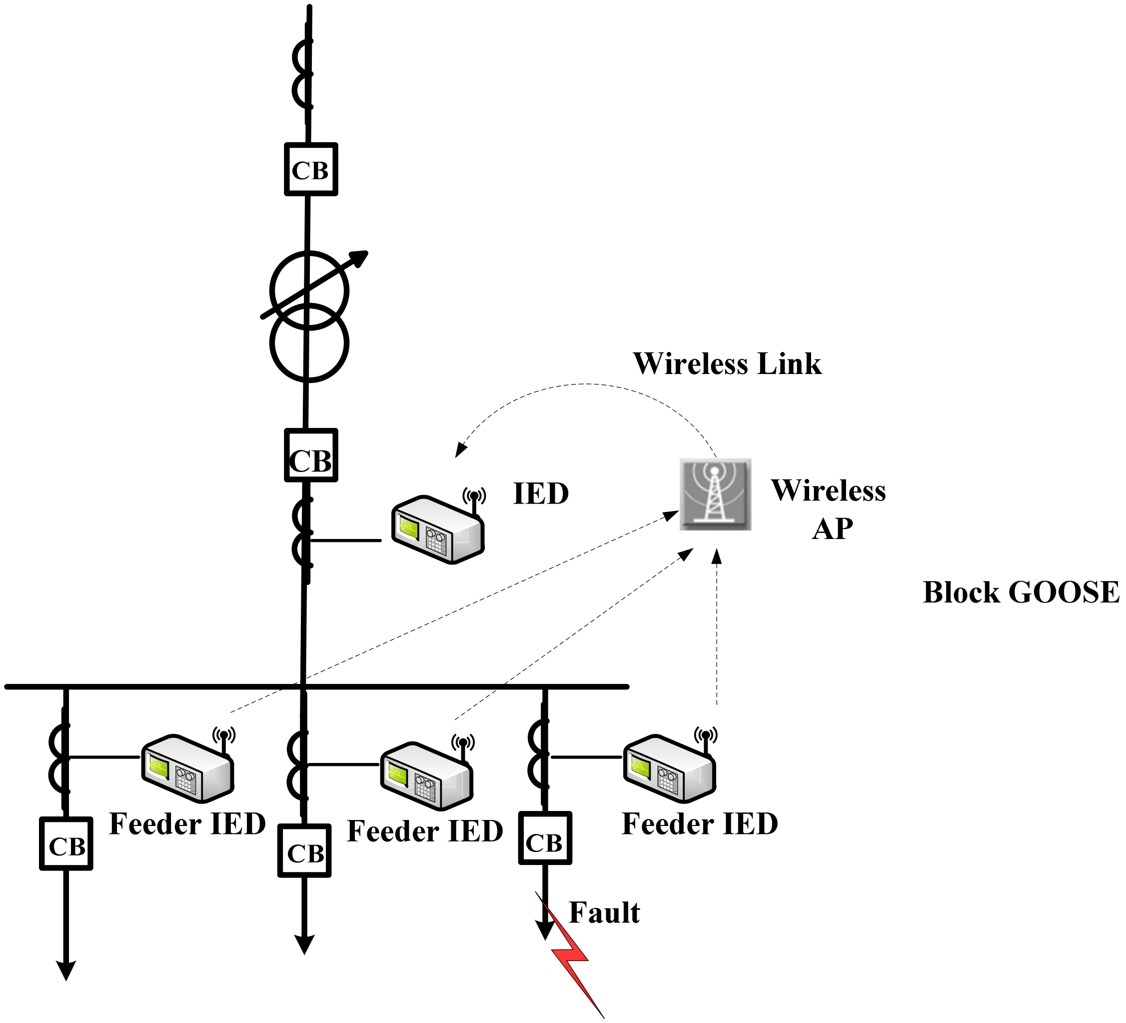


Figure 2-5 Wireless LAN communication for fast distribution bus protection

2.4.2 LTC Control and Monitoring for Enhanced Transformer Protection

Figure 2-6 shows the IEC 61850 based wireless LAN to enhance the distribution substation protection and automation. A technical report from IEEE PSRC [25] has presented protection and control applications using spread spectrum radio, some of the reported intra-substation applications which include an enhanced transformer differential protection. The wireless LAN channel can be installed to facilitate communication between LTC control/monitoring field device and transformer protection and control IED. The transformer IED can control LTC to maintain the bus voltages within the predefined range. The IEC 61850 GOOSE message can be used to communicate RAISE/DROP the transformer tap settings. The performance requirement for LTC control is 0.25 second [72], which can be well within WLAN average delay. On the other hand, the LTC sensor can retransmit the IEC 61850 GOOSE messages to confirm the POS (position status) signal of the transformer tap value. Normally, the LTC has ± 10% controllable tap setting range. And therefore, the transformer differential protection slope has to be set higher. However, this higher protection slope affects the sensitivity and dependability of the protection. The IEC 61850 GOOSE messages with current tap value can be communicated to the conventional transformer IED over the WLAN network. And, this way slope of the differential protection IED can be adjusted adaptively (according to the tap status). This way, with this wireless LTC sensor can enhance transformer differential protection by online monitoring of LTC position, as shown in Figure 2-6.

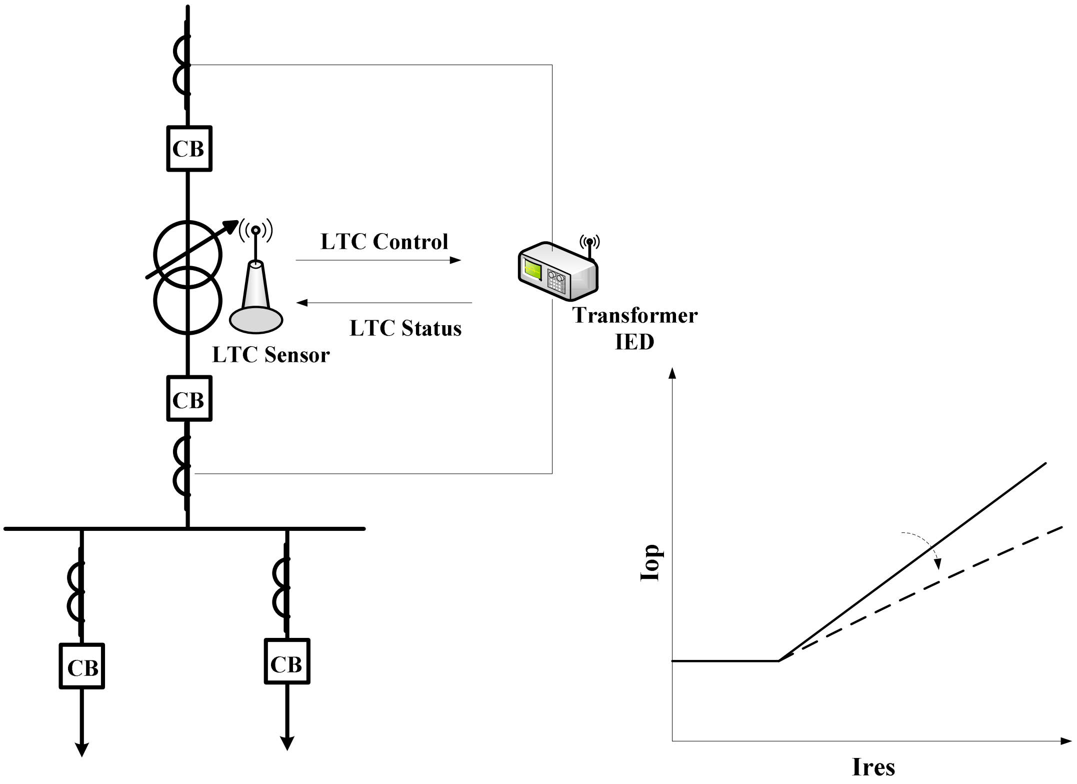


Figure 2-6 Wireless LAN communication for LTC control and monitoring

2.4.3 **Automatic Capacitor Bank Control**

Capacitor banks are more widely used in distribution systems for VAr (reactive power) or voltage control. The scheme for controlling the capacitor banks utilizes the single or multiple measurements, e.g. time of day, voltage level, power factor, and VAr flow. The VAr/voltage control device can be used to switch ON/OFF capacitors of the bank in order to minimize the reactive power flows on the system, and to maintain the bus voltage. VAr/voltage monitoring and voltage control allows communication delay up to 500-1000 ms [72]. This scheme not only enhances the control by considering multiple control parameters, but also reduces wiring cost by deploying low cost, plug-and-play wireless LAN devices.

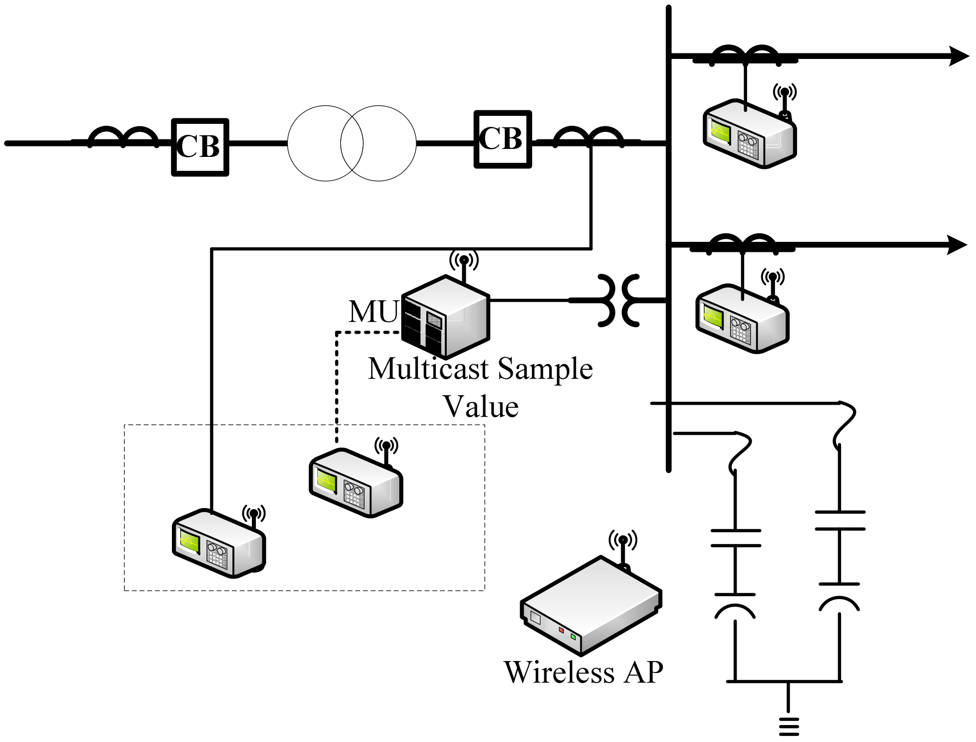


Figure 2-7 Wireless LAN communication for automatic capacitor bank control

2.5 Smart Distribution Substation Automation and Metering Application using WLAN

2.5.1 Distributed Digital Record Triggering

Modern protective digital IEDs have capability to record various user defined signals during an event as a part of oscillography or data logger. These digital IED recorders can be triggered to start recording while detection of a specific event. Actually, the protective IEDs for various zones of protection in a substation have different triggering (element) logic, and also they are connected to different signal sources (CTs/VTs). Therefore, it is not possible to have record of all signals (at least recording from adjacent zones of protection IEDs), and this may lead to lack of information for post-fault analysis. For example, it would be desirable for an overcurrent relay to trigger another relay on bus that could acquire bus voltage waveforms.

This concept uses IEC 61850 GOOSE messages over wireless LAN to trigger all adjacent/corresponding IEDs in order to record all various signals in a substation. This will minimize mesh wiring among substation IEDs, eliminate need of centralize digital fault records, and also help to reduce maintenance issues in a substation. In addition, currently many distribution substations do not have data logging implemented, but equipped with modern digital IEDs. This distributed recording can help post-analysis at affordable cost. In addition to that, wireless LAN can be used to carry out automatic oscillography data retrieval at the end of each event recording, which can provide tremendous manpower savings, and lead to quick post-diagnosis of the event. Trigger delay of in order of a few cycles is acceptable [72].

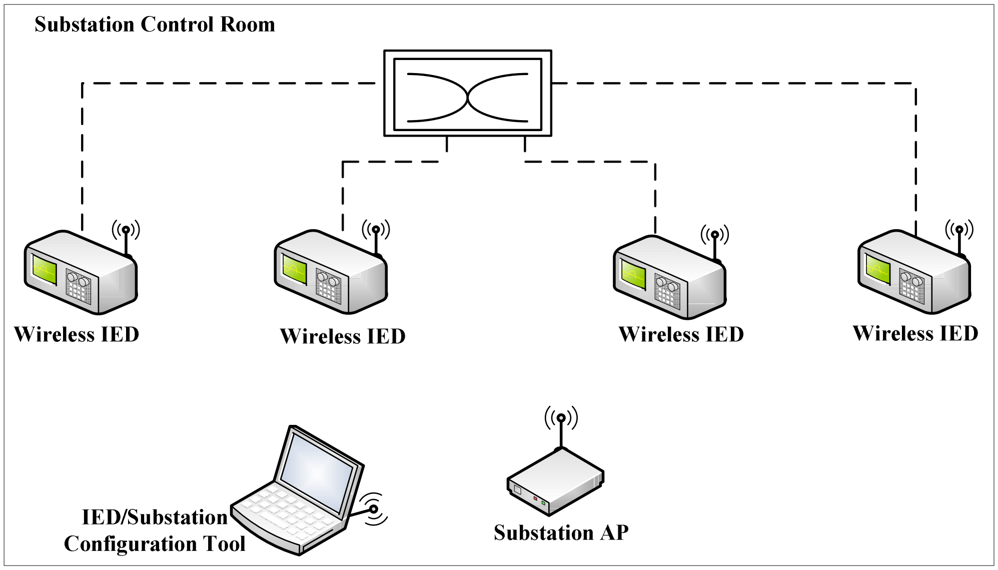


Figure 2-8 Wireless LAN communication for distributed digital record triggering

2.5.2 **Watt/VAr Measurement using Broadcasting Voltage Phasors**

In distribution substation, it is common to obtain bus voltage at every feeder (breaker) in order to carry out metering of active/reactive power, power factor, etc. in a feeder IED for all three phases. Digital IEDs allow metering since they already have access to feeder currents. However, it is very expensive to bring all three phase bus voltage to each of these substation IEDs. Therefore, current practice is to use a single phase of a station service voltage and assume that all phases are balanced.

The anticipated solution for this is to multicast IEC 61850 sampled value over wireless LAN containing all three phase bus voltages from a field device (merging unit) or from a substation control room IED connected to bus VTs. According to reference [72], these Watt/VAr measurements are intended for load range monitoring, an update rate of once per second is adequate, with accuracy of 1% in voltage magnitude and 3 degree in phase angle. Moreover, the multicasting of these SVs over WLAN is not time critical, and even missing of data for few seconds is tolerable without affecting the metering applications.

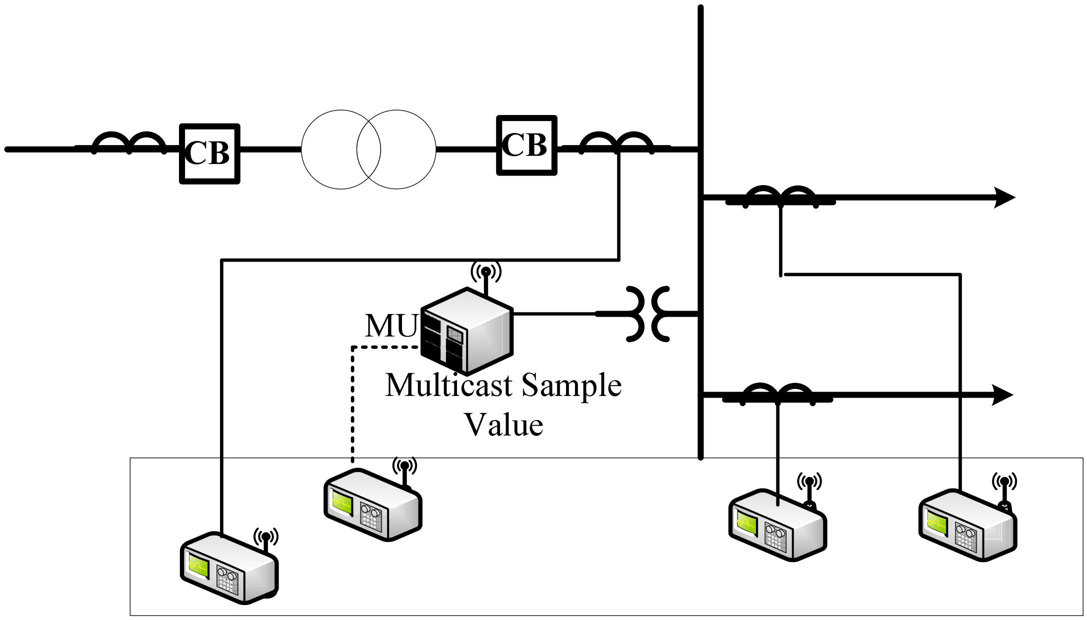


Figure 2-9 Wireless LAN communication for Watt/VAr measurment

2.5.3 **Centralized IED Configuration**

Each digital substation IED has a console port, either serial RS 232 or Ethernet based, which allows various access functionalities to a substation engineer, such as set the protective elements, check event data loggers, observe oscillography, etc. Normally, this console port is dedicated, and therefore may not be part of substation communication network. With the advent of IEC 61850-6 compliant IEDs, it is possible to configure IEDs automatically using various file types by interfacing vendor specific IED configurator with a single substation configuration tool. However, current practice is to exchange these configuration files manually, i.e. obtain .ICD files through memory stick/CD and bring all them to substation configurator, and after configuration, the .CID or .SCD file is stored in one the memory storage medium. This storage has access connected to a substation laptop connected to an IED, and then loaded to the substation IED. This process of uploading .CID or .SCD file into the IED has to be carried out for individual substation IEDs.

The potential solution is to use wireless LAN network within substation control room among substation IEDs and centralized configuration tool. This centralized configuration tool can be the IEC 61850-6 based configurator or a vendor specific IED configuration tool. The setting or accessing multiple substation IEDs (from the same vendor) using a vendor specific tool or automatic configuration of all substation IEDs through centralized IEC 61850-6 based substation configurator can easily achieve by exchanging files and commands over wireless LAN. This is a fast, easy, and low-cost solution for the non-critical information exchange within the control room. Moreover, the signal power of the wireless LAN access point can be minimize to limit the signal availability within the substation. Normally, few seconds of delay can be tolerable for this application.

2.6 Smart Distribution Substation Feeder Protection Applications using WLAN

2.6.1 Distribution Feeder Overcurrent Protection

Low Voltage (LV) distribution feeder is normally protected by an overcurrent (Inverse Definite Minimum Time- IDMT characteristic) relays, as shown in Figure 2-10. This protection application is relatively less time critical as the fault current is not significant and IDMT overcurrent coordination always has a backup from upstream relays. The operating time of these relays varies from fraction of seconds to few seconds. Therefore, IEC 61850 standard part-5 has specified communication performance requirements to be 10 ms for SV and GOOSE messages. Therefore, the delay of around 20 ms is tolerable for this LV overcurrent protection scheme. Moreover, the sampling frequency required for this LV substation protection is around 480 Hz (8 samples per cycle), which demands less channel bandwidth. Hence, cost effective wireless LAN based network can be considered for this less time critical LV distribution feeder based on IEC 61850 standard. In addition to economical advantage, the wireless LAN is free from wiring-theft, which is important for the small un-manned remote distribution substation.

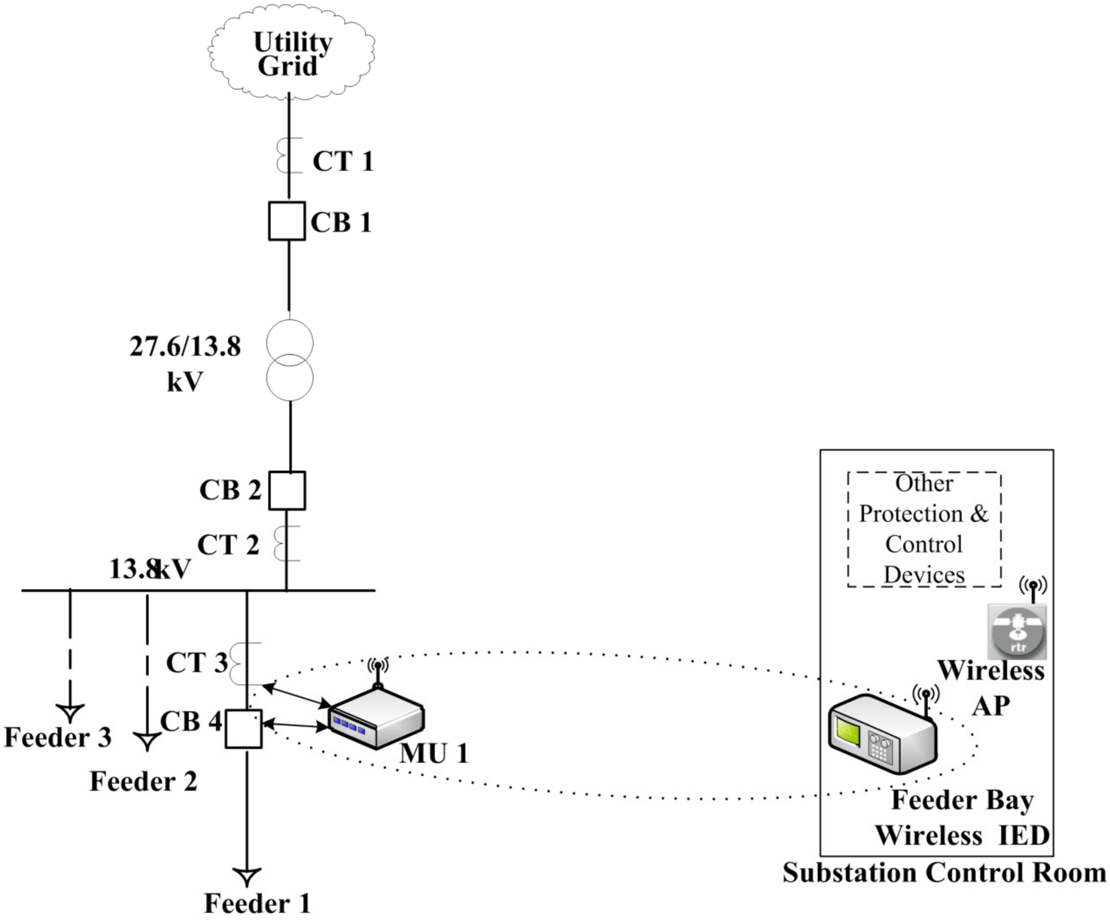


Figure 2-10 Wireless LAN for distribution feeder overcurrent protection

2.7 Microgrid Applications using WLAN

Microgrid is a cluster of various distributed energy resources (DERs), e.g. solar, wind, fuel cell, micro-turbine, diesel generator, battery systems etc., and sensitive loads. Seamless two-way communication plays an important role to accomplish operation and control functions of a microgrid, such as optimal control, protection, monitoring, metering, etc. Therefore, one of the ongoing research projects in this area is to explore the role of communication infrastructures, which include 1) international communication protocols, and 2) communication technologies, in order to achieve proper operation, control, and protection for a microgrid [74]. Information models and communication systems for various microgrid energy resources are standardized by International Electro-technical Commission (IEC) in IEC 61850 Part 7-420: Basic communication structure - Distributed energy resources logical nodes" [75]. As a communicaiton technology, by optimizing between installation cost and data rate requirements, wireless Ethernet (LAN) technology can be considered as one of the potential communication technologies for the microgrid applications. Main applications of wireless LAN for DERs in a microgrid is listed in Table 2-5 with corresponding IEC 61850 standardized message types and time delay performance requirements.

Table 2-5 Mapping of microgrid applications to corresponding IEC 61850 message types

Micro grid Applications	IEC 61850 Message Types	Time Delay Performance Requirements (in msec)
Control commands; State change	GOOSE (Type-1)	10
Protection functions	Sampled values (Type-4)	10
Condition monitoring	Low speed messages (Type-3)	100-5000
Data recording; Settings	File transfers (Type-5)	1000-5000

The control commands or any state change in a DERs should be directly communicated to Micro-Grid Central Control (MGCC), therefore, fast GOOSE (Generic Object Oriented Substation Event) message (with higher priority) are used for this microgrid application. For protection related applications, the analog signals (from instrument transformers) are digitized in Merging Units (MUs) and sent it to corresponding DER IEDs (Intelligent Electronic Devices). This type of stream of digitized measured values are categorized as Sampled Values (SV) in IEC 61850 standard. Most of the monitoring applications can have message delay of more than 100 ms according to IEC 61850 standard, therefore, condition monitoring application is considered as low speed messages over wireless LAN. Finally, file transfers from local DER IEDs to MGCC server for various data recordings, settings, achieving can be categorized as Type-5 of IEC 61850 messages which has requirements of 1000 to 5000 ms.

2.8 Applications between DAS and DER using WLAN

Distributed Energy Resources (DERs), such as, renewable energy sources (solar, wind), electric vehicle, battery, diesel generators, etc. are slowly proliferating on the distribution grid network. These DERs may have a grid interconnection to feed excess power. There are several challenges to distribution feeder protection scheme. And, therefore, it is recommended to island the DERs during the fault over the distribution feeder. Wireless technology is used already in use as a transfer-trip. With the advancement in IEC 61850 standard part7-420, it is possible to use wireless LAN point-to-point link between distribution automation system and distributed energy resources, as shown in Figure 2-11.For rural area distribution system with more dispersed DERs, it is not economical to deploy fiber-optic communication. Hence, wireless communication technologies are more feasible. The protection, control, monitoring, and metering between DAS and DERs have been studied in reference [76].

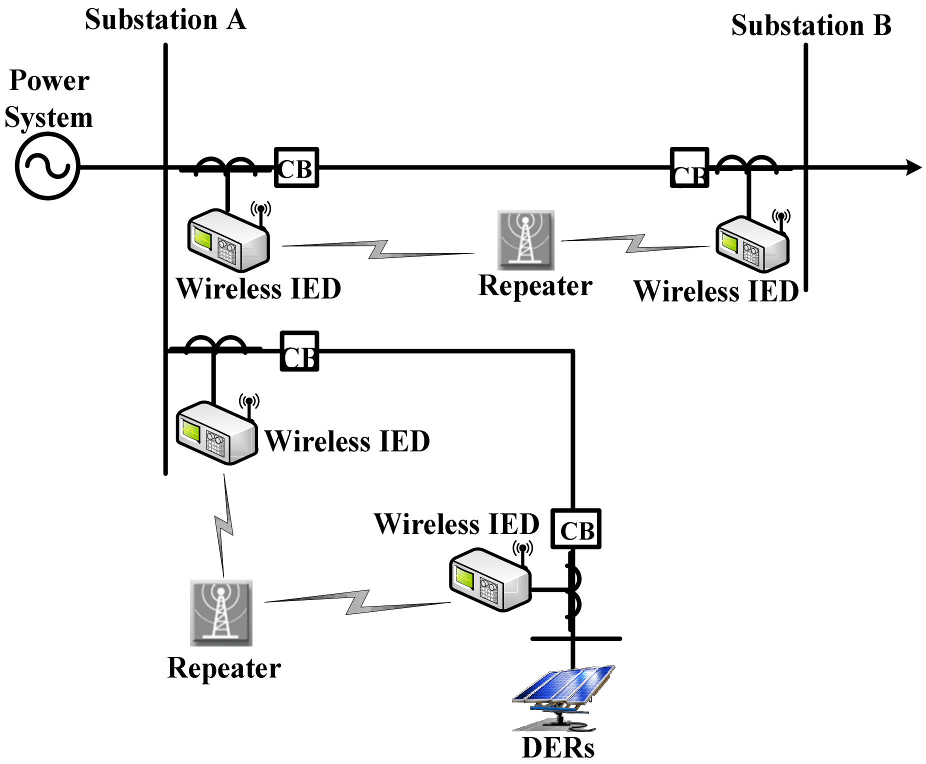


Figure 2-11 Wireless LAN communication between DAS and DERs

2.9 Summary

This chapter provided a brief introduction about IEC 61850 standard and IEEE 802.11 Wireless LAN standard. Application of wireless LAN based communication network for various smart distribution networks is presented and explained in detail. Following Table 2-6 summarizes various smart distribution substation applications with corresponding IEC 61850 message type (based on application requirements), and allowed ETE delay with suggested QoS priority levels.

Table 2-6 Performance requirements for smart distribution applications

Smart distribution substation applications	IEC 61850 Message	Allowed ETE delay at distribution (ms)
Control & Monitoring		
Automatic Capacitor Bank Control	GOOSE	500-1000
LTC Control and Monitoring	GOOSE	250-500
Fast Transfer Trip Scheme for Bus	GOOSE	400-500

Automation & Metering Application		
Watt/VAR Measurement	IP messages / Sample Values	1000-5000
Centralized IED Configuration	IP messages	1000-10000
Protection		
Feeder Over current Protection	Sample Value & GOOSE	20

One of the major challenges of wireless network implementation is EMI/RF interference present in to the substation site. For that reason, detail real filed noise substation noise measurement and analysis will be presented in next chapter.

Chapter 3

3. Noise Measurement in Electrical Substation Environment

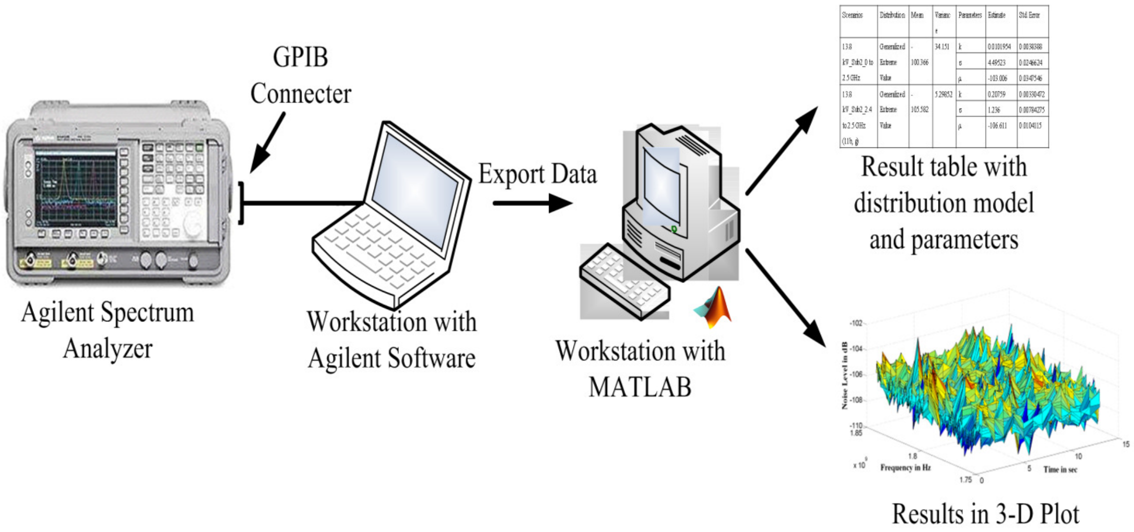
Most of the power distribution substations in North America are air-insulated (located in an open environment), with several types of equipment present at the site. The performance of wireless communication channels is influenced by atmospheric noise (mainly due to surrounding radio devices) and Electromagnetic interferences (from switching operations of substation switchgears), especially for Air Insulated Substations (AIS). In order to realize the identified smart distribution substation applications by deploying WLAN IEC 61850 devices, it is important to conduct noise-level measurements within the WLAN channels (2.4 GHz and 5.8 GHz bands) during not only regular operation of the substation devices, but also during switching operation of the switchgears. This chapter presents the noise measurement experiments and analysis carried out at 13.8 and 27.6 kV distribution substations owned by London Hydro and Hydro One at London, Ontario, Canada.

3.1 Noise Measurement Setup

Two types of measurements were conducted in 13.8 kV and 27.6 kV distribution substations: 1) measurement of Electro-Magnetic Interference (EMI) from gap or insulation breakdown due to Circuit Breaker (CB) switching; and 2) measurement of Radio Frequency Interference (RFI) from surrounding wireless LAN devices.

3.1.1 **Agilent Spectrum Analyzer for Noise Measurements**

Figure 3-1 shows the flow of spectrum measurement and analysis carried out using an Agilent spectrum analyzer. The details of each component used for this noise measurement can be read in Appendix B.



Scenarios	Distribution	Mean	Variance	Parameters	Estimate	Std. Error
13.8 kV_Sub2_0 to 2.5 GHz	Generalized Extreme Value	-100.366	34.151	k	0.0101954	0.0038388
				σ	4.49523	0.0246624
				μ	-103.006	0.0347546
13.8 kV_Sub2_2.4 to 2.5 GHz (11b, g)	Generalized Extreme Value	-105.582	5.29852	k	0.20759	0.00330472
				σ	1.236	0.00784275
				μ	-106.611	0.0104015

Figure 3-1 Agilent spectrum analyzer and data flow

The spectrum analyzer that connected to a laptop through a GPIB connector allowed automatic and continuous collection of noise measurements into the Agilent software. This allowed installation of the spectrum analyzer very close to the switchgear during its switching without the need for human intervention. Upon completion of switching events, the spectrum analyzer results from the Agilent software were exported into comma-separated value (CSV) files. These result files were loaded into the MATLAB tool for further analysis. The results obtained from the spectrum analyzer included noise level (in dBm) over WLAN radio spectrums. Based on this information, 3-D plots were obtained to study noise distributed over WLAN bands at the time of measurement. Further analysis of noise measurements was carried out using the "DISTTOOL" of MATLAB to model the best-suitable probability distribution function (PDF) and to obtain the model parameters. This exercise was repeated covering WLAN bands (meaning 2.4 to 2.5 GHz, and 5.75 to 5.85 GHz) during distribution substation switchgear operations at full load current.

3.1.2 AirPcap Analyzer for Signal-to-Noise Ratio (SNR) Measurements

The network analyzer setup based on AirPcap and CACE Pilot software is shown in Figure 3-2. The details of each component used for this noise measurement are outlined in Appendix B.

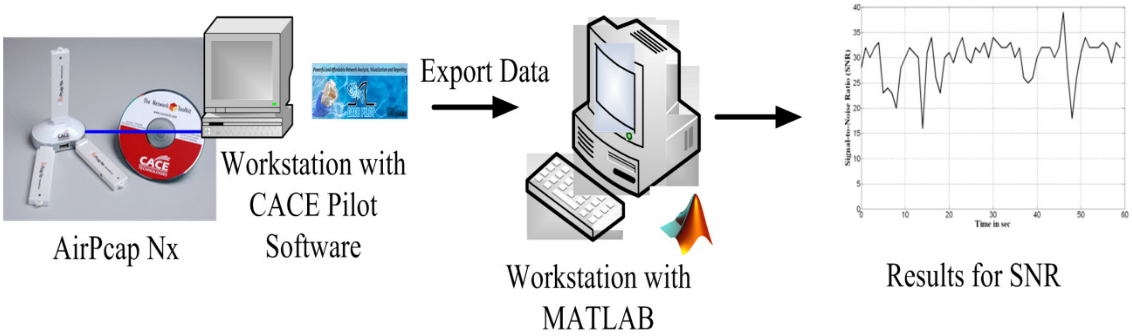


Figure 3-2 AirPcap setup with data flow

The AirPcap adapters with Pilot software allowed measurement of noise and signal levels over the WLAN channels. Based on these measurements, the Signal to Noise Ratio (SNR) in dB was calculated using equation (3-1).

$$\text{SNR [dB]} = 10 * \text{Log10} (S / N) \qquad (3\text{-}1)$$

Where, S = measured signal power [Watt] and N = measured noise power [Watt]

The noise level (in dBm) from Agilent spectrum analyzer and SNR (in dB) from AirPcap network analyzer are observed and plotted over the time for various 13.8 kV and 27.6 kV substations during CB (open/close) switching operations. The approximate CB opening and closing occurrence times are 5 and 9 seconds, respectively in following results.

3.2 Noise Measurement Results from 13.8 kV Substation 1

3.2.1 Test Setup in 13.8 kV Substation 1

Noise analysis was carried out at a 13.8 kV substation located in downtown London, ON. Full-load switching operations of 13.8 kV CB were performed for the noise measurement. Noise in both WLAN bands (2.4 to 2.5 GHz, and 5.75 to 5.85 GHz) was measured using the Agilent spectrum analyzer. At the same time, surrounding IEEE 802.11 networks (close to residential buildings) were studied using the AirPcap with CACE Pilot network analyzer. The following sections discuss the results of this test setup, and Figure 3-3 illustrates the setup close to the 13.8 kV CB during switching.

Figure 3-3 Test setup close to 13.8 kV CB at London Hydro distribution substation

3.2.2 **Results of 13.8 kV Substation 1**

The probability distribution function with the best-fit distribution curve of the noise data in the 2.4 GHz band is shown in Figure 3-4, and the parameters for the best-fit generalized extreme value distribution curve are tabulated in Table 3-1 Figure 3-4 shows the density curve of noise data measured during load disconnect operation on the 2.4 to 2.5 GHz bands. Most of the time, the noise level was between -108 and -105 dBm, however, the maximum measured noise level was as high as -52 dBm. Mean and variance values for the generalized extreme value distribution are specified in Table 3-1.

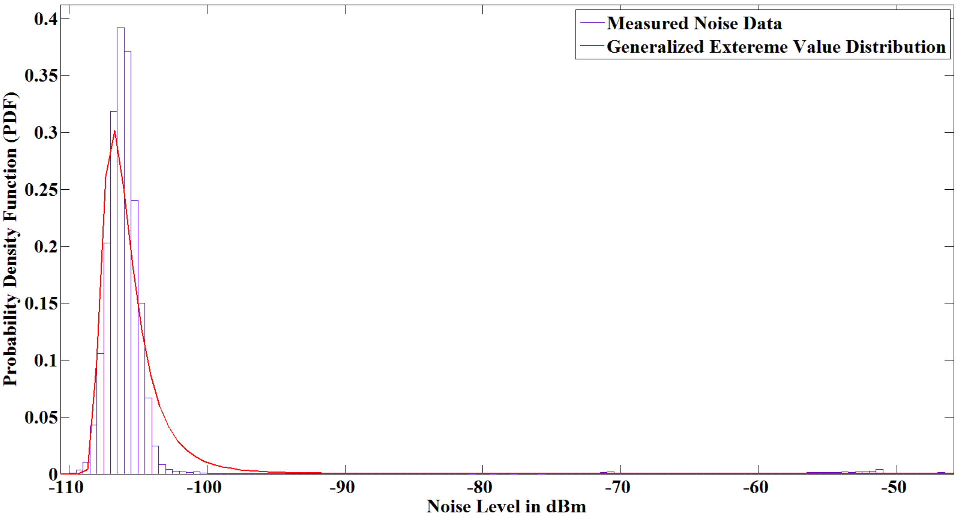


Figure 3-4 PDF of noise measurement data in 2.4 GHz band

Probability density function of the noise data measured in the 5.75 to 5.85 GHz bands is shown in Figure 3-5. Noise level was well within range of -110 to -104 dBm. As a result, normal Gaussian distribution was the best fit for this measured noise data.

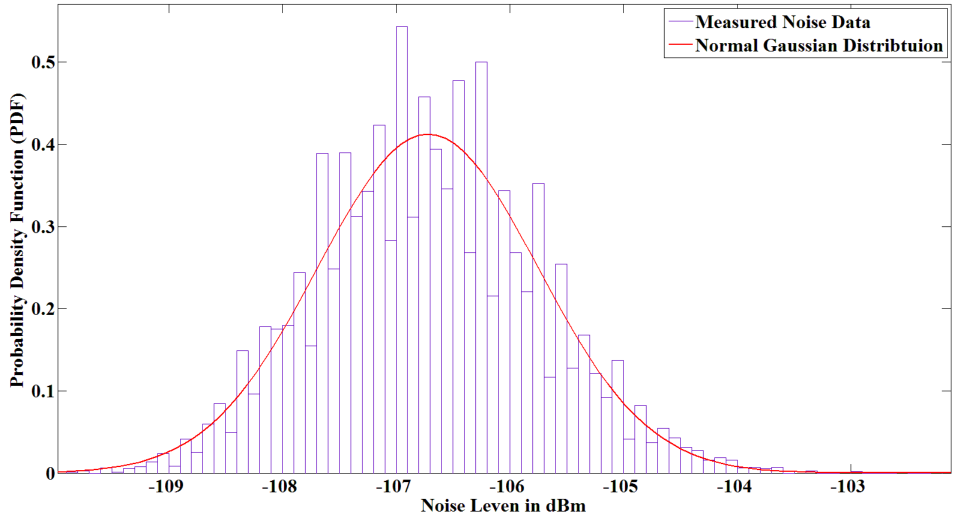


Figure 3-5 PDF of noise measurement data in 5.8 GHz band

Table 3-1 Distribution values and standard error for the measured noise data

Scenarios	Distribution	Mean	Variance	Parameters	Estimate	Std. Error
2.4 to 2.5 GHz band	Generalized Extreme Value	-105.582	5.29852	k	0.20759	0.00330472
				σ	1.236	0.00784275
				μ	-106.611	0.0104115
5.75 to 5.85 GHz band	Normal Gaussian Distribution	-106.721	0.93732	Mu	-106.721	0.00849126
				Sigma	0.968153	0.00600458

A 3-D plot featuring Time, Frequency and Noise level) for the 802.11b and g frequency bands is shown in Figure 3-6. Due to the data transfer from the other sources in the same channel, the 2.42 to 2.44 GHz band noise level increased to some -60 dB for some random interval of time, while for rest of the frequency 2.44 to 2.5 GHz band the noise level was -110 dB. Figure 3-7 shows the 3-D plot of the 5.75 to 5.85 GHz band. It shows that noise level was lower, in the range of -110 to -102 dB for the entire band.

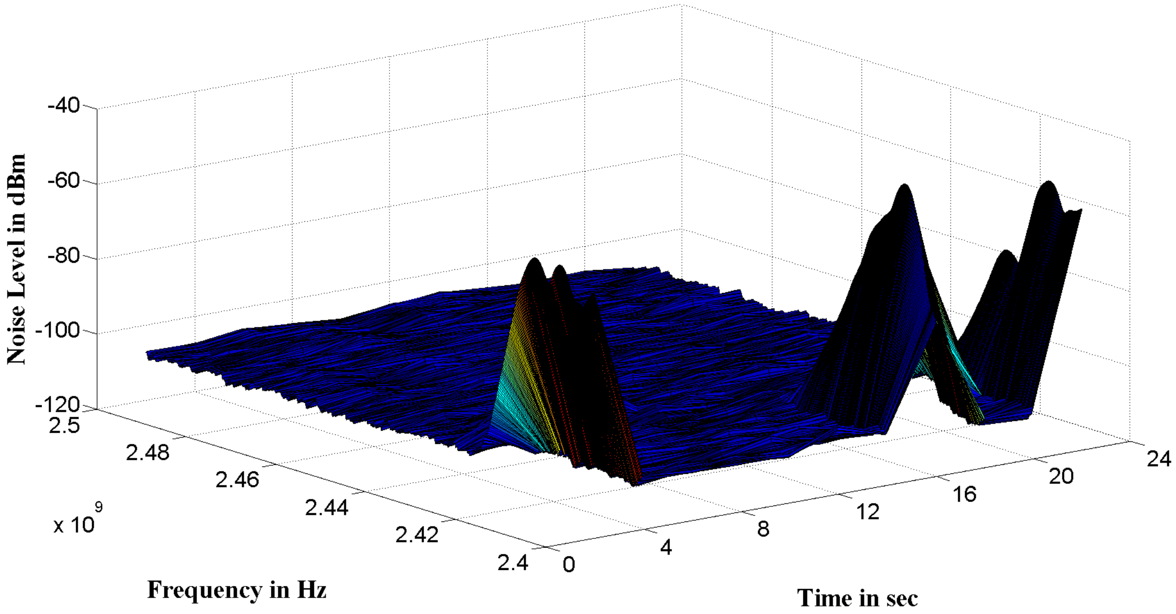


Figure 3-6 3-D Plot for 2.4 GHz band

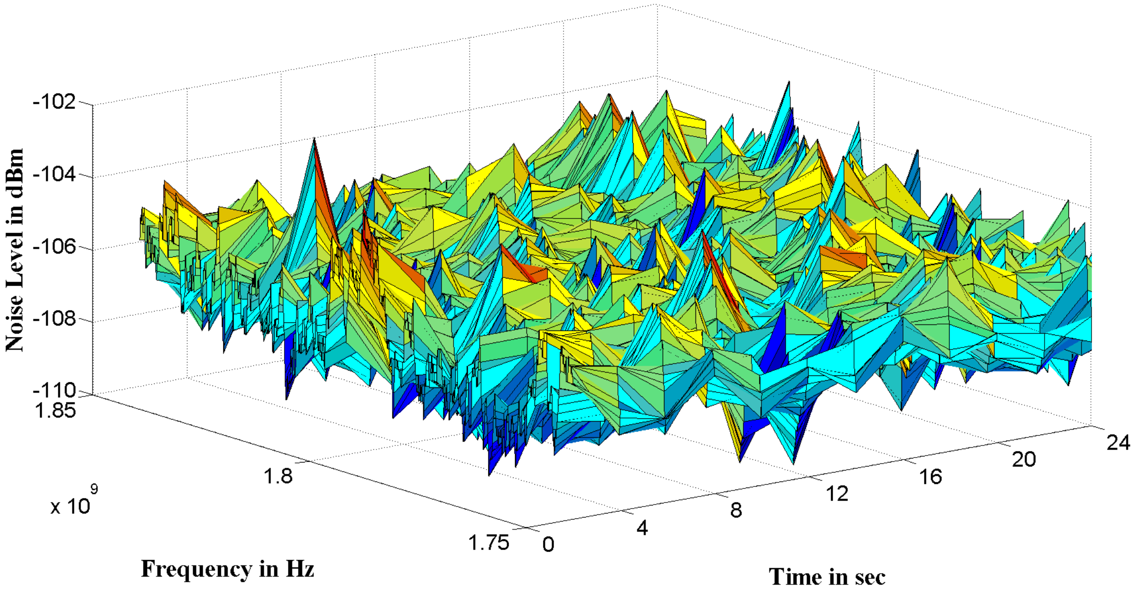


Figure 3-7 3-D Plot for 5.8 GHz band

Figure 3-8 shows SNR measured in the 2.4 GHz frequency band, for which the switching operation of the CB occurred at approximately 12 seconds. The minimum SNR value was

10 and maximum SNR value was 18. Therefore, the range of SNR was not good signal strength. The weakness in SNR was due to the fact that this 13.8 kV substation was located in downtown London and close to residential buildings. Numerous wireless APs over the 2.4 GHz frequency band were detected using the network analyzer. On the other hand, none of the wireless APs identified were in the 5.8 GHz frequency band, and hence, Figure 3-9 shows that the SNR was within the 38 to 44 dB range.

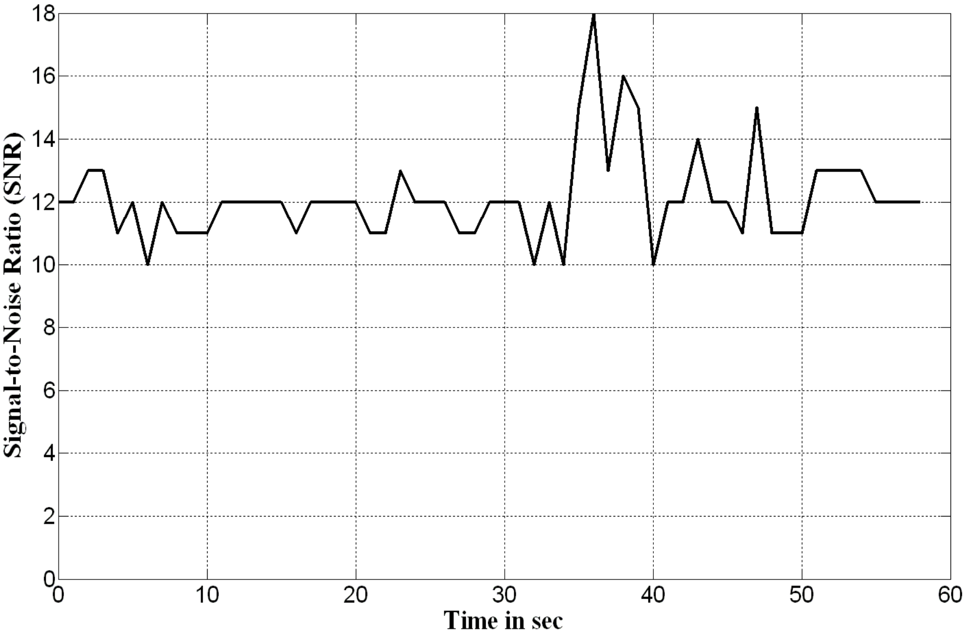


Figure 3-8 SNR in 2.4 GHz frequency band at 13.8 kV substation

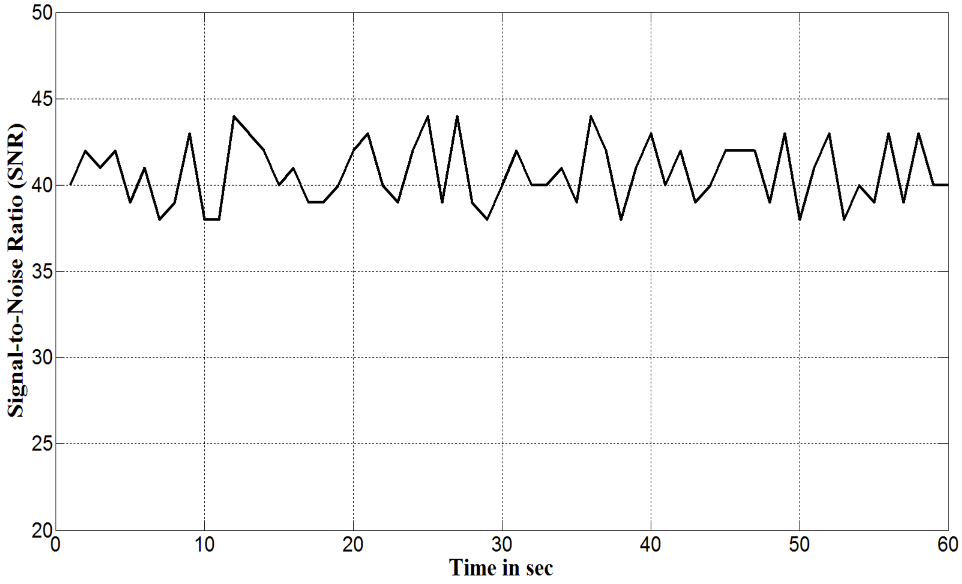


Figure 3-9 SNR in 5.8 GHz frequency band at 13.8 kV substation

3.3 Noise Measurement Results from 13.8 kV Substation 2

3.3.1 Results of 13.8 kV Substation 2

Figure 3-10 shows the PDF of noise data measured in the 802.11a band at 13.8 kV distribution substation location 2. The noise distribution value in the 5.8 GHz frequency band fit the Gaussian normal distribution. The noise level was almost negligible in the 5.75 to 5.85 GHz 802.11a band.

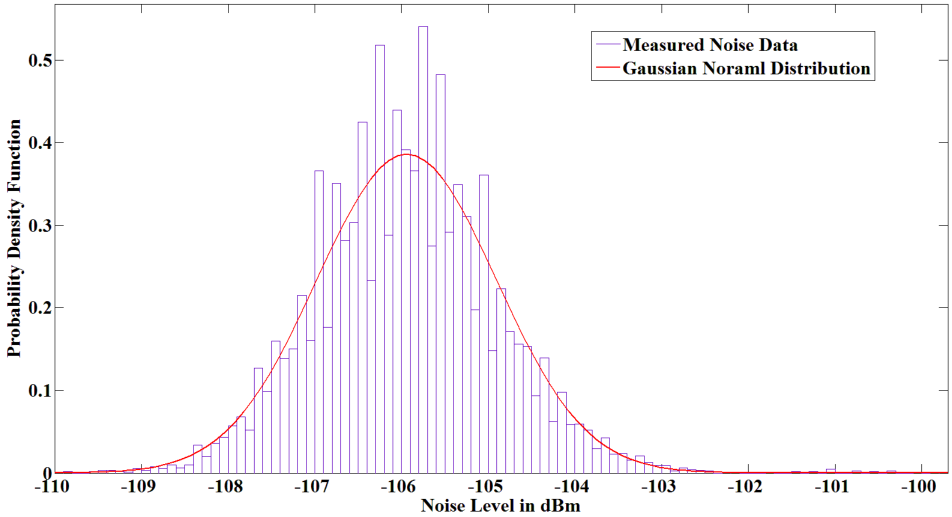


Figure 3-10 PDF of noise data in IEEE 802.11a band

Figure 3-11 shows the PDF for the measured noise data in 802.11b and g bands during switching operation. The figure shows that for the majority of the time, measured noise data was within the range of -110 to -100 dB. But, due to the effect of other traffic transmitting on same channels, the noise level measured at 2.4 to 2.5 GHz reached a maximum up to -75 dBm. Based on this measured data, the generalized extreme value distribution was the best fit for this set of data.

Table 3-2 Distribution values and standard error for the measured noise data

Scenarios	Distribution	Mean	Variance	Parameters	Estimate	Std. Error
2.4 to 2.5 GHz band	Generalized Extreme Value	-104.323	26.1828	k	-0.0421698	0.00448472
				Sigma	4.20254	0.0262508
				Mu	-102.58	0.0375714
5.75 to 5.85 GHz band	Normal Gaussian Distribution	-106	1.06	μ	-106	0.00905646
				σ	1.0326	0.00640425

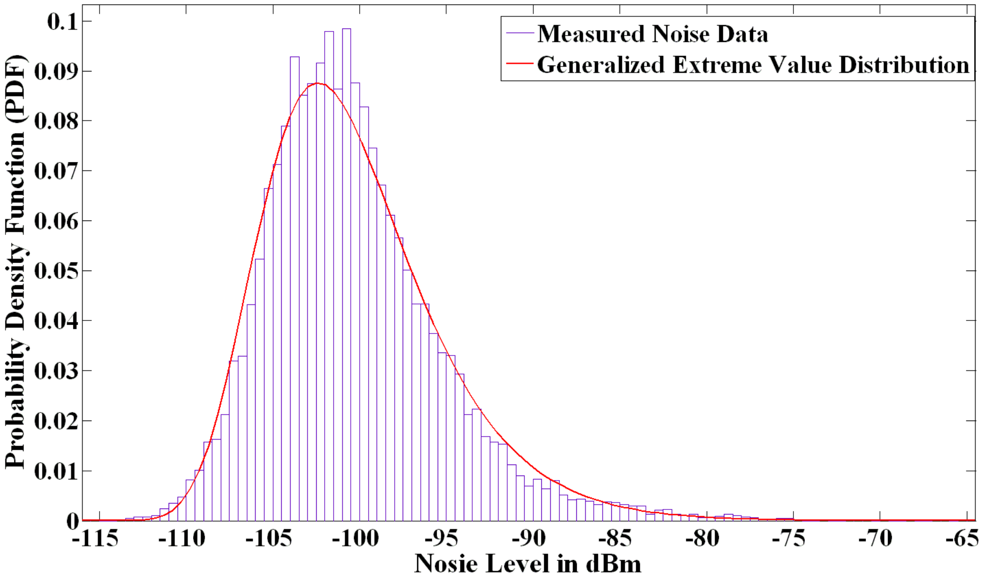


Figure 3-11 PDF of noise data in IEEE 802.11b and g bands

Figure 3-12 shows a time versus frequency noise-level plot for the 802.11b and g bands. Due to data transfer on the same channel from the different host at the same time, channel 1 and 3 bands measured higher noise level compared to the rest of the channel in this band. It is clear from the figure that for the band 2.44 to 2.5 GHz, the noise level was very low at around -110 dB. For the 2.4 to 2.44 GHz band, due to other sources sending signals on the same band, the noise level was higher, up to -70 dBm.

For the 802.11a (5.8 GHz) bands measured, the noise level was low, below -100 dB. No significant amount of noise was measured in these bands during normal or switching operations.

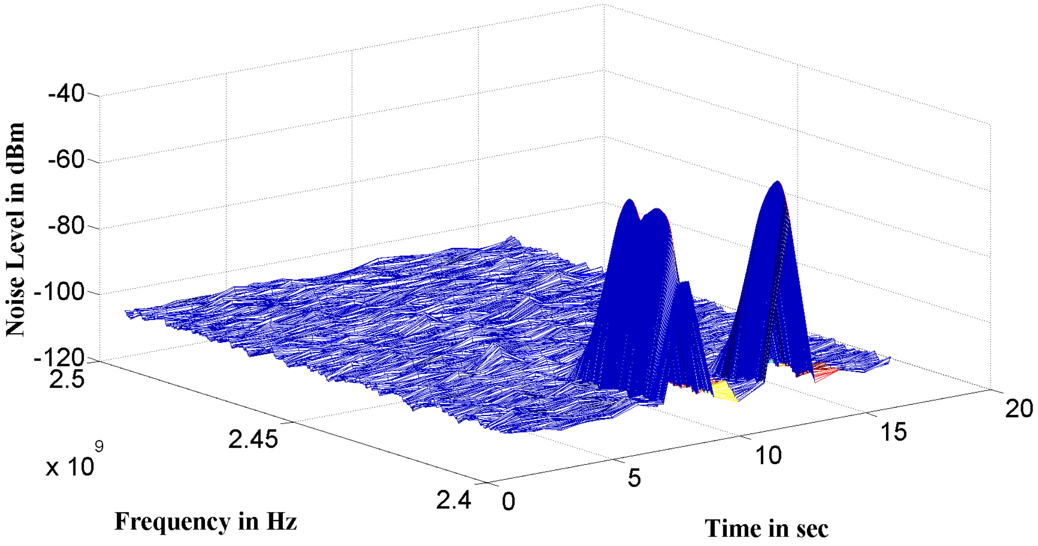


Figure 3-12 3-D plot for the 802.11b and g bands

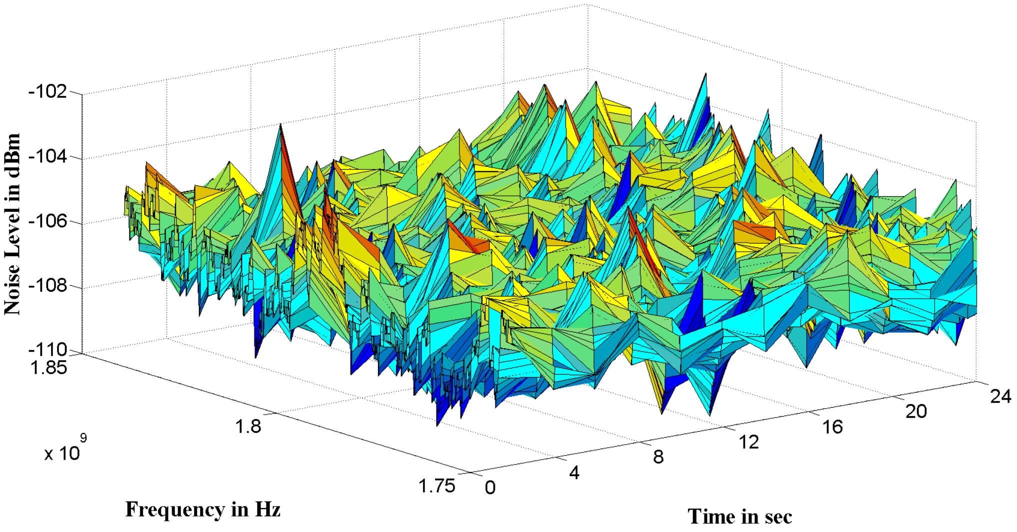


Figure 3-13 3-D Plot for the 802.11a band

Figure 3-14 shows the average SNR value of the 802.11 wireless channels for 13.8 kV distribution site 2 (CB operated at approximately 17 seconds). The SNR was 16 to 38, which is considered a good value for reliable signal communication.

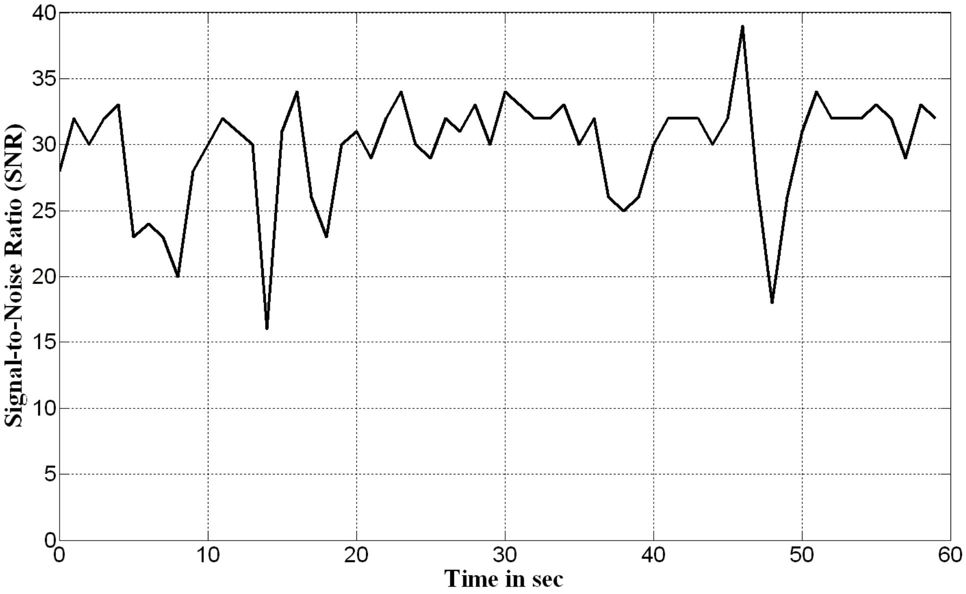


Figure 3-14 Average SNR of the 802.11b and g (2.4 GHz) band

3.4 Noise Measurement Results from 27.6 kV Substation 1

3.4.1 Setup in 27.6kV Substation 1

Noise measurements were taken at London Hydro 27.6 kV distribution substations. The first one was situated at Buchman substation and the other location within the city, the Southdale and Wonderland substation. Buchman substation had a SF6 circuit breaker with load current of 240 Amp. Southdale substation had an oil circuit breaker with 170 Amp of load current. All three test setups described in section 3.5 were conducted at both locations. Only one load disconnection switching operation was performed during these tests. The spectrum of 2.4 GHz was observed with the Agilent network analyzer. The AirPcap network analyzer observed all 802.11g channels and 802.11a channel 36. Results on these tests are discussed in the following section. Figure 3-15 shows the setup at Buchman substation.

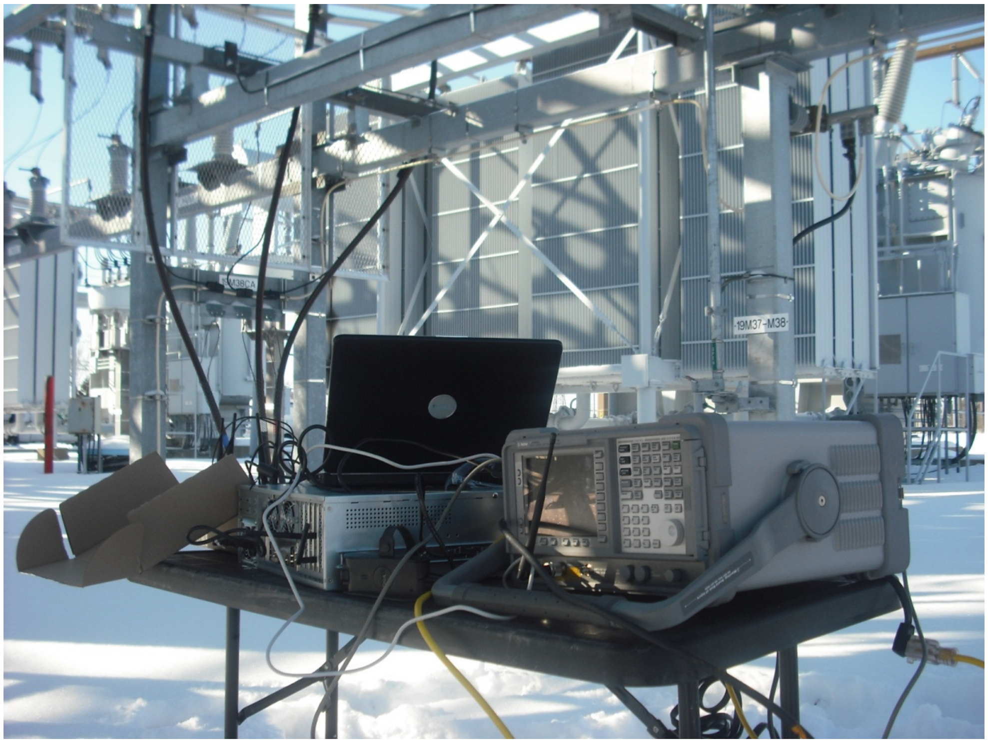


Figure 3-15 Setup at 27.6 kV distribution substation site

3.4.2 Results of 27.6 kV Substation 1

For the probability distribution function and its best fit distribution curve for the measured noise data in the 2.4 GHz band, the generalized extreme value distribution applied.

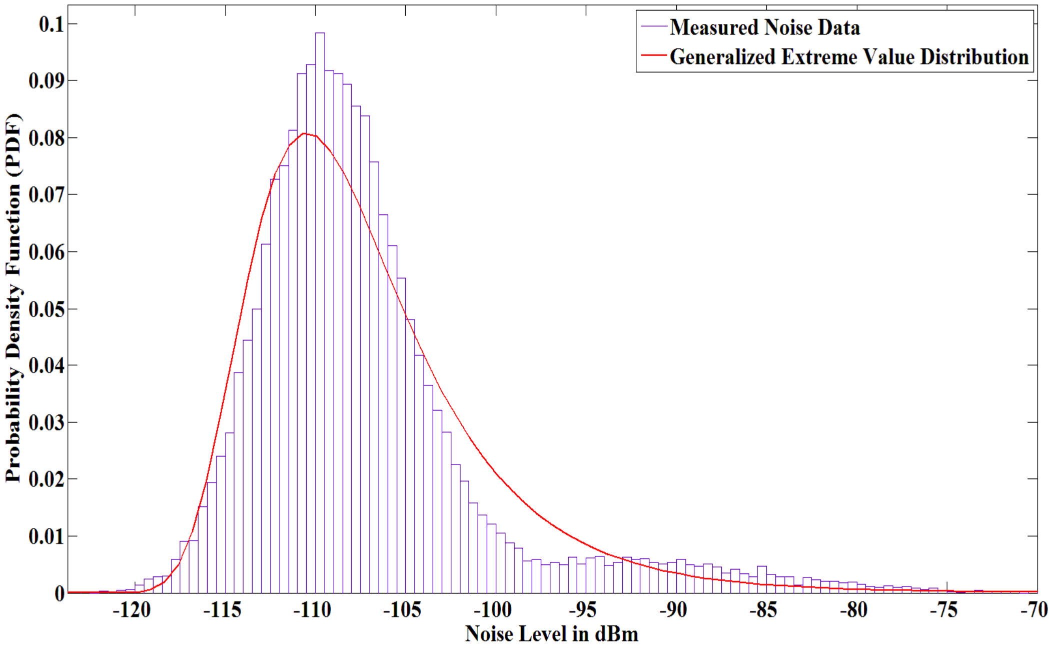


Figure 3-16 PDF and distribution curve fitting for 2.4 GHz frequency band

Figure 3-17 shows the 3-D plot for the noise data measured during the switching event in the 2.4 GHz frequency band. The noise level was low at higher frequency, around -110 to -100 dBm. However, the maximum noise level measured was -72 dBm.

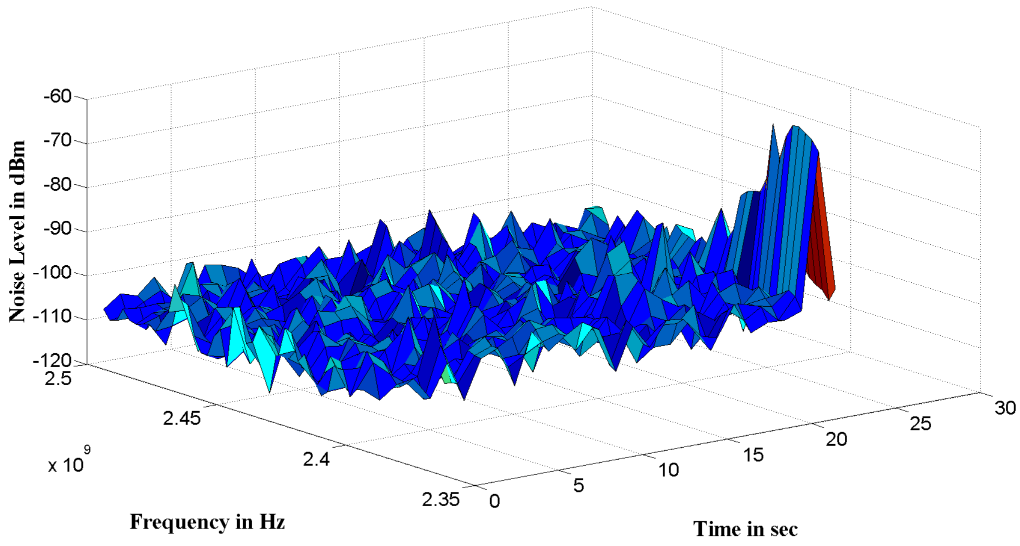


Figure 3-17 3-D plot for 2.4 GHz frequency band

The normal Gaussian value distribution was the best-fit probability distribution function for the IEEE 802.11a band, as shown in Figure 3-18. Mean, variance, and other distribution parameters are specified in Table 3-3.

Table 3-3 Distribution values and standard error for the measured noise data

Scenarios	Distribution	Mean	Variance	Parameters	Estimate	Std. Error
2.4 to 2.5 GHz band	Generalized Extreme Value	-107.21	41.8209	k	0.0694097	0.00341035
				Sigma	4.56084	0.0212235
				Mu	-110.178	0.0293178
5.75 to 5.85 GHz band	Normal Gaussian Distribution	-106.721	0.93732	μ	-106.721	0.00849126
				σ	0.968153	0.00600458

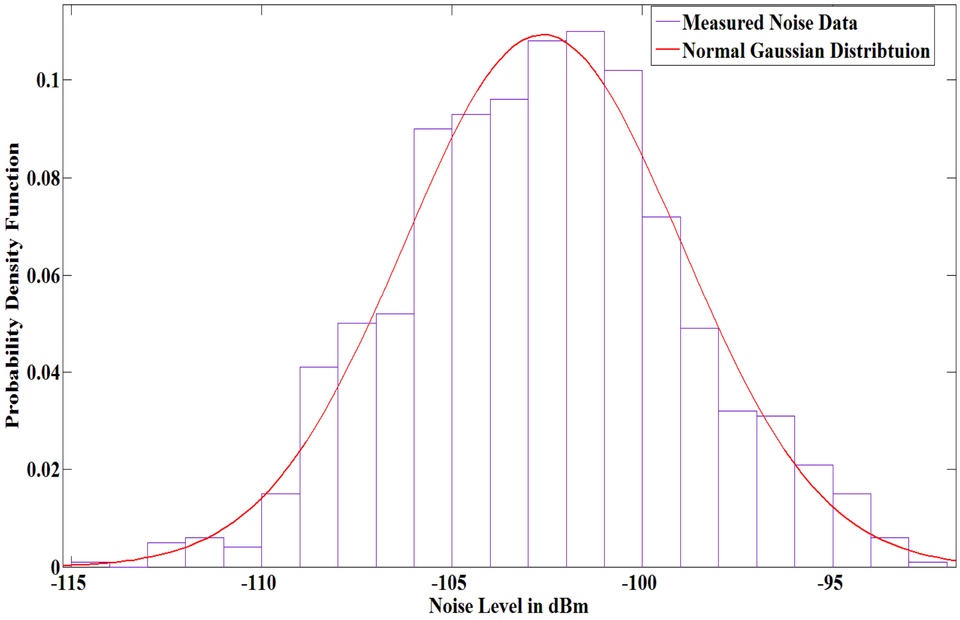


Figure 3-18 PDF of noise measurement data in 802.11a band

Figure 3-19 shows the 3-D plot for the noise data measured during the switching event in the IEEE 802.11a frequency band. The noise level was low at higher frequency, at around -110 to -104 dB.

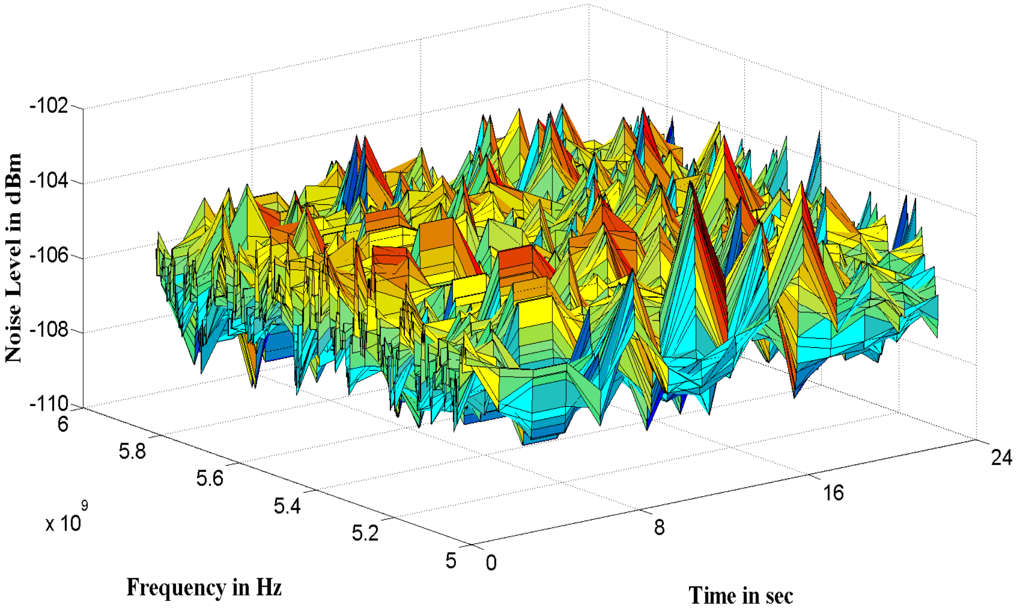


Figure 3-19 3-D plot for 802.11a band

Figure 3-20 shows the signal-to-noise ratio measured at the 27.6 kV substation site within the 2.4 GHz frequency band (CB operated at around 15 seconds). The minimum SNR value was 15 dB, which is considered a good environment for signal transfer.

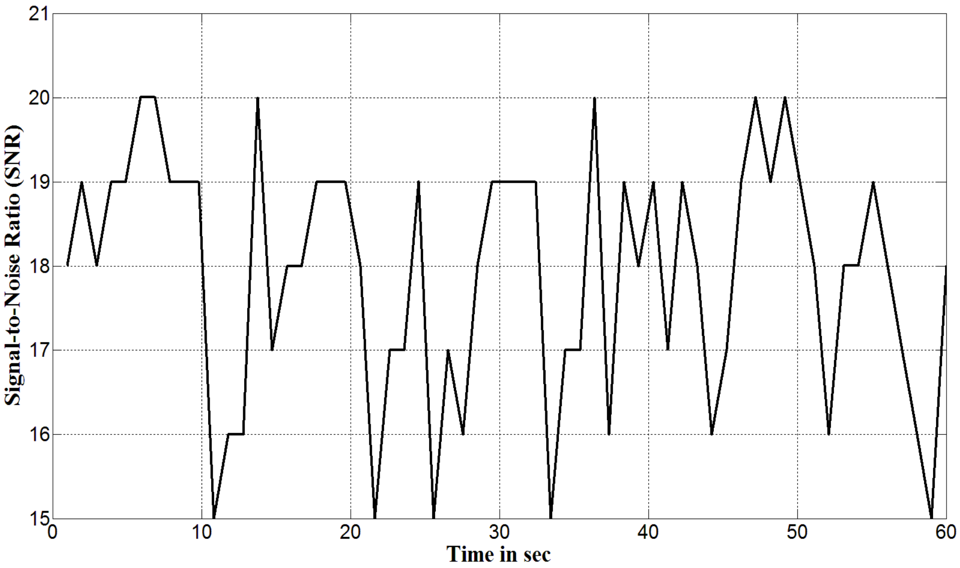


Figure 3-20 SNR ratio for 27.6 kV substation site in 2.4 GHz frequency band

3.5 Noise Measurement Results from 27.6 kV Substation 2

3.5.1 Results of 27.6 kV Substation 2

Figure 3-21 shows the PDF and generalized extreme value distribution function of the measured noise data in the 2.4 GHz frequency band for oil-tank circuit breaker operation at full load. The distribution function parameter and standard error is tabulated in Table 3-4.

Table 3-4 Distribution function parameters for the 27.6 kV substation

Scenarios	**Distribution**	**Mean**	**Variance**	**Parameters**	**Estimate**	**Std. Error**
2.4 to 2.5 GHz; oil tank CB operation	Generalized Extreme Value	-105.62	35.870	k	0.028369	0.0034905
				σ	4.49278	0.022019
				μ	-108.35	0.031033

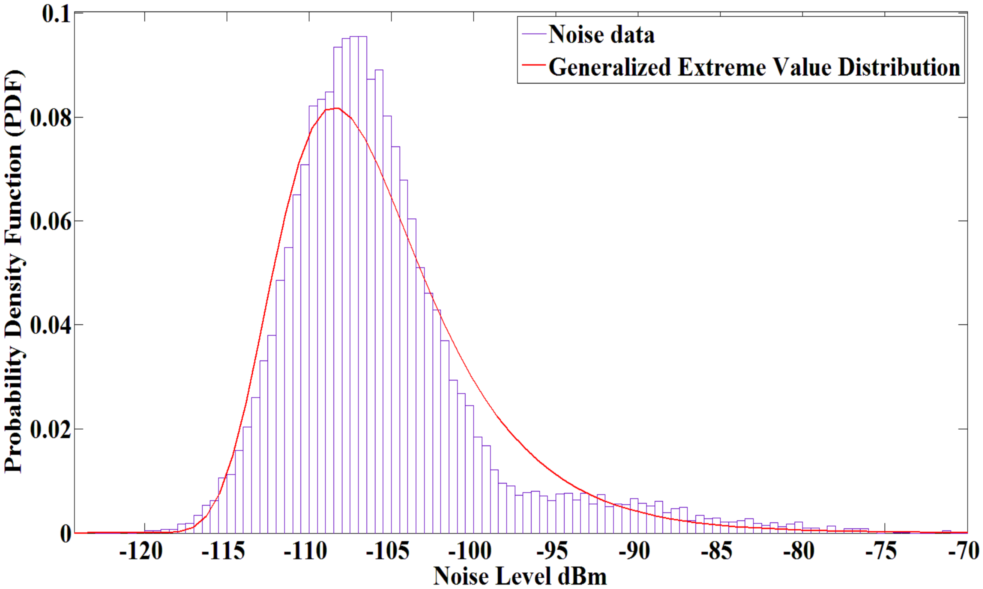


Figure 3-21 PDF and distribution function of noise level in 2.4 to 2.5 GHz band

Figure 3-22 shows the 3-D view of the measured noise data in the 2.4 GHz band during switching operation (at approximately 12 seconds). The figure shows that the noise level was as high as -80 dBm. This was due to interference from the other communication protocol using the same channel to transfer data.

Figure 3-23 shows the average SNR for the 802.11 wireless channels. The SNR was between 14 and 28 dB, with an average of 20 dB, which is considered good for reliable signal transmission.

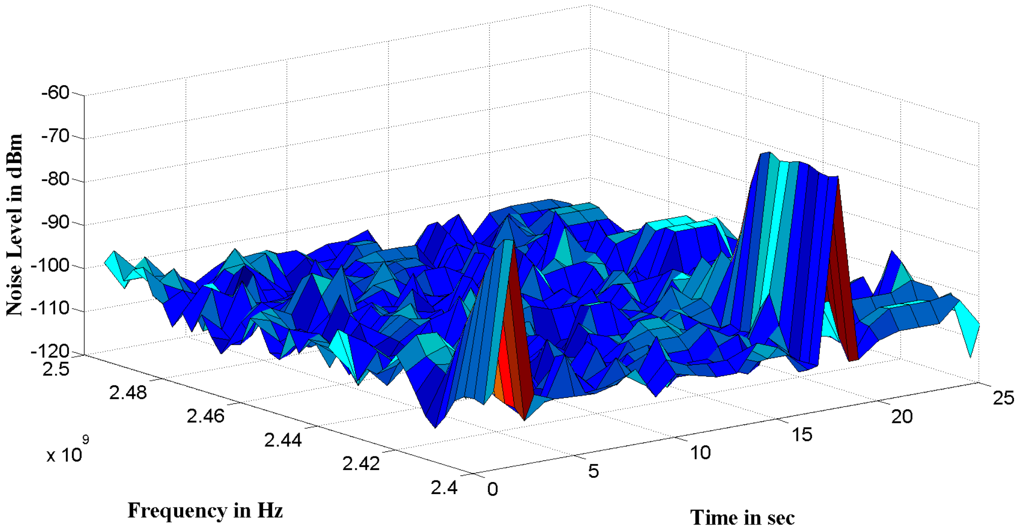


Figure 3-22 3-D view of frequency, time, and measured noise level

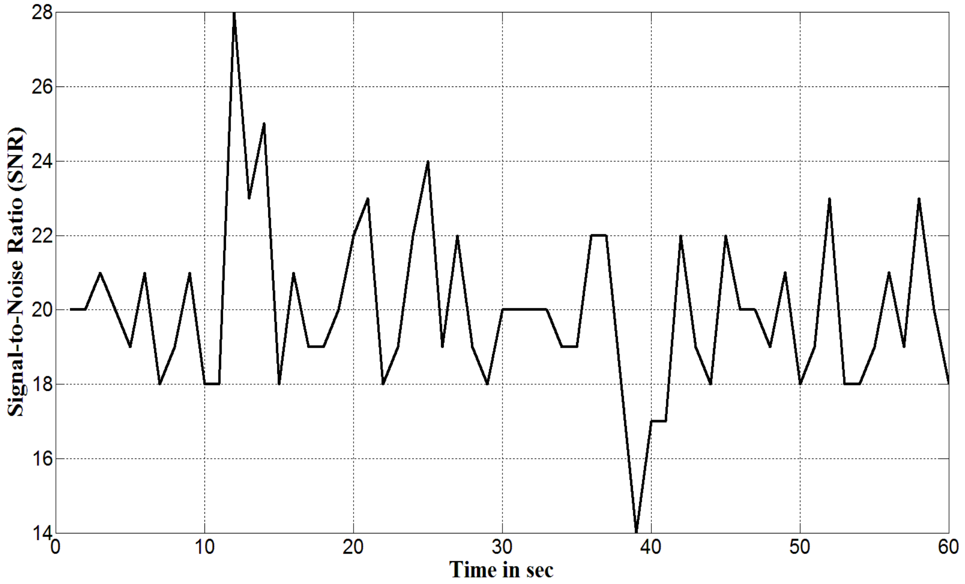


Figure 3-23 Average SNR value for 802.11 wireless channel

3.6 Noise Measurement at 27.6 kV Isolator Switch Operation

In addition to noise measurements during circuit-breaker switching operation, this station was subject to noise measurements during isolator switching. Figure 3-24 shows the field setup of spectrum and network analyzers installed in the vicinity of the isolator switch to be operated.

Figure 3-24 27.6 kV substation setup close to isolator switch in switchyard

The probability distribution function modeled for this event was the generalized extreme value distribution within the 2.4 GHz frequency band, as shown in Figure 3-25. Table 3-5 shows the parameters of generalized extreme value distribution function obtained from the MATLAB. The mean value of noise observed at this substation was -86 dB.

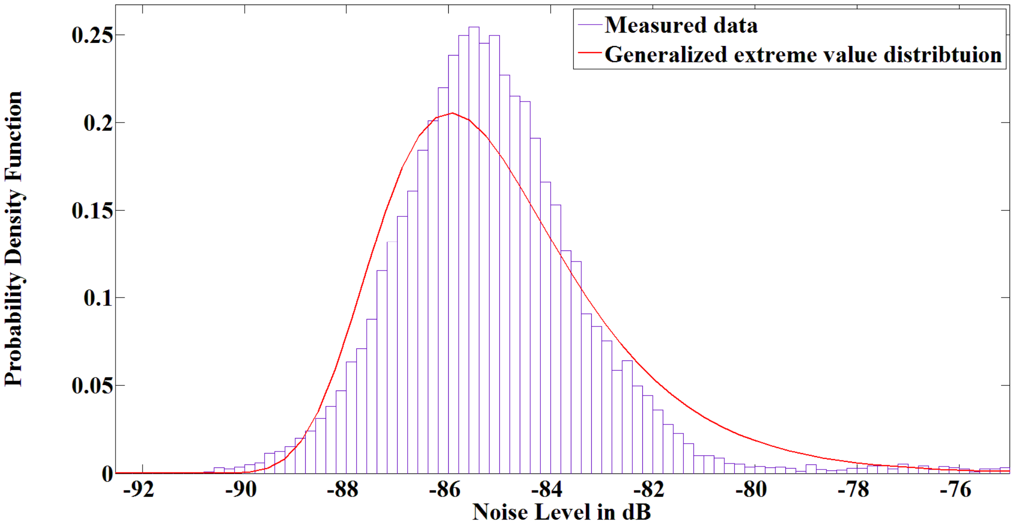


Figure 3-25 PDF and distribution function of noise level for 2.4 to 2.5 GHz band

Table 3-5 Distribution function parameters for the 27.6 kV substation

Distribution	**Mean**	**Variance**	**Parameters**	**Estimate**	**Std. Error**
Generalized Extreme Value	-88.9986	5.08394	k	0.0142539	0.00239074
			σ	1.079045	0.0081001
			μ	-86.0072	0.0119451

Figure 3-26 shows the 3-D plot of noise measurements through the isolator switching. The peak of noise observed was -75 dBm.

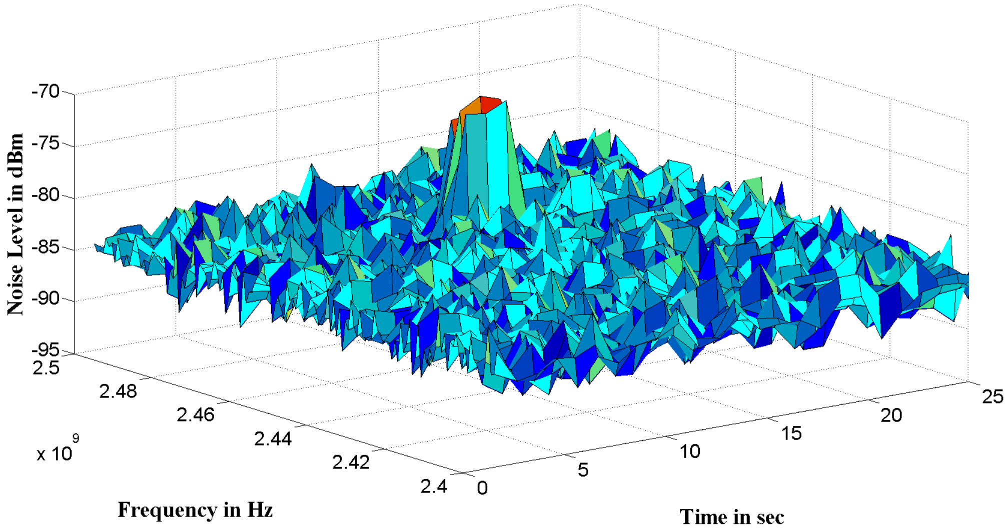


Figure 3-26 3-D view of frequency, time, and measured noise level

Figure 3-27 shows the SNR observed in WLAN channels during isolator switching. The lowest SNR observed in this substation was 13 dB, with an average of 18 dB.

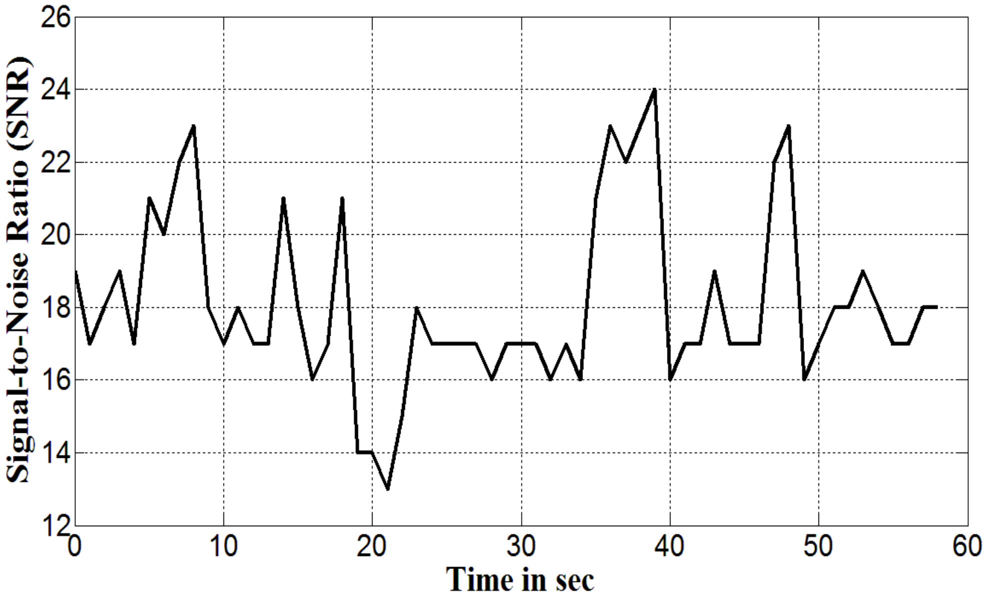


Figure 3-27 3-D view of frequency, time, and measured noise level

3.7 Summary

This chapter presented noise measurements in four distribution substations: two 13.8 kV substations and two 27.6 kV substations owned by London Hydro. The noise measurements included EMI measurements taken during switching operations at load currents using an Agilent spectrum analyzer and an AirPcap network analyzer. The results were presented in terms of 3-D plots (noise versus frequency versus time), probability distribution function (by modeling noise using MATLAB), and SNR (measured by network analyzer). It was observed that the EMI due to switching operation did not have any measurable noise within the 2.4 to 2.5 GHz and the 5.7 to 5.8 GHz frequency bands. Moreover, the SNR measured in the 13.8 kV substation 1 was very poor, as the substation was downtown (with dense network devices found in the 2.4 GHz band), however, there was no wireless AP detected in the 5.8 GHz band at any of these substations. The average SNR measured at the 27.6 kV substations (in the 2.4 GHz band) was comparatively higher.

The following chapter outlines how noise PDF modeled parameters were used further to simulate the substation environment noise using the industry-trusted tool, OPNET.

Chapter 4

4. OPNET Modeling of WLAN Automation Devices

In this chapter, the modeling and development of IEC 61850 based substation automation devices, such as protection and control IEDs and merging unit IEDs, are detailed. Configuration of various wireless LAN features, such as packet format and quality of service, as well as substation noise modeling, are described.

4.1 OPNET Tool

The OPNET Modeler simulation tool is considered to be the leading tool for the communication and networking industry and facilitates the design and study of communication networks, devices, protocols, and applications. It is based on a series of hierarchical editors that directly parallel the structure of real networks, equipment, and protocols.

OPNET supports model specification with a number of tools, called editors. These editors handle the required modeling information in a manner that is similar to the structure of real network systems. Therefore, the model-specification editors are organized hierarchically. Model specifications performed in the Project Editor rely on elements specified in the Node Editor. The rest of the editors are used to define various data models, links, nodes, and so on. This organization is described in the following sections.

4.1.1 Project Editor

The Project Editor is used to develop network models. Network models are made up of subnets and node models. This editor also includes basic simulation and analysis capabilities. It is the main staging area for creating a network simulation. You build a network model using models from the standard library, choose statistics about the network, run a simulation, and view results. It is also possible to create node and process models, build packet formats, and create filters and parameters, using specialized editors that you access from the Project Editor.

4.1.2 Node Editor

The Node Editor is used to develop node models. Node models are objects in a network model. They are made up of modules with process models. The Node Editor lets you define the behavior of each network object. Behavior is defined using different modules, each of which models some internal aspect of node behavior, such as data creation and data storage. A network object is typically made up of multiple modules that define its behavior.

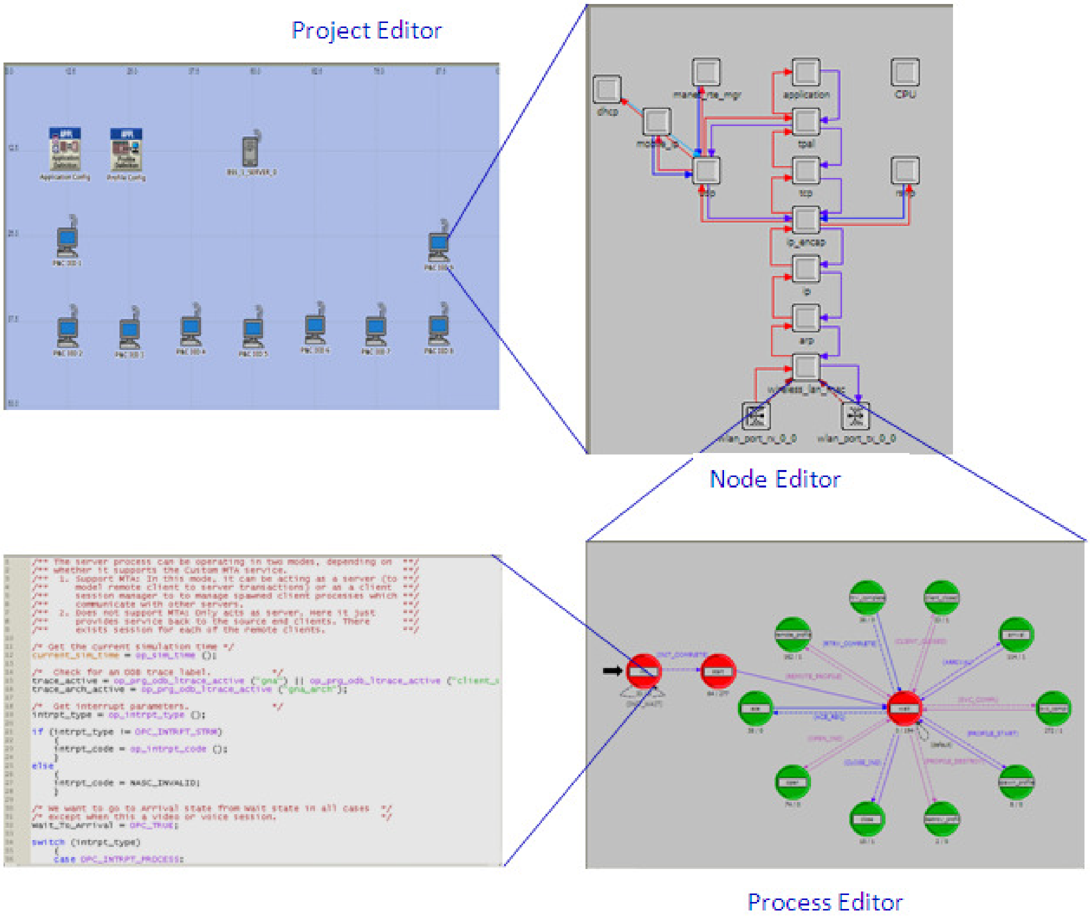
4.1.3 Process Editor

The Process Editor is used to develop process models. Process models control module behavior and may reference parameter models. They control the underlying functionality of the node models created in the Node Editor [55]. Process models are represented by Finite State Machines (FSMs) and are created with icons that represent states and lines that represent transitions between states. Operations performed in each state or for a transition are defined in embedded C or C++ code blocks.

4.1.4 Packet Format Editor

Packet format models are created using the Packet Format Editor. This editor defines the internal structure of a packet as a set of fields. A packet format contains one or more fields, represented in the editor as colored rectangular boxes. The size of the box is proportional to the number of bits specified as the field's size.

OPNET provides the most comprehensive open source library. Further, it is possible to develop any type of protocol or device model with OPNET process and node editors. The dynamic modeling of wireless substation automation devices and protocols are discussed in the following sections.



```
/** The server process can be operating in two modes, depending on **/
/** whether it supports the Custom MTA service.                      **/
/**   1. Support MTA: In this mode, it can be acting as a server (to **/
/**      model remote client to server transactions) or as a client  **/
/**      session manager to to manage spawned client processes which **/
/**      communicate with other servers.                             **/
/**   2. Does not support MTA: Only acts as server. Here it just     **/
/**      provides service back to the source end clients. There      **/
/**      exists session for each of the remote clients.              **/

/* Get the current simulation time */
current_sim_time = op_sim_time ();

/*  Check for an ODB trace label.              */
trace_active = op_prg_odb_ltrace_active ("gna") || op_prg_odb_ltrace_active ("client_s
trace_arch_active = op_prg_odb_ltrace_active ("gna_arch");

/*  Get interrupt parameters.                  */
intrpt_type = op_intrpt_type ();

if (intrpt_type != OPC_INTRPT_STRM)
    {
    intrpt_code = op_intrpt_code ();
    }
else
    {
    intrpt_code = NASC_INVALID;
    }

/* We want to go to arrival state from wait state in all cases  */
/* except when this a video or voice session.                   */
wait_to_arrival = OPC_TRUE;

switch (intrpt_type)
    {
    case OPC_INTRPT_PROCESS:
```

Figure 4-1 OPNET modeler

4.2 Modeling of Wireless Substation Automation Devices

Major devices to build wireless LAN for IEC 61850 based substation automation systems include intelligent electronic devices, merging units, and wireless Access Points (APs). This section outlines the modeling details of these devices to communicate in compliance with IEC 61850 functions.

4.2.1 **Intelligent Electronic Devices**

Figure 4-2 shows the dynamic model of an IED, particularly a Protection and Control (P&C) IED.

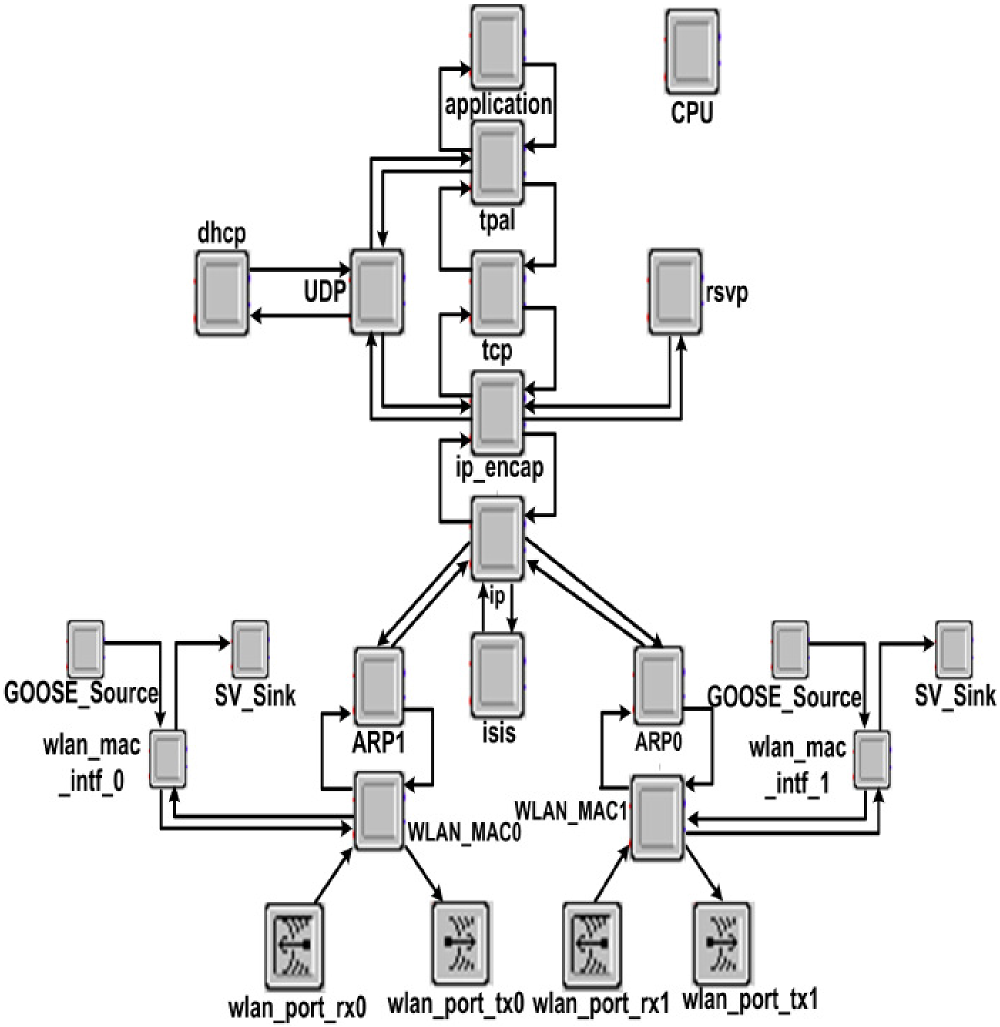


Figure 4-2 Modeling of IEDs in OPNET

IEDs should be capable of receiving sampled value packets (type 4) from an MU, sending GOOSE messages (type 1) to corresponding MUs and other P&C IEDs, and also client-server applications (type 2, 3, 5, 7) over TCP/IP, and time synchronization messages using UDP/IP. Although, the proposed IED model in Figure 4-2 has two Media Access Control (MAC) interfaces for wireless use, the developed model can support several wireless interfaces. The WLAN_MAC module models IEEE 802.11 CSMA/CA and related protocols. The GOOSE_Source module is capable of unicast, multicast, or broadcast GOOSE messages. The SV_Sink module receives the sampled values from MUs and calculates the end-to-end delays. All other types of messages can be configured to set the traffic flows in the application module to communicate over the OSI-7 layer stack using TCP/IP or UDP/IP.

4.2.2 **Merging Unit (MU)**

The functions of an MU are: 1) to send sampled value packets (type 4) to the subscribed P&C IEDs; and 2) to receive GOOSE messages (type 1) from corresponding P&C IEDs.

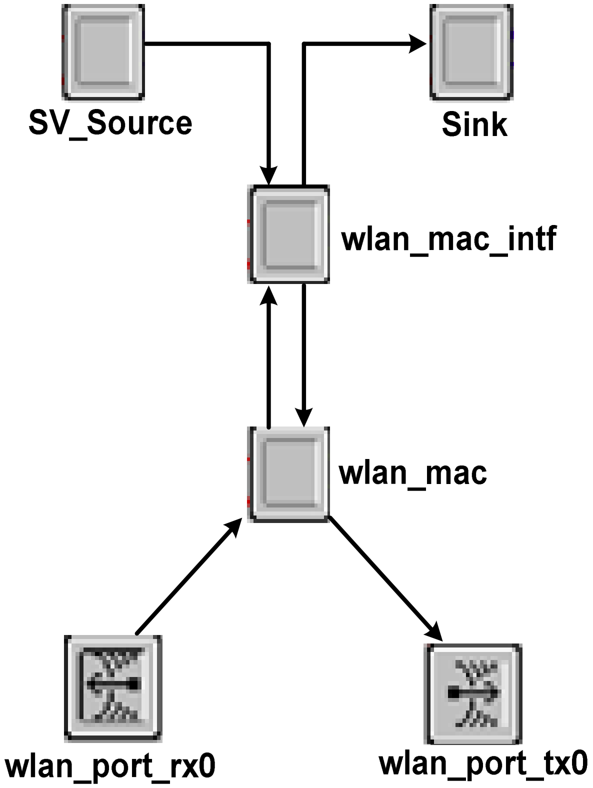


Figure 4-3 Modeling of MUs in OPNET

These two functions are mapped directly to the data link layer as shown in Figure 4-3. The SV_Source module generates the sampled value packet, whereas Sink receives GOOSE messages from the data link layer and calculates the delay.

4.2.3 Access Point (AP)

The access point architecture of WLAN has advantages over an ad-hoc architecture, including better security, quality of service, coverage, signal reliability, and power saving. Therefore, access point architecture is preferable for substation automation applications, although it is expensive as compared to ad-hoc. The functions of an AP in IEC 61850 based substation automation systems are: 1) provide Quality of Service (QoS); 2) reduce interference; 3) reduce collision; and 4) facilitate expandability. Figure 4-4 shows the model of wireless AP, which can also be connected with a wired Ethernet LAN. Although the figure shows two interfaces, this model can accommodate any number of wired and wireless interfaces. The standard OPNET library facilitates various system management, network configuration, security, and related modules.

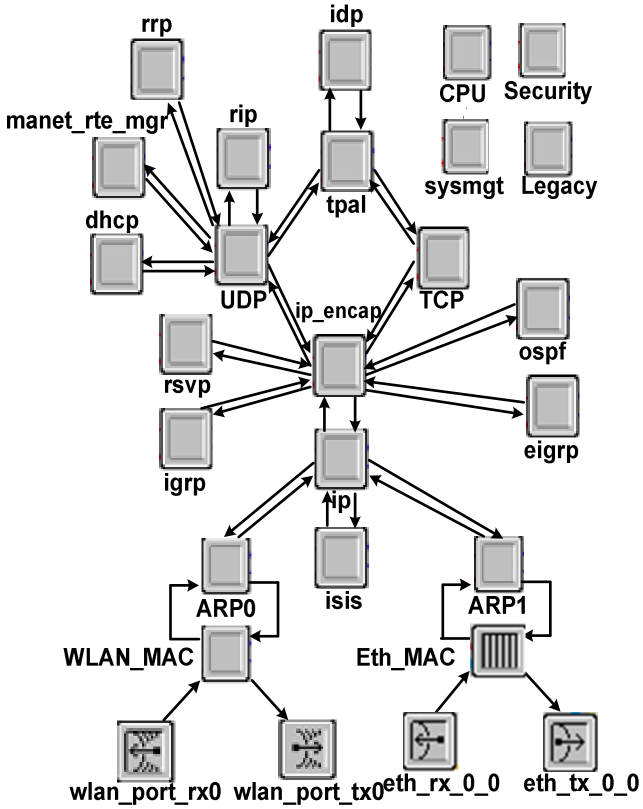


Figure 4-4 Access Point model in OPNET

4.3 Configuration of Wireless Packet Format and QoS

4.3.1 Wireless Packet Format in Compliance with IEC 61850

IEC 61850 provides a packet format only for the wired Ethernet (IEEE 802.3) protocol. On the other hand, the wireless Ethernet (IEEE 802.11) protocol's packet format is complex compared to IEEE 802.3 packet formats. The Packet Editor of OPNET allows for design of the IEEE 802.11 packet format in compliance with IEC 61850. Figure 4-5 shows the IEEE 802.11 data packet format for raw data sampled values compatible with the packet fields required by IEC 61850, for example the Application Protocol Data Unit (APDU) consists of many Application Services Data Units (ASDUs), QoS control, etc.

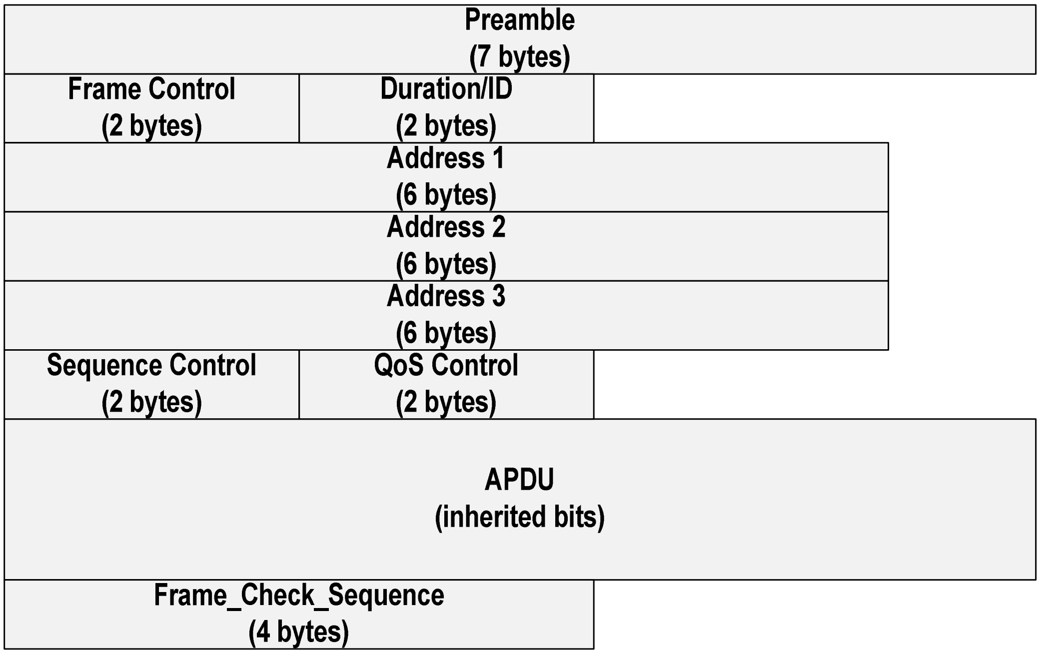


Figure 4-5 IEC 61850 based wireless packet format

The fields are explained as follows. The **frame control** field specifies the type of packet. Length of the fragmented packets is identified by the **duration/ID** field, for which the MAC packet format has three address fields each of 6 bytes. The **address** allocation contains source address, destination address, and transmitter or receiver address. Two bytes are allocated to **sequence control**. The first 4 bits are used for fragmentation and reassembly, and the remaining 12 bits are used to number frames sent between a given transmitter and receiver. The priority tagging for the data are set by the 2 bytes of the **QoS control** field, as explained in the following section. The **APDU** field consists of the 0-2312 bytes of data or fragment of the data. The structure of APDU is proposed in IEC 61850, and an APDU can include several ASDUs. Each ASDU contains three-phase-and-neutral voltages and currents from Voltage Transformer (VT) and Current Transformer (CT) respectively. Cyclic redundancy is checked by the 4 bytes of a **frame check sequence**.

4.3.2 Configuration of Priority Tagging to IEC 61850 Messages

The increasing popularity of wireless networks results in demand to transmit multimedia messages. This has brought more requirements to the network, creating a need for end-to-end QoS. Enhanced QoS support to the MAC is specified by IEEE 802.11e [77]. The first 3-bits of the 2-byte QoS field (as shown in Figure 4-5) are referred to as User Priority bits and allow the user to provide a total of eight (0-7) priorities to the time-critical messages according to IEEE 802.11e [78].

The enhanced QoS of 802.11e is achieved by defining a coordination function named Hybrid Coordination Function (HCF). The HCF incorporates different classes of frames with different priorities when accessing the radio channel. It can access the channel with or without contention. The contention channel access is facilitated by Enhanced Distributed Channel Access (EDCA). And, contention-free access is allowed by controlled channel access, referred to as the HCF-Controlled Channel Access (HCCA) mechanism. For contention-based channel access, EDCA defines the access category (AC) mechanism that provides support for the priorities at the stations. Each station can have up to four ACs to support eight User Priorities (UPs). One or more UPs are assigned to one AC [77]. A station accesses the medium based on the AC of the frame to be transmitted.

One additional attribute is added to the MAC of 802.11e based station, named transmission opportunity. It defines a time during which the station has time to initiate the transmission on allocated radio resources. A shorter Contention Window (CW) is assigned to an AC with higher priority in order to ensure that the higher priority AC is able to transmit before the lower priority AC. This is done by setting the CW limits CWmin and CWmax . Typical values of CW limits for different ACs in the QoS parameters set are shown in Table 4-1[77].

Table 4-1. Typical QoS parameters

Access Category	**CWmin**	**CWmax**
0	CWmin	CWmax
1	CWmin	CWmax
2	[(CWmin+1)/2]-1	CWmin

The message with higher numerical value of user priority transmits before the lower priority one, and thus the time delay is less. The IEC 61850 message types for smart grid applications in distribution substations with allowed delay (according to IEC 61850) are outlined in Table 4-2.

Table 4-2 IEC 61850 messages for smart grid applications in distribution substation

IEC 61850 Message Type	**Implemented Smart Grid Applications**	**Allowed Message Delay at Distribution [3]**	**User Priority Levels**
Publisher/subscriber messages			
GOOSE/GSE (type 1)	Control commands to trip, block, and so on; state change	3-10 ms	7
Sampled values (type 4)	Protection functions; metering	10 ms	6
Client/server messages			
Medium speed messages (type 2)	Voltage control	50-100 ms	4
Low speed messages (type 3)	Condition monitoring	100-5000 ms	2
File transfers (type 5)	Data recording; event/alarm list; settings	1000-5000 ms	0

There are two types of smart grid applications that can be achieved for distribution substations: 1) publisher/subscriber; and 2) client/server. Sampled value (type 4) messages can be used for enhanced protection and control functions, in which wireless

LAN can be used to obtain data from a wireless LAN sensor and provide a back-up link for a wired Ethernet switched network. Moreover, the sampled values can also be used for less time-critical metering applications. GOOSE/GSE (type 1) messages are mainly used for state change (ON/OFF), and commands (TRIP, BLOCK, START, STOP, and so on). Client/server message types are commonly used for comparatively less time-critical applications, for example voltage control, condition monitoring, data recording, setting value exchange, and event/alarm list.

Traffic configured in the substation WLAN can be divided into three categories: 1) event-triggered messages, which include GOOSE/GSE (type 1) messages whose priority has been set to the highest value; 2) time-triggered sample values (type 4) messages; and 3) event-triggered client/server application messages (types 2, 3, and 5).

4.4 Modeling of Noise Interference

The modeling of the radio noise interference present in typical distribution substations was carried out using OPNET. This section discusses the modeling of the wireless physical (air/shared) medium in OPNET, followed by incorporation of measured noise models into OPNET.

4.4.1 Wireless Physical Medium in OPNET

As illustrated in Figure 4-6, OPNET supports radio pipeline stages between transmitter and receiver in order to simulate the exact shared (air) medium where all receivers are part of same medium. All 13 stages are executed for each packet transmission from transmitter to receiver. Stages 2 to 13 are repeated for each receiver present in the WLAN. The first five stages of pipeline stages (transmission delay, link closure, channel match, Tx antenna gain, and propagation delay) are part of the radio transmission pipeline. Stages 6 to 13 (Rx antenna gain, received power, interference noise, background noise, signal–to-noise ratio, bit error rate, error allocation, and received power) are involved with the radio receiver pipeline stages.

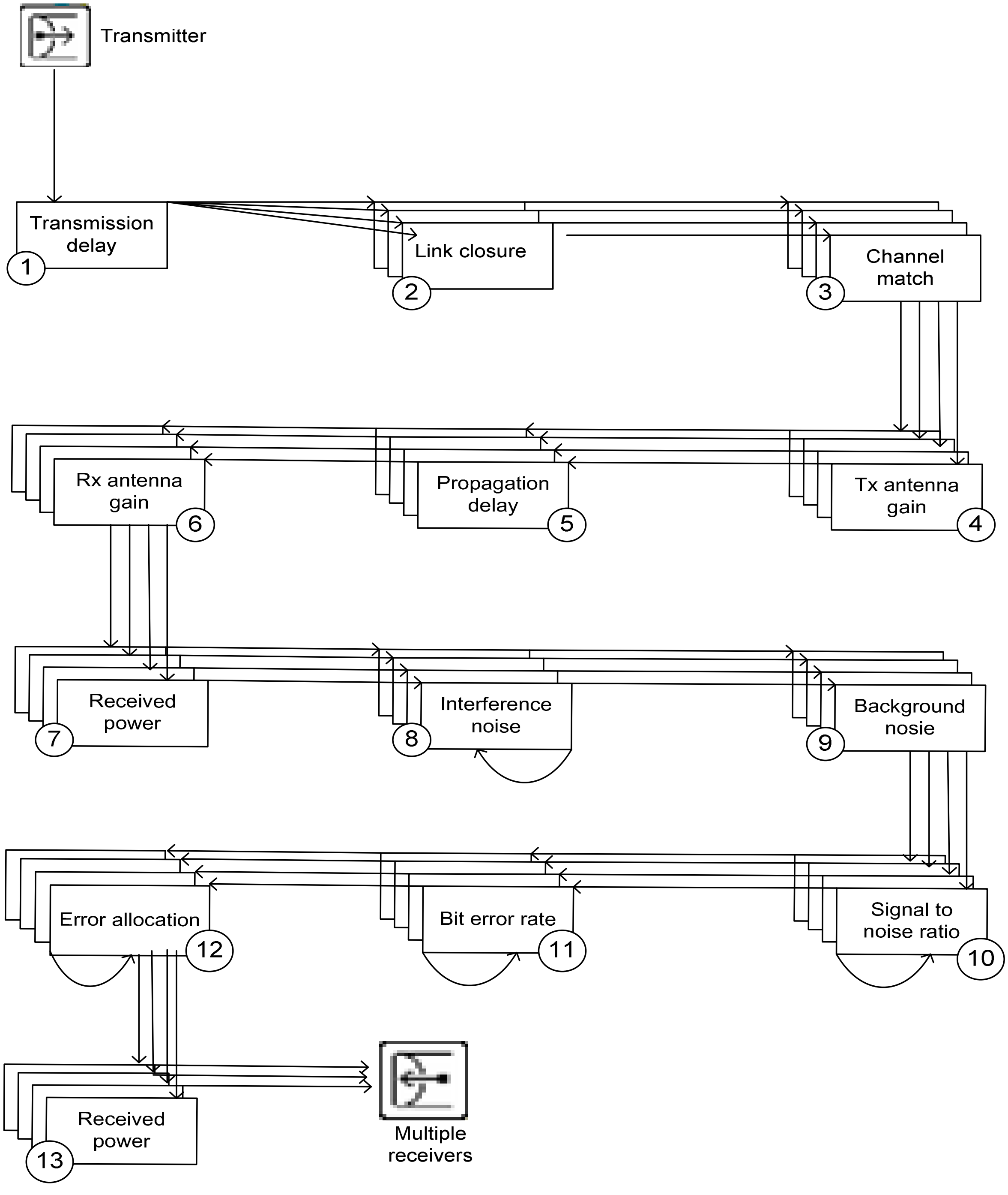


Figure 4-6 Wireless physical medium between radio transceivers

Stage 1 calculates the total transmission time required by the full packet for successful transmission. This computed time is common for all the destinations, so this stage is executed only once during the transmission process. Stage 2 checks the possibility of successful communication between the transmitter and receiver by assuring/checking whether the transmission channel can reach the receiver channel and have some impact on receiver channel or not. This stage is evoked once for each receiver channel specified in the transmitting channel's destination address set. Transmissions enter in to stage 3, which is invoked once for the each receiver channel, which meets the standards of the link closure. The classification of the transmission with respect to the receiver channel is done in this stage. It classifies the transmission packet into three categories, whether it is valid, noise, or ignored packet. Stage 4 executes immediately after the end of channel match stage. It is carried out for each destination channel, which has the transmission packet marked as valid or jammer at the channel match stage. The results of this stage are used at stage 7 for the calculation of received power. Depending upon the distance between the source and destination, the time required for the packet to travel from radio transmitter to receiver is calculated at stage 5: Propagation delay. It is evoked for the each receiver channel that has cleared the stage 2 and stage 3 successfully. The result of the propagation delay stage is also used to calculate total time of the packet reception in addition to the transmission delay stage.

Stages associated with the radio receiver start from stage 6: Receiver antenna gain. This stage computes the gain based on the direction of the vector leading from the receiver to the transmitter. It calculates the gain for each eligible destination channel. At pipeline stage 7 (Receiver power), it calculates the received power of the arriving packets in watts. The calculation is affected by the power of the transmitter, the distance between the transmitter and receiver, the transmission frequency, and antenna gain of the transmitter and receiver signal. For the noise packets also, the received power is analyzed to support the relative strengths of the packets. Stages following stage 7 are relevant for the valid packets only. Stage 8 (Interference noise) is invoked for a packet in two conditions, either the packet is valid and arrives at the destination channel while another packet is already being received, or the packet is being received while another (valid or invalid) packet arrives. This way, this stage only considers communication interferences between packets.

Stages 9 to 12 of the pipeline stages are responsible for analyzing the link's performance with respect to change in signal condition. Stage 9 is for background noise. The outcome of this stage is the sum of the power of other noise sources, which are measured at the receiver's location and in the receiver channel band. Most common background noise sources are thermal or galactic noise, emissions from neighboring electronics, and some unmodeled radio transmissions, such as television and commercial radio. The value of the background noise is added with other noise values to calculate the signal-to-noise ratio later. Stage 10 is for the signal-to- noise ratio and is invoked for the valid packet under three circumstances: the packet arrives at its destination channel; the packet is already being received and another packet arrives; the packet is already being received and another packet completes reception. The computation of the SNR is based on the received power, background noise, and interference noise. Once computed, stage 11, for Bit Error Rate, is executed under any of the three circumstances mentioned in stage 10. The purpose of this stage is to derive the probability of bit errors during the past value of constant SNR. Stage 12 is the Error allocation stage. It estimates the number of bit errors per packet segment where bit error probability is constant. If bit error probability is constant throughout the packet then this stage calculates bit errors for the whole packet.

The last stage of the pipeline is stage 13: Error correction stage. The purpose of this stage is to determine whether or not the arriving packet can be accepted and forwarded via the channel's corresponding output stream to one of the receiver's neighboring modules in the destination node.

4.4.2 Modeling Radio Noise Interference of a Distribution Substation

The EMI present in the air medium of a distribution substation needs to be modeled in pipeline stages in order to study the impact of distribution substation noise on the performance of IEC 61850 based WLAN. As explained in the previous section, pipeline stages 9 to 12 facilitate performance of the WLAN link, and especially stage 9 considers background noise present in the air. Therefore, the distribution substation radio noise models (developed from the actual measurements in Chapter 3) are implemented in stage

9 (background noise pipeline stage). As explained in Chapter 3, the measured noise models are classified into: 1) normal distribution, and 2) generalized extreme value distribution. The details of these models are explained in Appendix C. The Proto-C language code of background noise model is provided in Appendix D.

4.5 Summary

Detailed modeling of IEC 61850 based wireless substation automation devices, specifically the protection and control IED and merging unit, was developed using the industry-trusted tool OPNET. Various WLAN features as well as noise modeling were also incorporated to perform complete analysis of the WLAN communication network for the various distribution network applications. The next chapter outlines results.

Chapter 5

5. Performance Evaluation of Wireless LAN using OPNET Simulations

In this chapter, the performance of the wireless LAN communication network for various distribution network applications, e.g. various protection, control and monitoring application within substation, between distribution substation and DERs and with in micro grid is analyzed using the OPNET simulation tool. Also, the impact of various parameters, such as data rate, noise, bit error rate, distance on message delay, and throughput are studied in detail.

5.1 Parameters for Evaluation of WLAN Using OPNET

The IEC 61850 messages for corresponding distribution automation and protection applications were classified in Chapter 2 (Table 2-6). The smart distribution substation applications are classified in three types of IEC 61850 messages, these being sampled values (for streaming of raw data messages), GOOSE (event-triggered messages), and IP messages (slow messages with client/server based TCP/IP stack). The IEC 61850 message parameters considered for the performance of distribution substation applications are for: 1) control and monitoring; 2) automation and metering; 3) protection, and these are tabulated in Table 5-1.

Table 5-1 IEC 61850 message parameters for smart distribution applications

Smart Distribution Substation	**Examples of Applications**	**IEC 61850 Message**	**Allowed Delay at Distribution (ms)**	**Message Size (Bytes)**	**Message Inter-arrival Time (ms)**	**IEC 61850 Message Transmission Mode**
Control and monitoring	Automatic capacitor bank control; LTC control and	GOOSE	250-1000	128	1	Constant rate per IED (IEC 61850-8-1 re-

	monitoring; fast transfer trip scheme for bus					transmission)
Automation and metering application	Watt/VAR measurement; centralized IED configuration; data recording/archiving.	IP messages	1000-10000	1470	40	Exponential distribution rate per IEC 61850 device
Protection	Feeder over-current protection	sample value (and GOOSE)	20	256	2	Constant rate per MU (480 Hz sampling rate)

The control and monitoring applications can be achieved over GOOSE messages by utilizing analog and digital datasets defined in IEC 61850. The range of allowed delay is 250 to 1000 ms, depending on the application and utility practice. The message size of a typical GOOSE message is 128 bytes (measured from GOOSE generated by the Real Time Digital Simulator (RTDS) GTNET-GSE card). Normally, IEC 61850 GOOSE messages are on average retransmitted every millisecond per protection IED. Message transmission mode depends upon the type of application defined in IEC 61850. The distribution control and monitoring applications are required to retransmit GOOSE at every fixed interval, and this rate increases in case any event occurs, therefore, combined constant rate retransmission of GOOSE is set. The automation and metering applications are normally based on client/server-based IP message communication, which has performance requirements between 1 to 10 s. The messages are generally transmitted 25 times a second per IEC 61850 device (for example, 40 ms inter-arrival time from each IED/MU), with a typical message size of 1470 bytes. The client request is not at a fixed rate but random, and hence a memory-less probability distribution function, meaning an exponential distribution, is appropriate. For the protection application, the raw data Sample Values (SV) are transmitted at 480 Hz frequency per MU (hence, constant rate for transmission mode), with a typical size of 256 bytes (obtained from SV generated by RTDS GTNET-SV card). The allowed delay for SV is 10 ms from the field merging unit to the protection IED, and GOOSE delay to trip feeder breaker is another 10 ms, therefore total allowed communication network delay is 20 ms for a distribution protection application. The performance of this distribution substation wireless LAN for various smart grid applications was assessed in terms of message delays of GOOSE, SV, and IP messages by considering nominal parameters of a typical substation environment simulated in OPNET. The nominal parameters considered throughout the study are tabulated in Table 5-2. The priority tagging of the message was enabled for various applications (shown in Table 2-6), as well as the most prevalent WLAN technology. IEEE 802.11g at 54 Mbps data rate is used if not specified. The typical substation average SNR used was 17 dB (and equivalent BER of 0.003). Since, the noise level (SNR) in 5.8 GHz radio bands is negligible, the SNR for IEEE 802.11a is observed around 25 dB.

Table 5-2 Nominal simulation parameters

Parameter	**Base Value**
IEEE 802.11e QoS	Enabled
Data rate	54 Mbps
WLAN technology	IEEE 802.11g
Signal-to-noise ratio	17 dB
Bit error rate (BER)	3×10^{-3}

5.2 Performance of WLAN for Smart Distribution Substation Applications

5.2.1 A Typical Distribution Substation Simulated Using OPNET

Figure 5-1 shows the layout of a typical 27.6/13.8 kV distribution substation in a smart grid environment. The figure also shows the IEC 61850 based distribution automation systems for protection and control of bus bar and feeder 1.

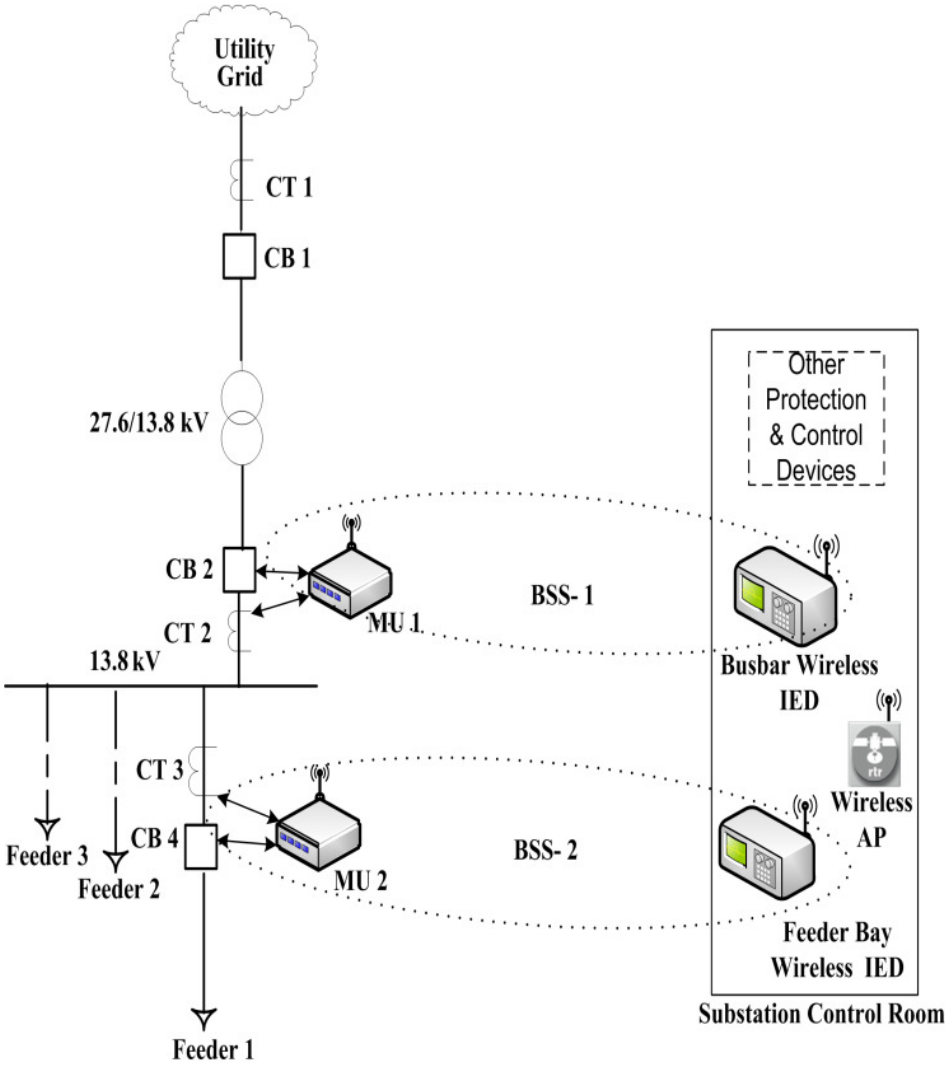


Figure 5-1 OPNET simulation of typical 27.6 kV/13.8 kV distribution substation applications over WLAN

Because the feeder requires current signals for over-current protection, current transformer 3 (CT 3) is connected to Merging Unit 2 (MU 2). Bus protection requires current signal from CT 2, which is obtained from MU 1. These merging units digitize these input analog signals and merge these values into the sampled value packet format. These sampled value packets are transmitted to the corresponding protection and control IED over a wireless communication network.

To analyze various smart grid applications, a substation wireless LAN is set up in the OPNET simulation tool, as shown in the figure. The automation and protection devices of both bus and feeder 1 have been separated into two basic service sets (BSS) of wireless infrastructure architecture. The busbar protection and control IED communicates with MU 1 in BSS 1, whereas, the feeder 1protection and control IED is connected with MU 2 in BSS 2.

5.2.2 Analysis of Distribution Control and Monitoring Applications

The performance is evaluated using End-to-End (ETE) delay of GOOSE messages from bay protection IEDs to corresponding MUs. Various WLAN data rates are considered for this analysis, such as 1 and 11 Mbps of IEEE 802.11b, 54 Mbps of IEEE 802.11g, and 54 Mbps of IEEE 802.11a. Figure 5-2 compares the GOOSE delay between 1 and 11 Mbps networks. The average and maximum ETE delays with 1 Mbps are 2.17 ms and 7.15 ms, respectively, whereas for 11 Mbps, delays are 2 ms and 2.85 ms respectively. For the same GOOSE message network load, as data rate increases, the maximum delay reduces due to lower retransmission requirements.

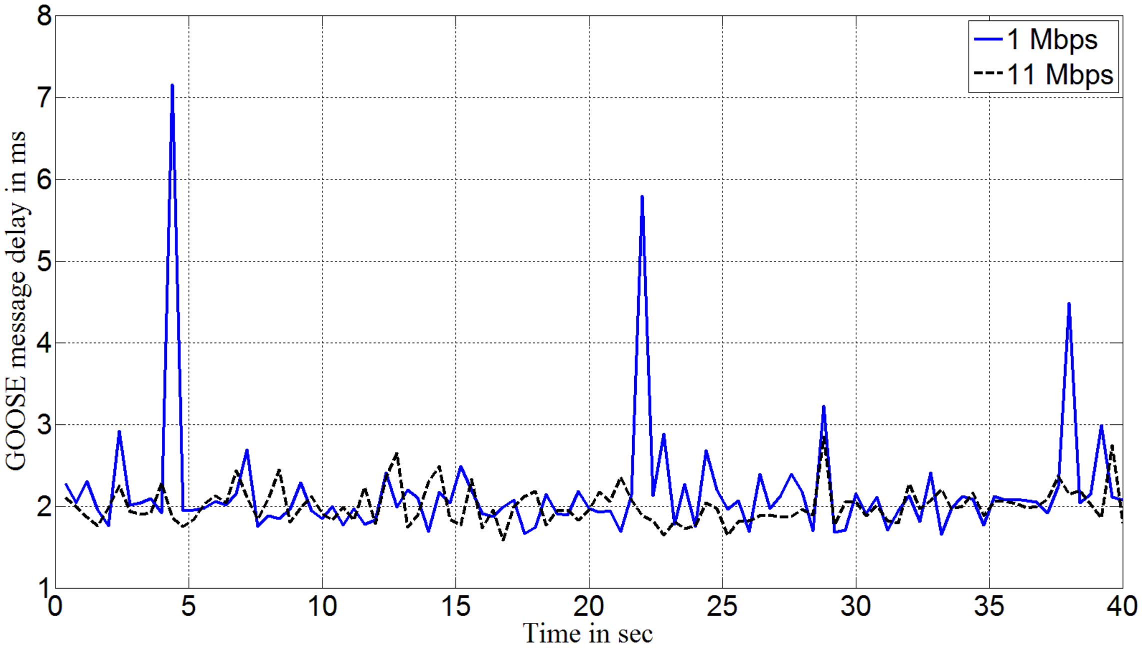


Figure 5-2 GOOSE ETE delay over IEEE 802.11b WLANs

Figure 5-3 shows the two WLAN technologies (IEEE 802.11g and IEEE 802.11a) at 54 Mbps. The average delays are 1.73 ms and 0.71 ms respectively, and maximum delays are 2.1 ms and 0.75 ms respectively. For short distances, IEEE 802.11a (based on OFDM) outperforms with respect to other technologies, however, this technology is complex and expensive.

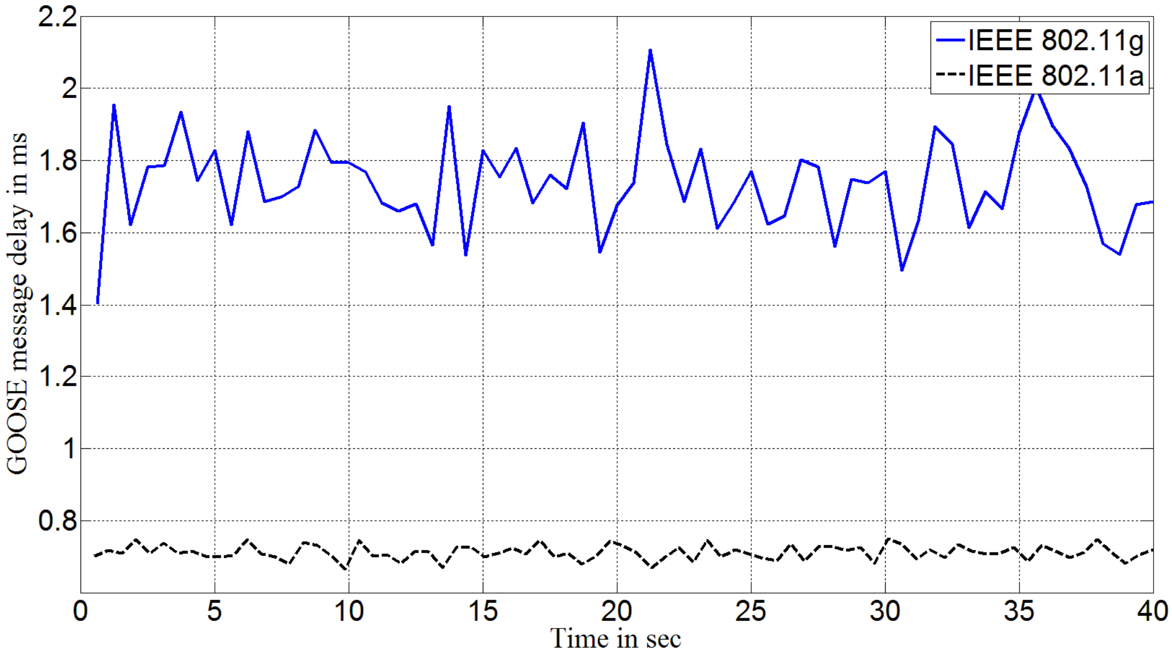


Figure 5-3 GOOSE ETE delay over IEEE 802.11g and IEEE 802.11a WLANs

5.2.3 Analysis of Distribution Automation and Monitoring Applications

As explained earlier in this chapter, distribution automation and monitoring applications were studied using IP messages based on client/server communication among IEC 61850 devices, meaning the IEDs and MUs. Figure 5-4 illustrates the IP message ETE delay for 1 Mbps and 11 Mbps.

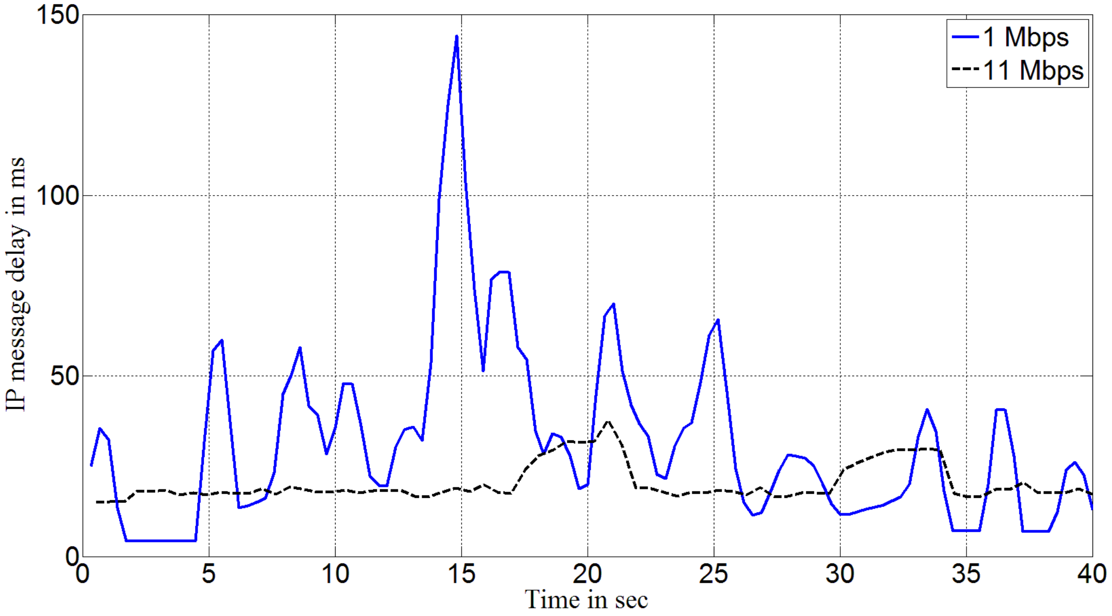


Figure 5-4 IP message ETE delay over IEEE 802.11b WLANs

Since the IP messages are communicated based on exponential distribution, not per fixed inter-arrival rate (like GOOSE and SV), with insufficient data rate (for example 1 Mbps), the large IP messages face higher delays, with average ETE times of 32 ms and maximum ETE is 144 ms. Increasing the data rate to 11 Mbps, the average and maximum delays are reduced to 20.25 ms and 37.73 ms respectively. The performance with a 54 Mbps data rate is depicted in Figure 5-5. With the IEEE 802.11g network, the average and maximum delays of IP messages are 11.76 ms and 14.42 ms respectively. For IEEE 802.11a WLAN, the average and maximum delays reduce to 4.2 ms and 4.28 ms respectively.

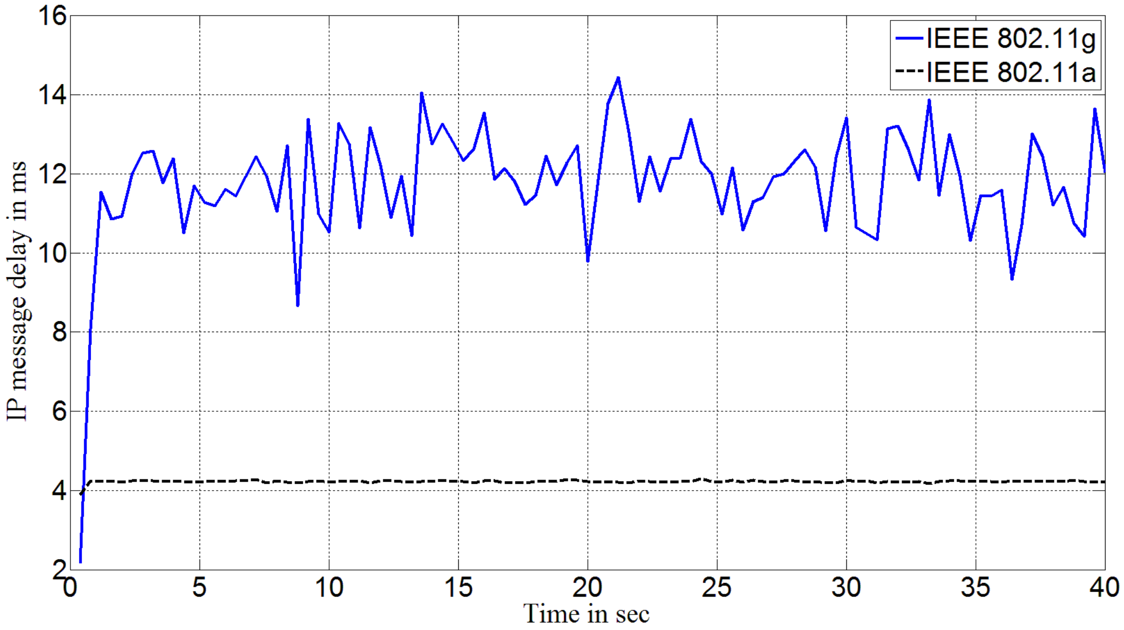


Figure 5-5 IP message ETE delay over IEEE 802.11g and IEEE 802.11a WLANs

5.2.4 **Analysis of Distribution Protection Applications**

The WLAN performance is presented using SV messages. Normally, both SV and GOOSE messages are used. The SV messages are communicated from MU to the corresponding protection IED, whereas GOOSE messages are transmitted from protection IED to MU. Since the performance of GOOSE messages originated from bay protection IEDs to MU is already presented in the previous section for control and monitoring applications, this section only discusses ETE delay of SVs.

Figure 5-6 and Figure 5-7 show the SV ETE delay for the data rates. The average and maximum delays for 1 Mbps are 10 ms and 18.69 ms respectively. For 11 Mbps, they are 5.18 ms and 8.88 ms respectively. For 54 Mbps with IEEE 802.11g, the delays are 3.58 ms and 5.73 ms, whereas with IEEE 802.11a, they are reduced to 1.53 ms and 2.6 ms. It can be observed that with the increases in data rate, the delays are reduced for the same amount of message load/transmissions per second.

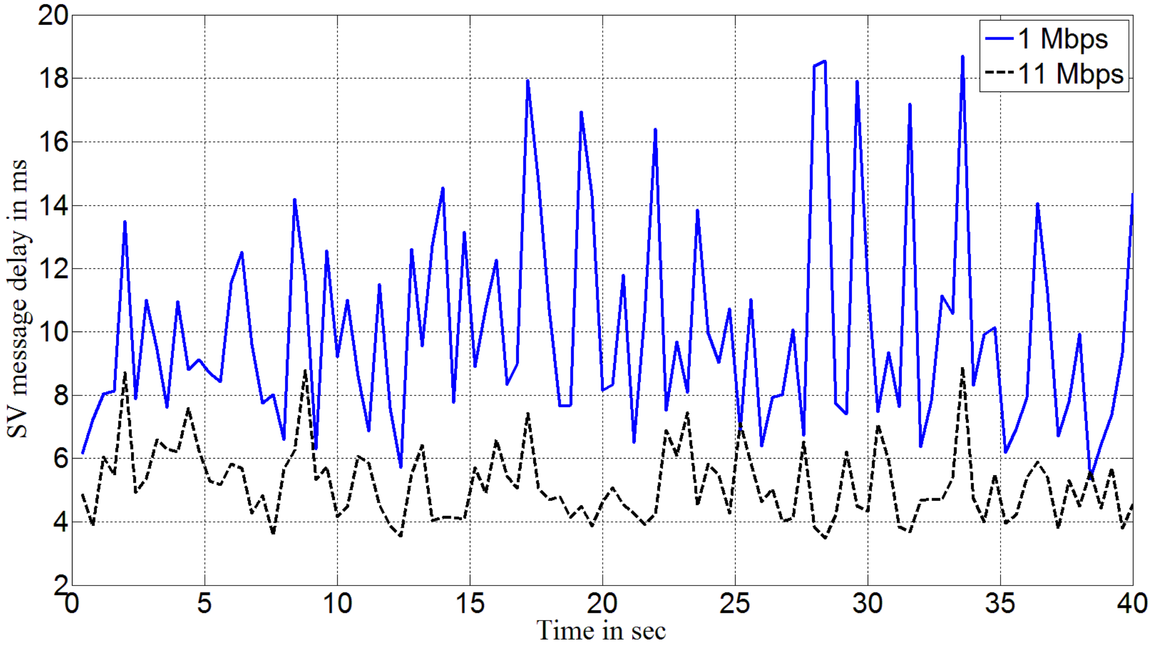


Figure 5-6 SV ETE delay over IEEE 802.11b WLANs

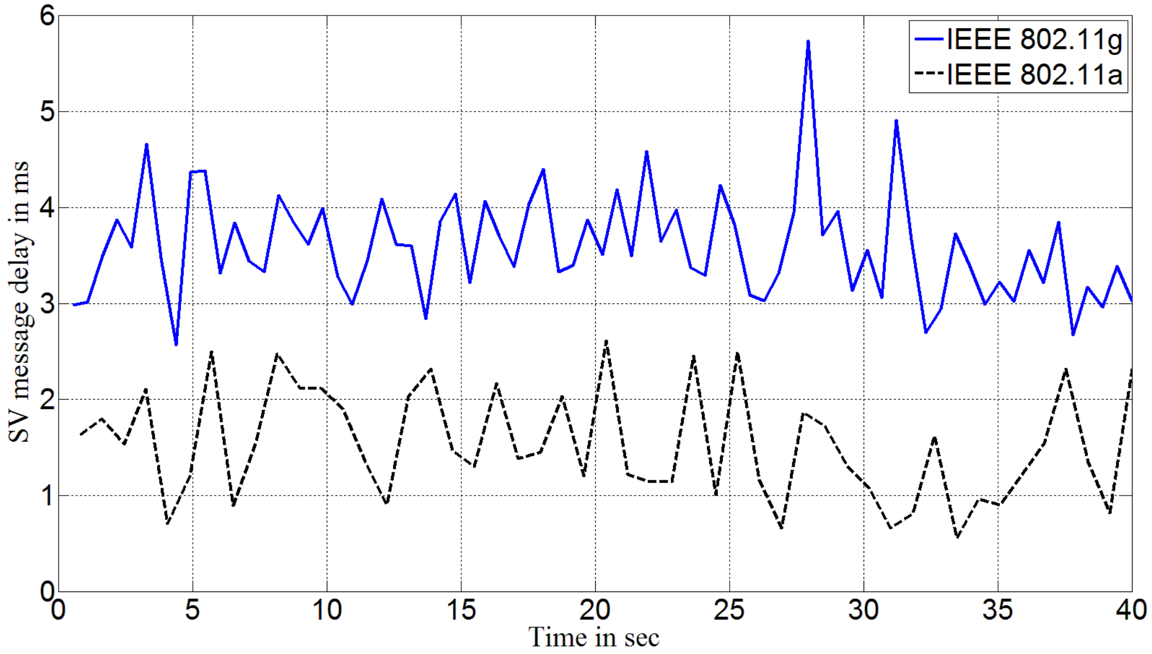


Figure 5-7 SV ETE delay over IEEE 802.11g and IEEE 802.11a WLANs

5.3 Performance of WLAN for Entire Smart Distribution Substation

5.3.1 A Typical Distribution Substation Simulated Using OPNET

Figure 5-8 shows the layout of a typical 33/11 kV distribution substation. This substation is equipped with 6 Current Transformers (CTs), and 4 Circuit Breakers (CBs) for various substation protection and automation applications. Each MU can be connected with eight analog signals (three-phase and neutral connection from two instrument transformers), and also interfaced with control of one circuit breaker and two isolators. Therefore, there is need of three MUs in this distribution substation, as shown in Figure 5-8. This wireless communication network for the distribution substation has been configured and simulated using OPNET, as shown in Figure 5-9. There are four access points, three for each protection function, and one for the station level communication. Moreover, the three bay level access points have two wireless interfaces to communicate with: 1) the protection devices within the basic service set and 2) the wireless backbone of station bus BSS 4. For example, one interface of Feeder 1 AP is part of BSS 1, which interfaces with Feeder 1 protection and control IEDs and MU 2 for bay level protection functions. Another interface of Feeder 1 AP is connected with the wireless backbone (BSS 4) through the station AP. Other station level devices, such as Station PC, HMI, and Server, are connected to substation backbone (BSS 4).

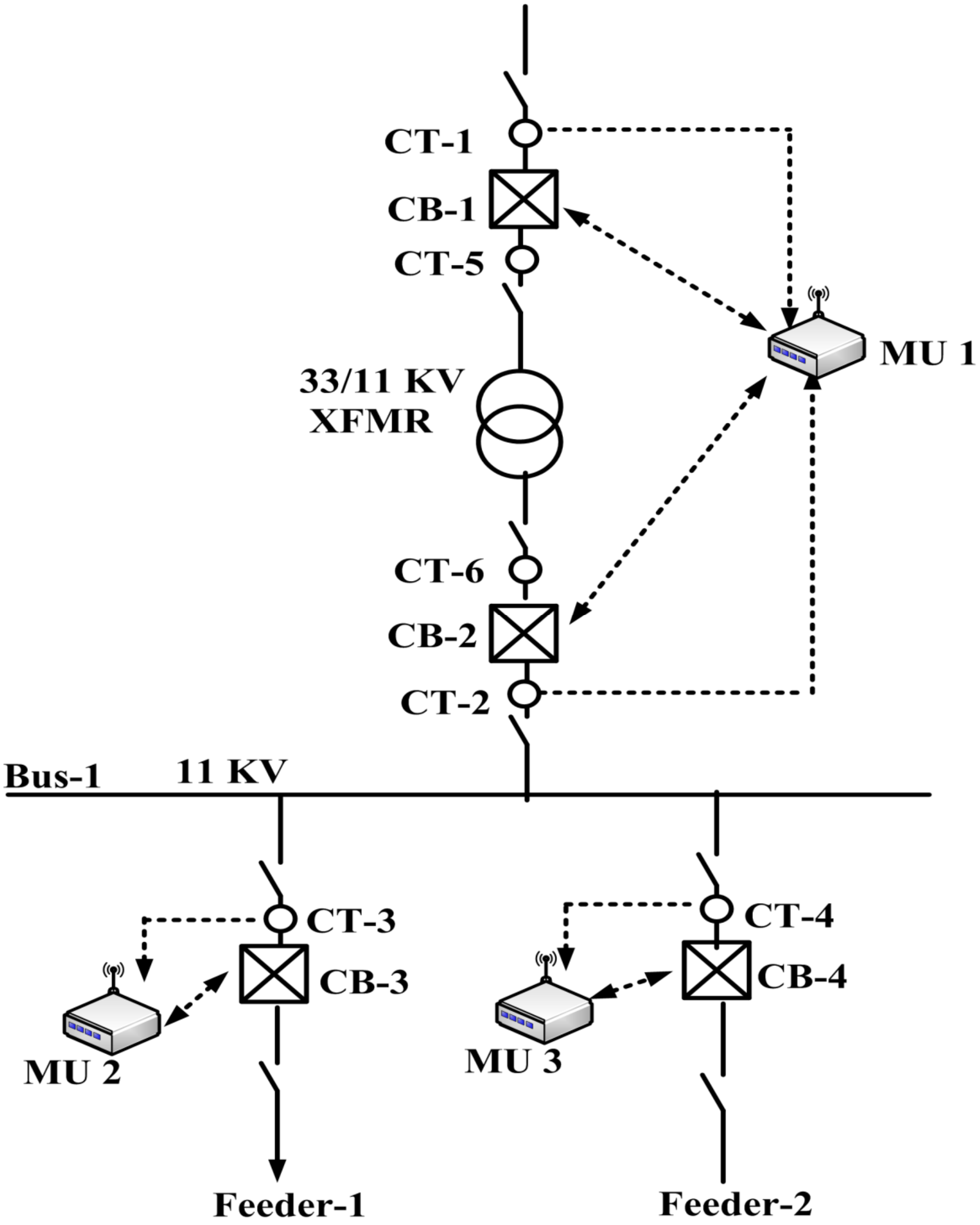


Figure 5-8 A typical 69/33 kV substation layout

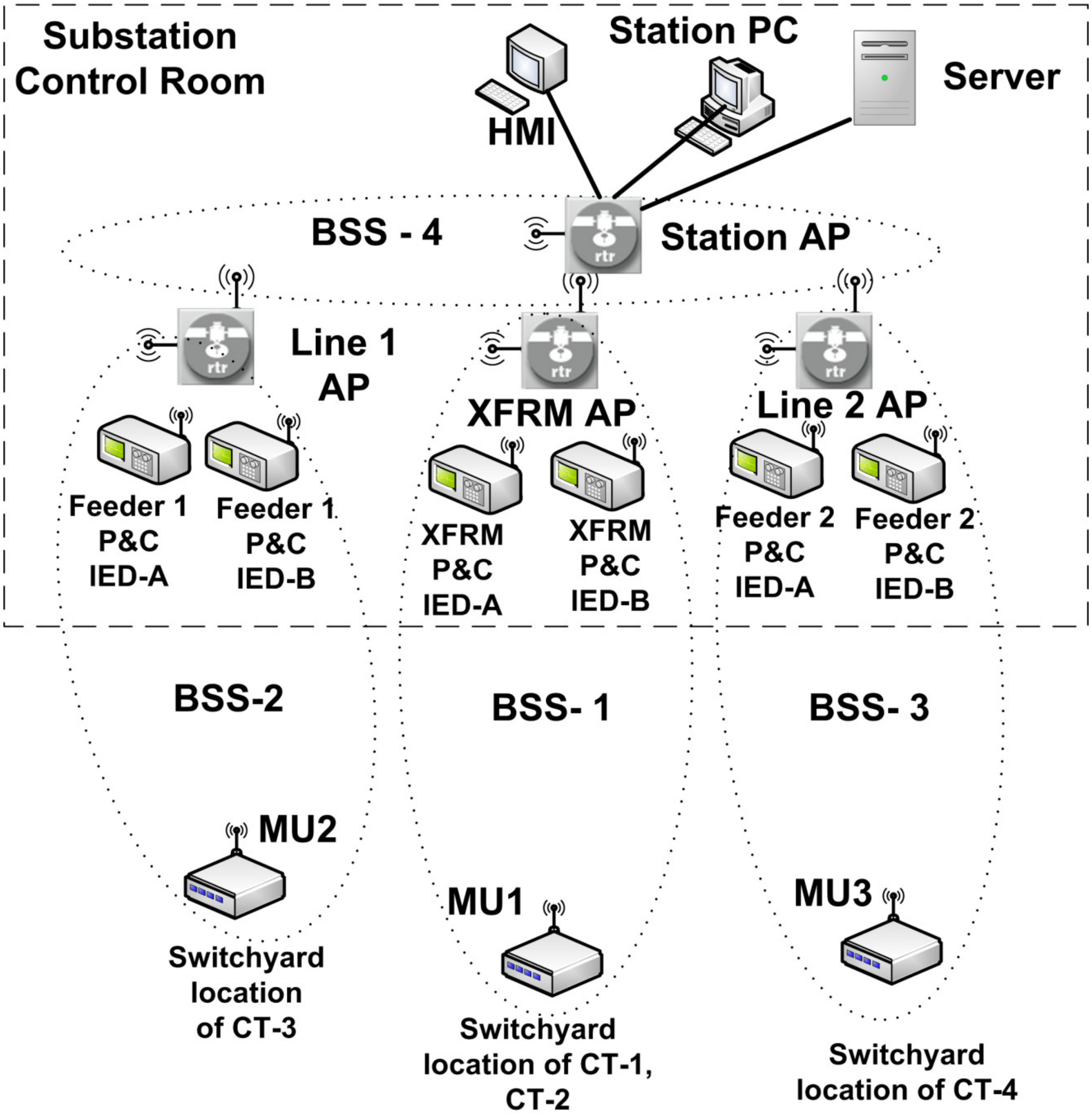


Figure 5-9 Wireless communication network for 69/33 kV distribution substation simulated in OPNET

The impact of each parameter is analyzed individually, by keeping the rest of the parameters at their base values as outlined earlier in Table 5-2.

5.3.2 IEEE 802.11e QoS

Figure 5-10 shows the GOOSE/GSE message delay values for two scenarios, with QoS enabled and disabled. QoS based priorities can be set to different types of IEC 61850 messages. Maximum GOOSE/GSE message delay is 2.7 ms when QoS is enabled. It is around 300 ms without QoS. Therefore, it is recommended to enable QoS for smart grid applications in the distribution automation network.

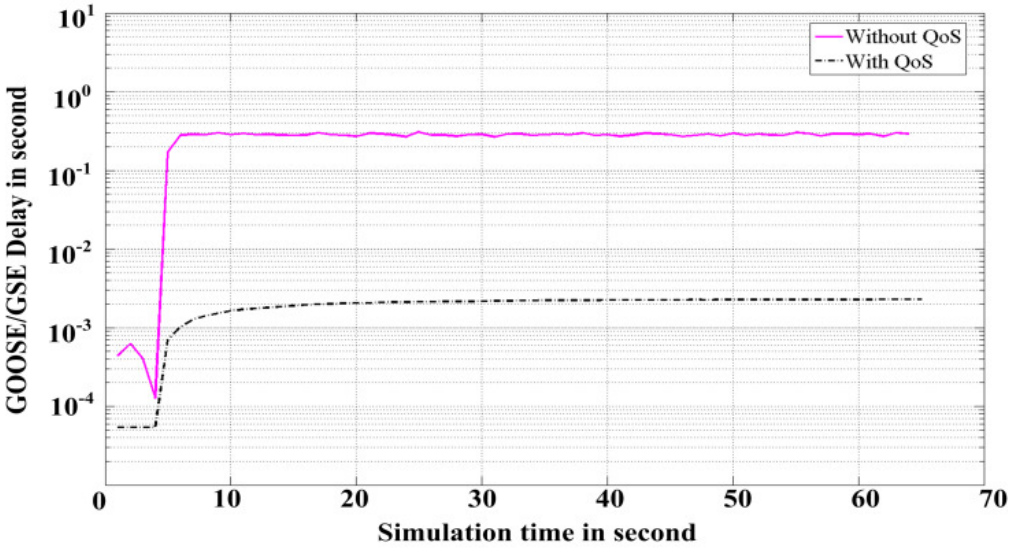


Figure 5-10 Effect of IEEE 802.11e QoS on GOOSE/GSE delay

It can be observed from

Figure 5-11 that the probability distribution function of the GOOSE/GSE delay remains between 2.1 ms to 2.7 ms, due to the QoS implementation.

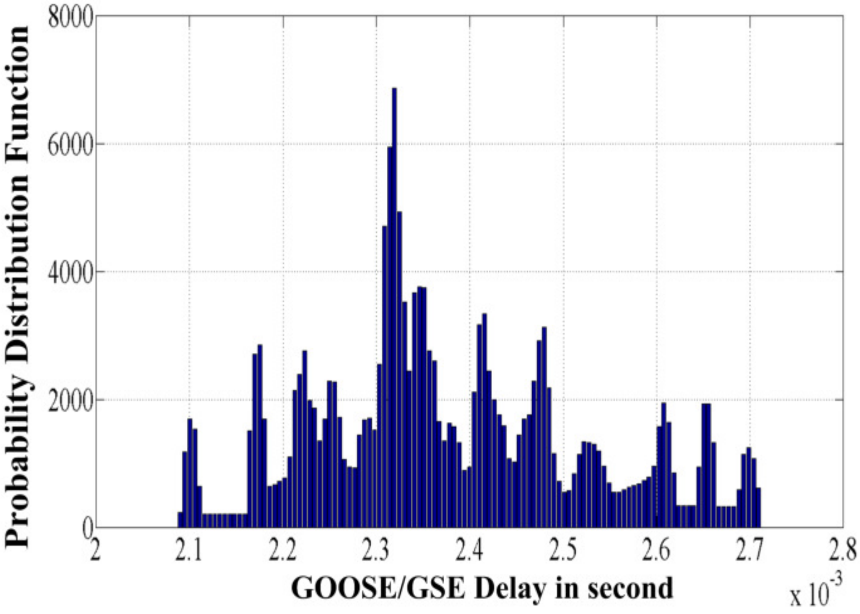


Figure 5-11 Probability distribution function of GOOSE/GSE delay with QoS

5.3.3 Effect of WLAN Technologies

Two different data rates from IEEE 802.11 were selected for the analysis, 11 Mbps and 54 Mbps. For the distribution level substation, sampling rates of 480 Hz or 960 Hz are specified in IEC 61850 part 5, and an additional sampling frequency of 1920 Hz is also considered for this analysis. Note that the data traffic on the substation WLAN increases with the sampling frequency.

It can be observed from Table 5-3 that the GOOSE/GSE, sampled value, and client/server message delays are within the allowable range with the throughput of 8000 Kbps, in cases with 54 Mbps data rates at 480 Hz and 960 Hz sampling frequencies. GOOSE/GSE message delays are within the range for 11 Mbps and 54 Mbps, as these are event-triggered and may be transmitted only a few times a second, whereas sampled value messages are transmitted 960 times a second (for 960 Hz). Moreover, the priority of the GOOSE/GSE messages is higher than sampled value messages. At 11 Mbps, the WLAN throughput reduces traffic, which results in high sampled value and client/server message delays.

Table 5-3 Effect of different data rates and sampling frequencies

Data Rate (Mbps)	**Sampling Rate (Hz)**	**Delay (ms)**						**WLAN Throughput (Kbps)**
		Sampled Value		GOOSE/ GSE		Client/Server Messages		
		Avg	Max	Avg	Max	Avg	Max	
11	480	200	420	6.0	8.2	254	382	3600
	960	140	400	2.0	3.8	271	404	3549
	1920	500	505	1.6	3.5	303	412	3400
54	480	5.0	6.0	2.2	2.4	61	66	8010
	960	5.1	7.2	2.3	2.7	63	69	8000
	1920	16	250	1.6	2.0	72	80	5945

5.3.4 Effect of Substation Noise/Interference Levels

The effect of noise/interference level on the time-critical message delays and WLAN throughput is illustrated in Figure 5-12.

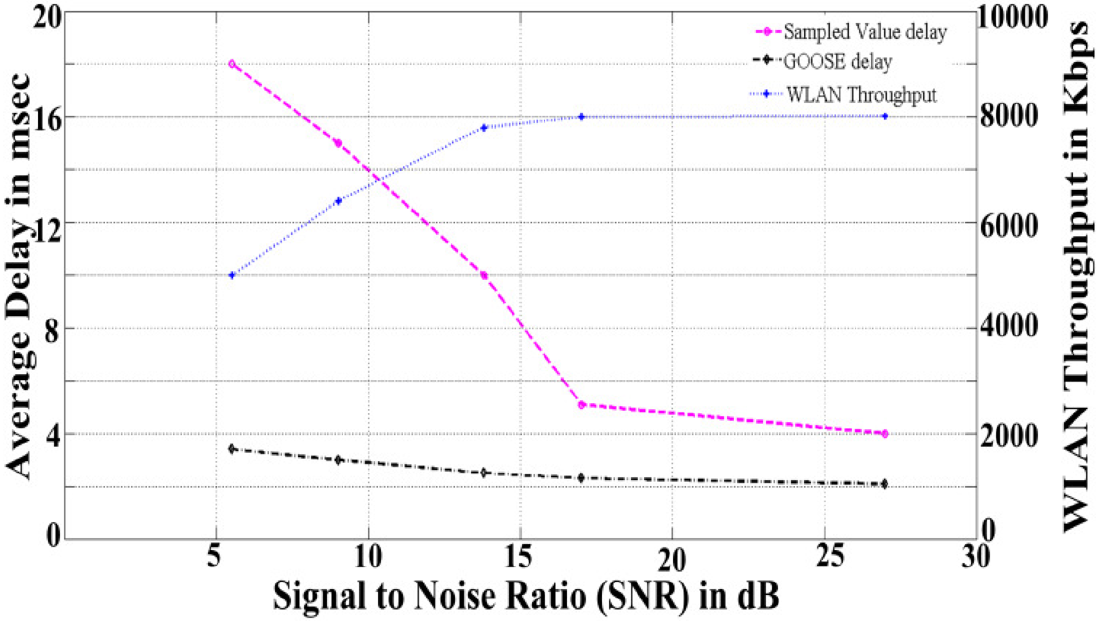


Figure 5-12 Effect of SNR on average delays and throughput

For this analysis, signal-to-noise ratio varied from 5 dB to 27.8 dB by using the developed model at various locations of substation. Note that the lower the value of SNR, the higher the effect of noise. It can be observed from the figure that in case of lower noise/interference level (SNR of 27.8 dB), sampled value and GOOSE/GSE message delays are 4 ms and 1.8 ms respectively, while throughput is around 8000 Kbps. As the noise/interference level increases (SNR reduces to 5.5 dB), the sampled value average delay increases to 18 ms and WLAN throughput decreases to 5000 Kbps.

5.3.5 **Effect of Bit Error Rate**

Figure 5-13 shows the impact of BER on time-critical messages and communication network throughput. The BER varied between $2.0\text{x}10^{-3}$ to $18\text{x}10^{-3}$, and the average delays of time-critical messages and WLAN throughput were analyzed. The results show that time-critical message delays and WLAN throughput are affected by BER, as the probability of packet rejection increases due to the reception of packets with high bit error. At BER of $4.5\text{x}10^{-3}$, the average sampled value delay is almost 10 ms and network throughput also starts declining. A further rise in BER causes time-critical message delay and throughput to unacceptable levels.

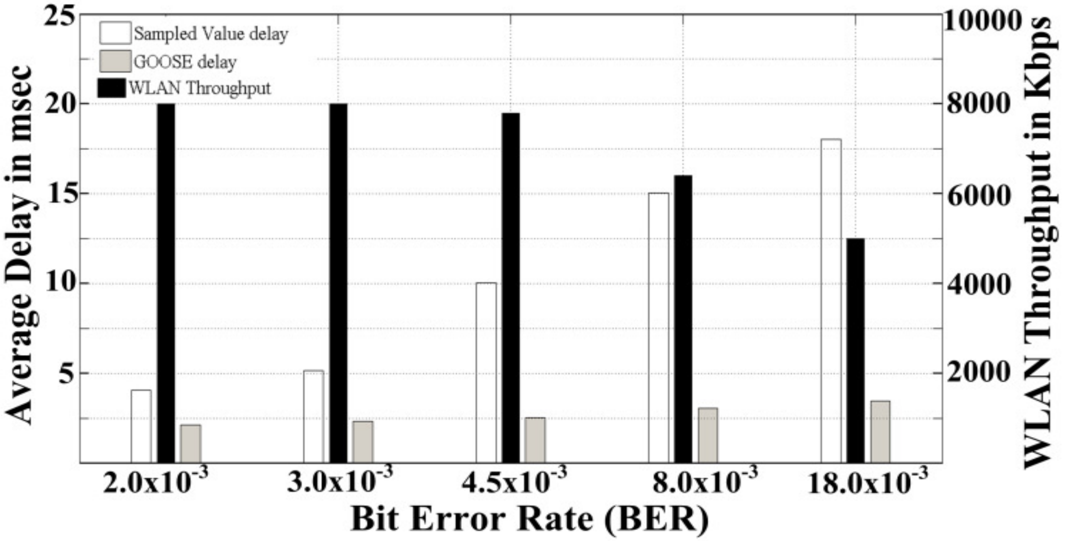


Figure 5-13 Effect of BER on average delays and throughput

5.3.6 Effect of Distance between IEDs and MUs

As the time-critical messages are communicated between the substation control room and the switchyard, it is important to study the effect of distance between the protection and control IED in the control room and the MU in the switchyard. As outlined in Table 5-4, as the distance increases the WLAN throughput decreases and delay increases due to the path loss. For a distance of more than 200 meters, the time-critical message delay values can cross the allowable range as the WLAN throughput starts decreasing. However, GOOSE/GSE results remain strong even at 300 meters.

Table 5-4 Effect of distance

Distance (meters)	**Delay (ms)**						**WLAN Throughput (Kbps)**
	Sampled Value		GOOSE/GSE		Client/Server Messages		
	Avg	Max	Avg	Max	Avg	Max	
100	4.1	5.5	2.0	2.6	60	67	8050
200	5.1	7.2	2.3	2.7	63	69	8000
300	7.8	11.5	2.3	2.7	78	100	7100

5.4 Performance of WLAN for Microgrid Applications

References [74] and [75] discuss the use of wireless LAN in a microgrid environment. However, an in-depth study examining suitability of promising wireless LAN for various microgrid applications is needed. Therefore, the performance of control, protection, and monitoring applications for distributed energy resources (DERs) in the microgrid was assessed in terms of average and maximum message transfer delays and throughput over the WLAN. Extensive analysis of wireless LAN was conducted using OPNET, considering different communication data rates and radio noise levels. Performance results are presented in this chapter to identify suitability of WLAN for microgrid applications.

5.4.1 **Simulation of a Typical Microgrid Using OPNET**

The OPNET Modeler simulation tool [55] is considered the leading tool in the communications network industry. Moreover, OPNET facilitates authentic models of commercially available networking devices. Figure 5-14 shows a WLAN for a typical microgrid system simulated in OPNET.

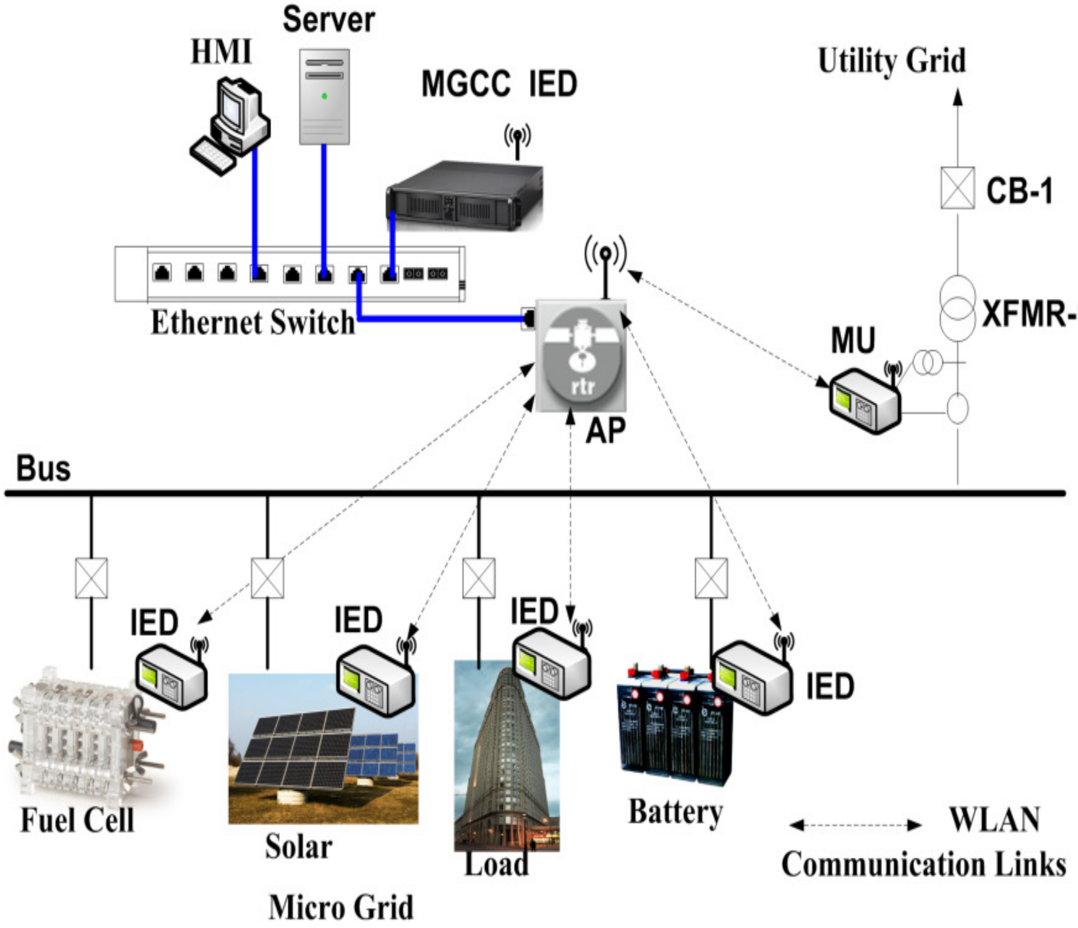


Figure 5-14 Wireless LAN for various microgrid applications simulated in OPNET

Since all DERs are controlled by a single Micro-Grid Central Control (MGCC) IED, a wireless Access Point (AP) is located near the MGCC IED by connecting the IED and other local DER IEDs over wireless LAN. A server is connected through an Ethernet switch to the MGCC IED. Local wireless IEDs at each DER location have capabilities to control, monitor, and protect an energy source locally, as well as coordinate DERs by communicating with MGCC over wireless LAN. GOOSE messages are generated for control applications between the MGCC IED and local IEDs every 1 ms. The MU located at the point of integration between the microgrid and utility grid sends sampled values messages at 480 Hz sampling frequency (2 ms) to the corresponding MGCC IED for microgrid protection applications. Moreover, condition monitoring of DER plants and data recording are obtained from local DER IEDs to the MGCC IED at exponentially distributed average rates of 1 sec and 10 secs respectively. The parameters and message sizes considered for the simulation are listed in Table 5-5.

Table 5-5 Nominal OPNET parameters and message sizes

Parameter	**Value**
Data rate	54 Mbps
Sampling frequency	480 Hz
Signal-to-noise ratio (SNR)	17 dB
Distance between MGCC IEC and DERs	150 meters
Application Message	**Size (bytes)**
GOOSE	128
Sampled value	256
Condition monitoring	1024
Data recording	1470

5.4.2 Results and Discussion

Performance results obtained from OPNET for all four applications at different data rates of an IEEE 802.11 network are tabulated in Table 5-6. At 11 Mbps, the average delay for time-critical protection applications is higher than that specified in the standard (as listed in Table 2-5), and the throughput is much lower. By increasing data rates to 36 Mbps, SV message delays are within 10 ms, the condition monitoring is within 100 ms, and throughput improves to 3100 Kbps. At 54 Mbps, complete applications can be achieved with throughput of 3800 Kbps and delays kept within the standard’s specifications.

Table 5-6 Effect of different modulation types and data rates

Application	**Delay (ms) for Different 802.11 Data Rates**

	11 Mbps		36 Mbps		54 Mbps	
	Avg	Max	Avg	Max	Avg	Max
Protection (SV)	43	68	4.6	8.75	1.35	5
Control (GOOSE)	4.5	7.9	2.1	2.4	0.7	1.75
Condition monitoring	153	207	69	86	38	50
Data recording (File transfer)	4400	5300	2300	2800	800	1200
Total throughput	1800 Kbps		3100 Kbps		3800 Kbps	

On the other hand, Figure 5-15 shows average delay and throughput for time-critical protection and control applications at various noise levels. If noise level is high enough to reduce SNR below 17 dB, it can result in higher delays and lower throughput.

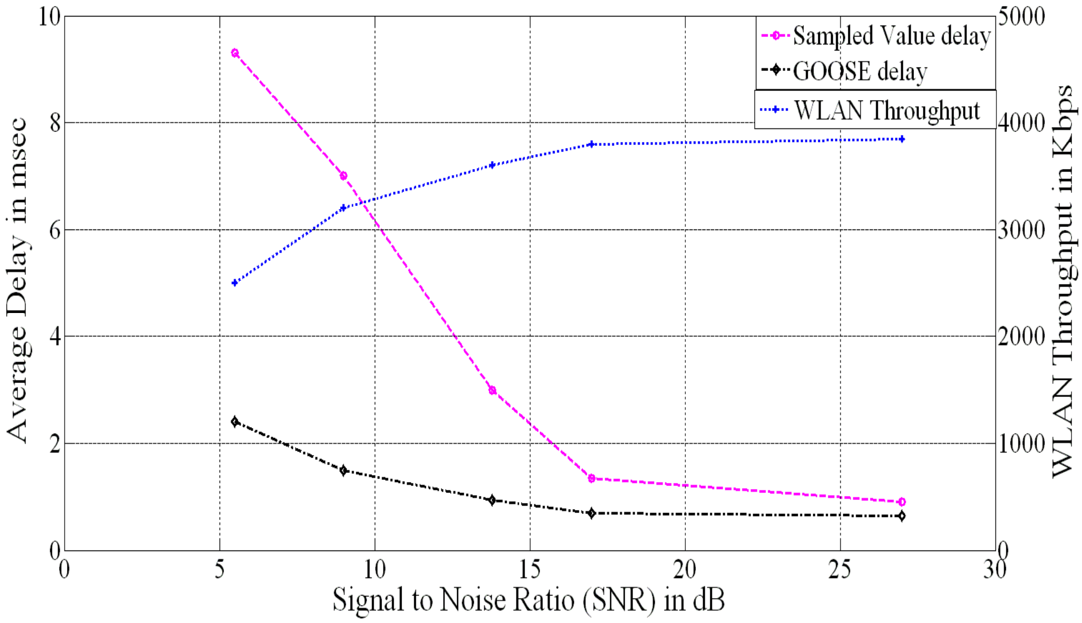


Figure 5-15 Average delay and throughput for different SNRs over wireless LAN

5.5 WLAN Communication Network between DAS and DERs

Communication networks between the distribution automation system (DAS) and DERs were simulated using OPNET. The OPNET Modeler facilitates the design and study of communication networks, devices, protocols, and applications. OPNET Modeler is based on a series of hierarchical editors that directly parallel the structure of real networks, equipment, and protocols. As defined in IEC 61850, substation protection and control IEDs have two separate communication stacks. Client-server applications have the entire all OSI-7 layers stack, which is used for the communication of metered (measured) values, whereas the GOOSE and raw data sampled values will directly use an Ethernet link layer in order to reduce the latency due to processing and overhead. Both kinds of communication stacks were simulated using OPNET. Moreover, the time-critical messages used priority tagging, which further reduced the latency due to queuing. Queue size and processing speed were considered from commercial product models available in OPNET. The following sections discuss the performance of different communications systems using latency and throughput of the communication link.

5.5.1 System Under Study

To study the performance between an IEC 61850 based DAS and DERs, a typical 69 kV/11 kV distribution substation was considered, as shown in Figure 5-16. DER is connected on the outgoing feeder 2. Only one DER source was considered for the analysis. This section analyzes the different types of communication between the feeder 2 IED and the DER IED.

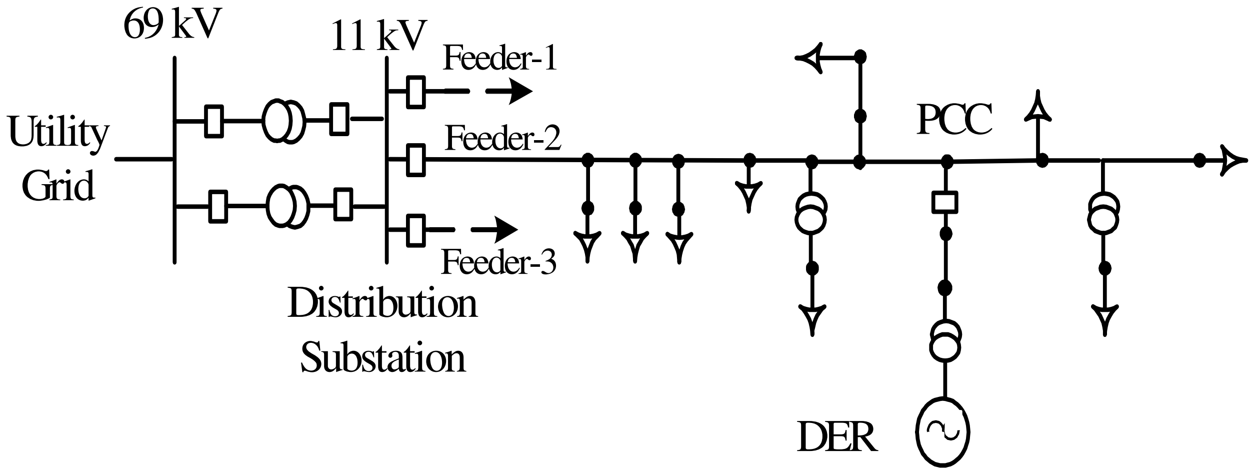


Figure 5-16 A typical 69kV substation single line layout

5.5.2 **OPNET Simulations**

Figure 5-17 shows the simulation setup for a 69 kV DAS and communication link with DER P&C devices in the OPNET Modeler simulation tool. There is a communication link between the feeder 2 IED from the line bay and the DER protection and control IEDs, as shown . Different communication system scenarios were simulated in OPNET for protection, control, monitoring, and metering data exchange.

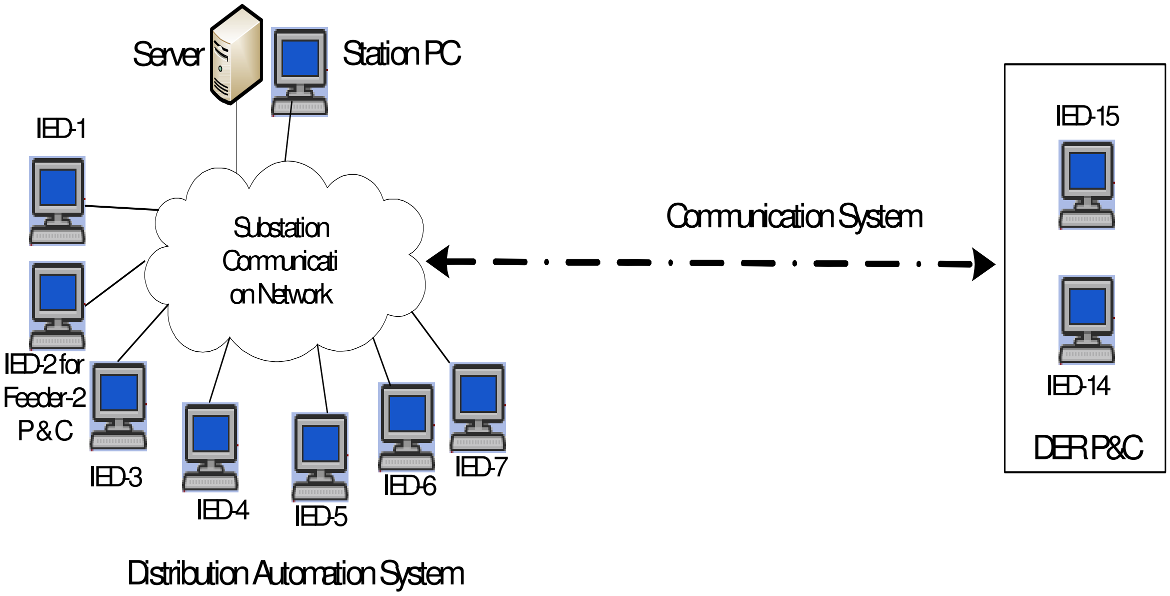


Figure 5-17 Concept of communication system between DAS and DERs

5.5.3 **Wireless LAN Network Simulation**

As shown in Figure 5-18, wireless technology based on frequency hopping spread spectrum (FHSS) (IEEE 802.11) can provide a communication range up to 1 km. One Mbps and 2 Mbps data rates were considered for the simulation study.

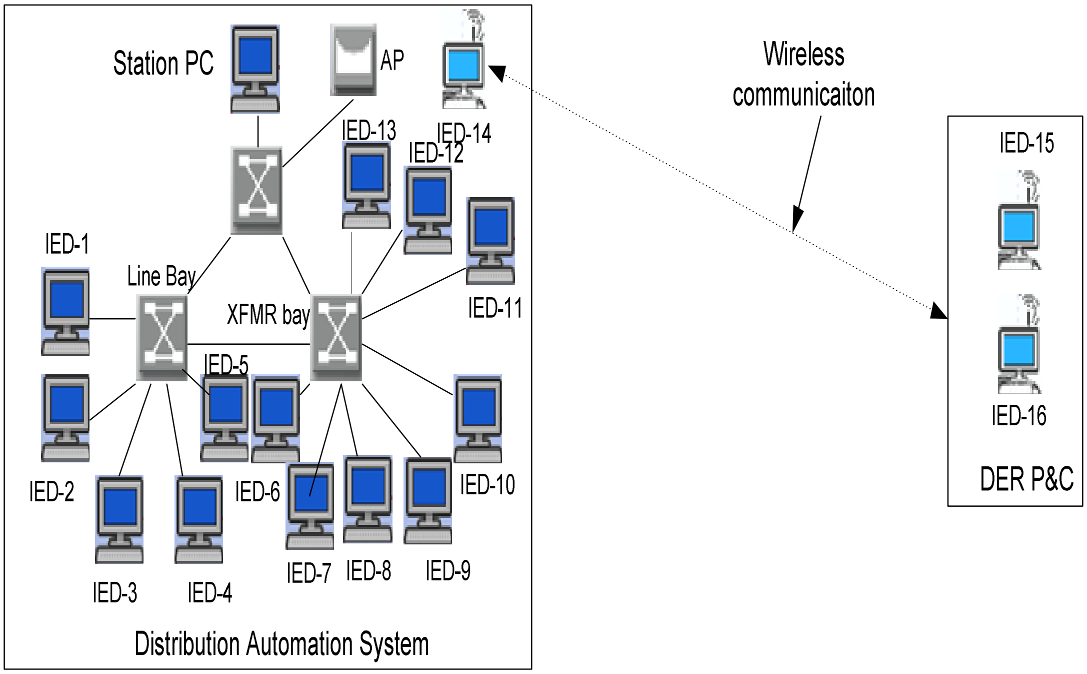


Figure 5-18 Wireless communication network without repeater

As Table 5-7 shows, the maximum GOOSE message time delay for a wireless network without repeater is around 9 ms, which is less than the allowed time delay (16 ms). The time delay for metering (measured value) messages is between 400 and 600 ms.

Table 5-7 Wireless technology performance evaluation without repeater

Type of Message	**Data Rate**					
	1 Mbps (for 1 km)			2 Mbps (for 1 km)		
	Delay (ms)		Throughput (kbps)	Delay (ms)		Throughput (kbps)
	Avg	Max		Avg	Max	
GOOSE	4.5	6.1	26	3	9	25
Metering / Measured	580	600	550	420	430	530

5.5.4 **Wireless Network Simulation with Repeater**

To increase the coverage of wireless networks, it is a common practice to use repeaters. The function of the repeater is to receive the message and transmit it with comparatively high power to cover more distance. However, this adds some transmission delay. The simulated wireless communication network with a repeater is shown in Figure 5-19.

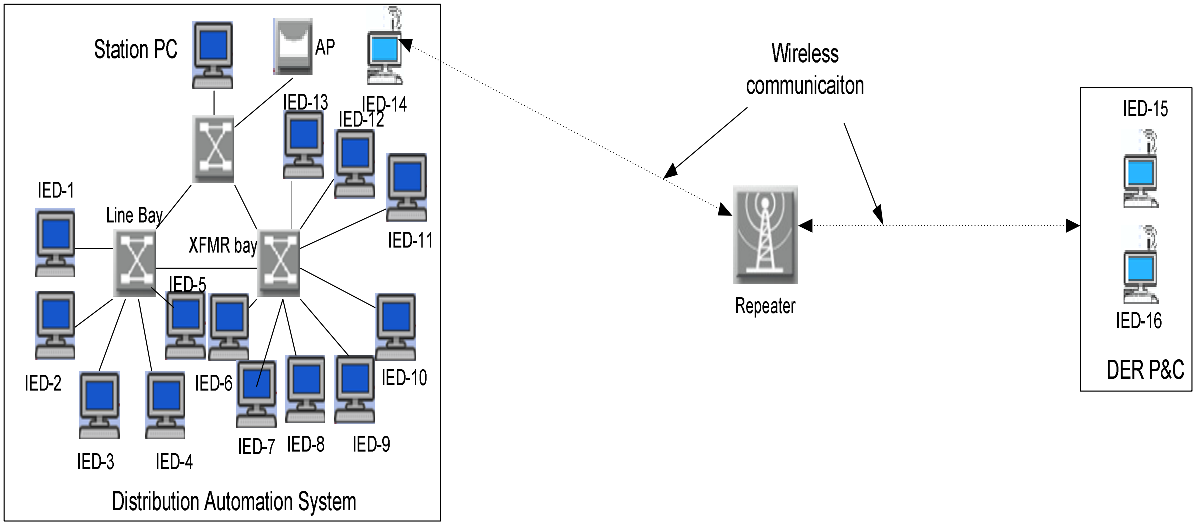


Figure 5-19 Wireless communication network with repeater as specified in the standard specified in the standard.

Table 5-8 shows that time delay with a repeater is higher than the time delay without a repeater. The distance between DAS and DER wireless nodes has increased to around 2.5 km, but the throughput increases as the date rate increases. Due to the repeater, the time delay increases by a small value. However, all the delays of this scenario are within the allowable range specified in the standard.

Table 5-8 Wireless technology performance evaluation with repeater

Type of Message	**Data Rate**					
	1 Mbps (for 2.5 km)			2 Mbps (for 2.5 km)		
	Delay (ms)		Throughput (kbps)	Delay (ms)		Throughput (kbps)
	Avg	Max		Avg	Max	
GOOSE	7	11	31	10	18	35
Metering / Measured	1100	1400	300	1400	1700	500

5.6 Summary

In the first part of the OPNET simulation study, the performance of individual smart distribution substation applications, such as control and monitoring, automation and metering, and protection, over WLAN communication network was analyzed for various data rates/technologies. Table 5-9 summarizes the results, which show that overall end-to-end (ETE) delays are reduced with higher data rate networks. The ETE delays are within the allowable range, except for protection applications at 1 Mbps, for which the delays are higher than the limit of 10 ms. Even at 11 Mbps, the SV maximum delay was 8.88 ms (close to limit). Therefore, it is recommended to consider the 54 Mbps WLAN data rate for applications within a distribution substation. The delays with IEEE 802.11a are less than IEEE 802.11g (even at the same data rate of 54 Mbps), but IEEE 802.11a is comparatively costly and complex.

Table 5-9 Summary of WLAN performance for various distribution substation applications

WLAN Technologies	**IEC 61850 Message ETE Delays (ms)**					
	Control and Monitoring (GOOSE)		Protection (SV)		Automation and Metering (IP – Client/Server)	
	Avg	Max	Avg	Max	Avg	Max
1 Mbps of IEEE 802.11b	2.17	7.15	10	18.69	32	144
11 Mbps of IEEE 802.11b	2	2.85	5.18	8.88	20.25	37.73
54 Mbps of IEEE 802.11g	1.73	2.1	3.58	5.73	11.76	14.42
54 Mbps of IEEE 802.11a	0.71	0.75	1.53	2.6	4.2	4.28

Further analysis demonstrated the significance of the developed IEC 61850 platform in OPNET, including performance of the entire distribution substation over WLAN, small microgrid applications using WLAN, and a slow data rate but higher range WLAN between a DAS and DERs. It was concluded that wireless LAN at 54 Mbps is feasible for control, protection, and monitoring applications of the distribution substation and microgrid applications, and that with a lower higher data rate, the distance coverage of the WLAN can be increased. In the following chapters, laboratory and field testing of various applications are examined by developing hardware devices for IEC 61850 based smart distribution substation applications.

Chapter 6

6. Development of WLAN Hardware Setup

In this chapter, the wireless LAN performance is evaluated in a laboratory by developing hardware prototypes of WLAN enabled IEC 61850 devices, such as wireless IEDs and merging unit playback, using the QNX Real Time Operating System (RTOS) over an embedded platform. In addition to these IEC 61850 devices, the distribution automation and protection laboratory is set up, including a commercial wireless access point, traffic generator noise sources, network analyzer, and spectrum analyzer. The communication network performance for distribution substation monitoring, control, and protection applications is tested using this distribution laboratory setup. The test results from the laboratory setup are presented in terms of Round Trip Time (RTT) of IEC 61850 messages.

6.1 Hardware Platform Development

A general-purpose hardware platform is configured to develop IEC 61850 based wireless IEDs and MU playback in the laboratory (Figure 6-1). The device includes: 1) Intel's DH55HC ATX single-board computer; 2) ANTEC's industrial hardened 3U rack-mount chassis [79]; 3) CISCO's Linksys WMP600N wireless LAN transceiver [80]; and 4) QNX Real-Time Operating System (RTOS) [81]. This section describes this general-purpose WLAN-enabled industrial embedded device.

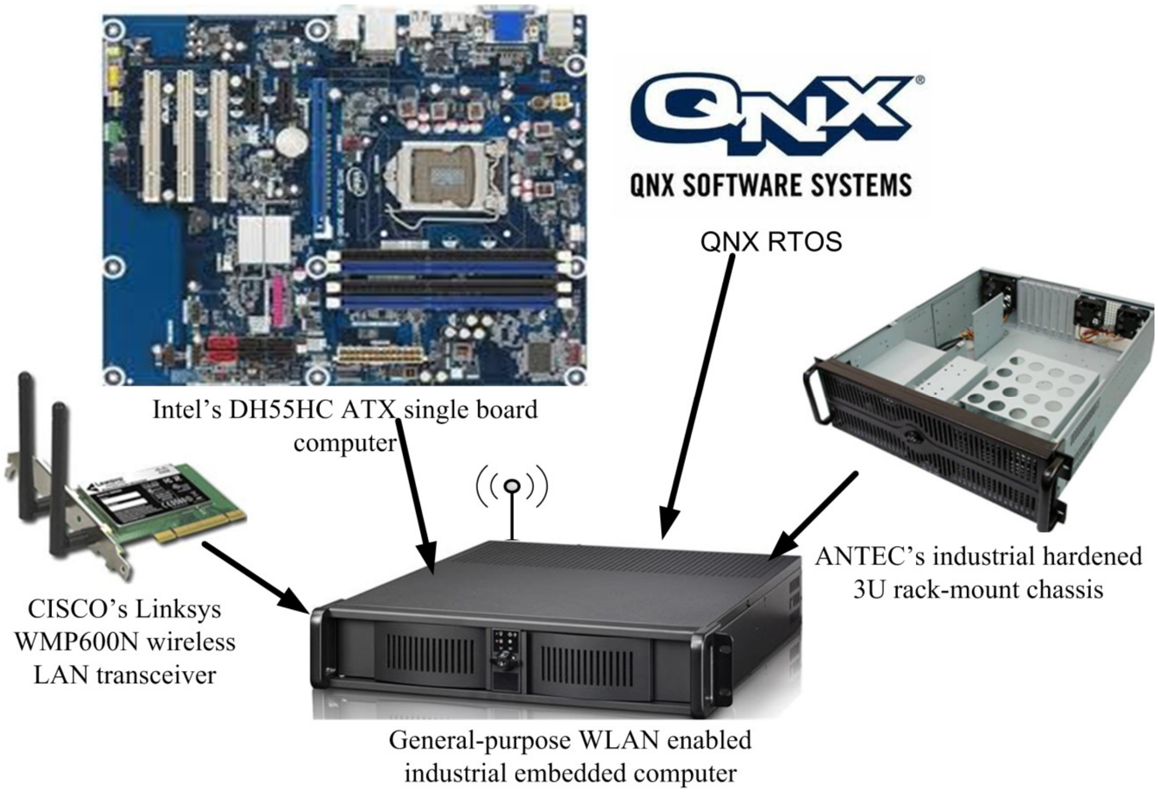


Figure 6-1 General-purpose WLAN-enabled industrial embedded device

At the time of development, the licenses of QNX RTOS were already available in the Department of Electrical and Computer Engineering at the University of Western Ontario in Canada. Therefore, hardware components (ATX motherboard and WLAN network interface card) were selected considering compatibility with QNX, high performance, and economy for the purchase of multiple systems. Intel's ATX system DH55HC motherboard offers a 3.2 GHz processor and various interfaces: three PCI conventional bus connectors, single PCIe-x16, and a PCIe-x1. The ANTEC-supplied industrial-graded rack-mount chassis with 650 W power supply was used. The CISCO-made Linksys WMP600N, dual-band PCI adapter operates in the 2.4 and 5 GHz radio bands. Moreover, it also offers optimal performance when connected to any of the wireless LANs, for example IEEE 802.11-g, -b, -a, -n networks [80]. It supports industrial-strength WPA2 (IEEE 802.1i protocol) and up to 128-bit encryption for security.

QNX Neutrino is one of most-used hard real-time OS in various industries, where hard real-time refers to immediate. Hard real-time performance of the IEC 61850 devices is achieved with the help of various capabilities of the real-time platform, such as hard real-time timers, multithreads for parallel processing, and input/output packet (io-pkt). The QNX Neutrino RTOS [81] claims deterministic response times at the application level and in all subsystems. Moreover, it is a microkernel operating system that includes only the most fundamental services, such as signals, timers, and schedulers. All other components (file systems, drivers, protocol stacks, applications) run in the safety of a memory-protected user space. QNX also offers adaptive partitioning, which ensures that critical processes are never starved of resources and always meet real-time deadlines.

Various functionalities of IEC 61850 were developed using hard real-time QNX and general-purpose hardware with wireless LAN connectivity, as explained in following sections.

6.2 Development of WLAN Enabled IEC 61850 Prototype Devices

Normally, round-trip time of communication messages is measured to evaluate the performance of the communication network. Hence, two WLAN-enabled IEDs were developed to study RTT for various IEC 61850 messages: 1) processing-IED; and 2) echo IED. These IEDs resemble the functionality of any IEC 61850 based device communicating control, monitoring, or metering application (GOOSE or client/server based IP) messages. The processing IED sends IEC 61850 messages with a unique ID and registers sending time using hard real-time timers. An echo-IED, upon reception of the IEC 61850 messages, echoes-back the same message to the processing IED. Finally, the processing IED matches the unique ID of the IEC 61850 message and calculates RTT by subtracting receiving time of the echo-back IEC 61850 message with the registered sending time of the same IEC 61850 message.

In order to investigate the performance of the distribution protection application discussed earlier, the developed IEC 61850 based devices were: 1) MU playback; and 2) a protection and control (P&C) IED. The MU is a field device that converts measured current transformer/voltage transformer analog signals to digital and encapsulates them in IEC 61850 sampled value messages. The developed MU playback communicates the IEC 61850 sampled value messages (which include current/voltage signals obtained from PSCAD/EMTDC simulation) to the P&C IED. The P&C IED implements inverse over-current protection functions. In case of a short-circuit fault condition on the component to be protected (meaning the distribution feeder in this case), the protection IED issues a trip command to the circuit breaker using an IEC 61850 GOOSE message. Upon receipt, the MU calculates total protection time by subtracting the GOOSE receiving time with sending time of the SV message that corresponds to the fault inception time.

In summary, a processing IED, echo IED, MU, and protection and control IED were developed. Functionalities of these four prototypes of IEC 61850 devices are described as follows.

6.2.1 Development of Processing IED

Figure 6-2 is a functional diagram of a processing IED. A processing IED streams the IEC 61850 message to the echo IED over the wireless LAN. The echo IED echoes-back the same message in order to evaluate total RTT over the network. As depicted in Figure 6-2, the processing IED has two separate real-time threads of QNX operating systems. These threads are executed simultaneously, such that the processing IED can send/receive an IEC 61850 message at the same time. Thread 1 is responsible for sending the IEC 61850 message; whereas, thread 2 captures the IEC 61850 message and computes total RTT over the wireless LAN.

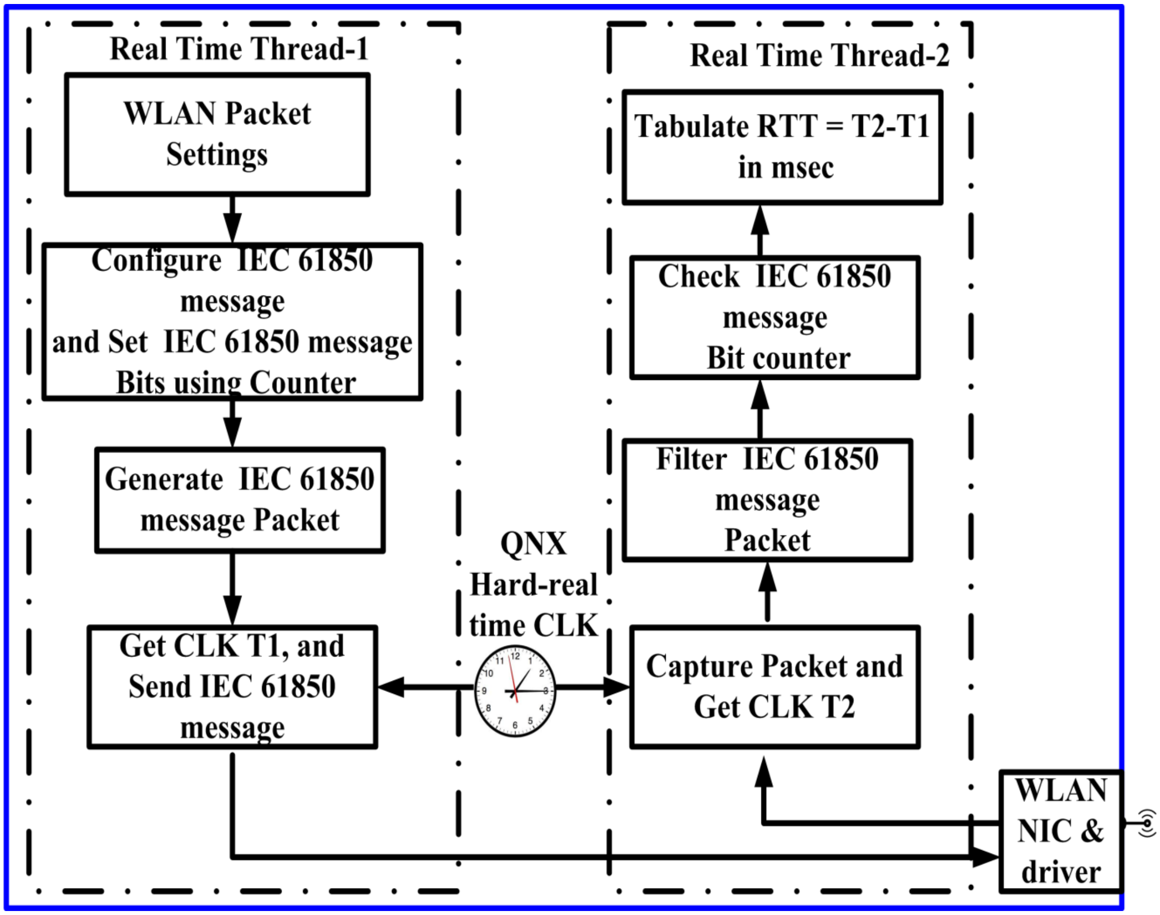


Figure 6-2 Functional block diagram of the developed wireless processing IED

As a part of thread 1, each IEC 61850 message has the following IEC 61850 compliance WLAN settings:

- i. WLAN MAC addresses
- ii. BSS ID
- iii. EtherType / IEC 61850 based AppID
- iv. Unique message ID

WLAN MAC addresses specify source and destination MAC addresses, and BSS ID is applied according to the AP of the wireless LAN. IEC 61850 has already specified the AppID in order to identify the IEC 61850 protocol and message type. Moreover, each IEC 61850 message has been stamped with a unique identification number using a digital counter in order to compute RTT. Another purpose of thread 1 is to configure the IEC

61850 message and also stamp the unique packet ID using a counter. Thereafter, the message is scheduled for communicating over the WLAN, and time of sending message (T1) to the WLAN NIC is registered from the hard real-time clock (CLK) of the QNX system. Thread 2 of the processing IED continuously reads the WLAN NIC card for new packets, and stamps the time (T2) with the received packet using the QNX CLK. The next function is to filter out IEC 61850 messages and identify the packet ID/counter. From the packet ID, thread 2 pulls the message sent time (T1) and subtracts the received time (T2) from the sent time, to compute total RTT.

6.2.2 **Development of Echo IED**

Figure 6-3 shows the major functions developed for the echo IED. Upon receipt of a packet from the processing IED by the packet capture function from the WLAN transceiver driver, the echo IED filters for the IEC 61850 message. The received IEC 61850 messages are dissected to sweep source and destination addresses. Finally, the message is encapsulated and scheduled to send it back to the processing IED over wireless LAN.

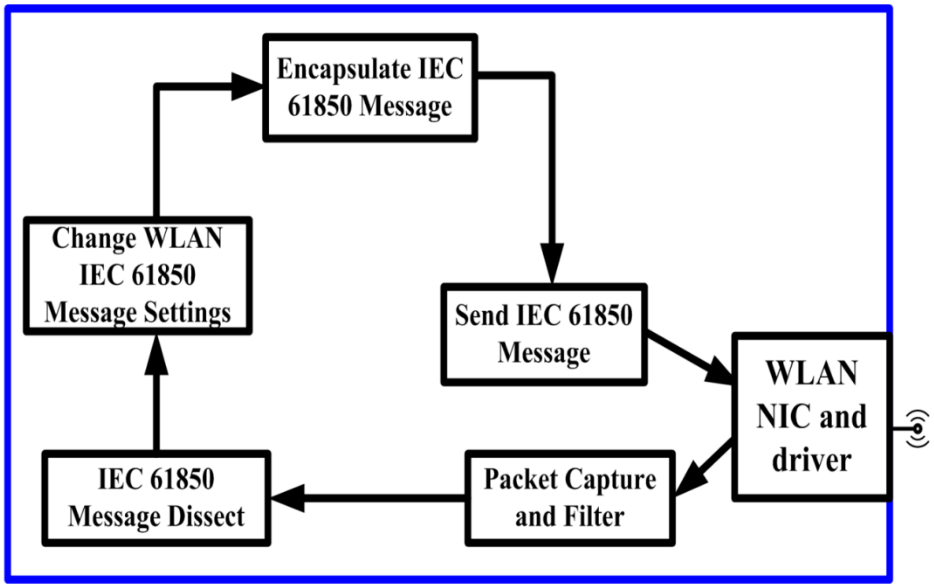


Figure 6-3 Functional block diagram of the developed wireless echo IED

6.2.3 Development of Merging Unit (MU) Playback

Figure 6-4 illustrates the flow for obtaining current signals from the PSCAD/EMTDC simulation tool and conversion of these current data streams into IEC 61850 SV messages. The power system model of a distribution substation and various short-circuit scenarios are simulated using PSCADE/EMTDC. The current signals for all these simulated scenarios are recorded using the COMTRADE file format. On a Windows-based computer, the IEC 61850 SV messages are configured, including WLAN packet settings, and convert COMTRADE data into captured packet file format "*.pcap" using the libpcap tool offline at the required sampling rate. This "SVpkt.pcap" file can be played-back in real-time using the QNX Neutrino RTOS.

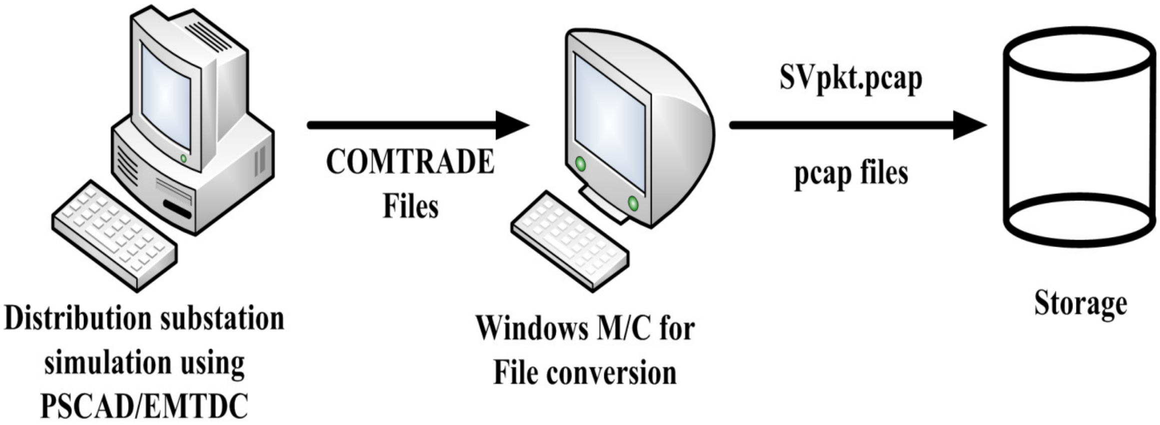


Figure 6-4 Flow of obtaining IEC 61850 raw data messages

The merging unit is implemented as a real-time data playback as shown in Figure 6-5. Since the SVpkt.pcap file is already made available offline, the QNX target machine can schedule the SV packet delivery, also explained in [82], [83]. Two separate threads are implemented to develop the MU: 1) thread 1 plays-back the SV messages, and sends them to the protection IED; 2) thread 2 captures the IEC 61850 GOOSE messages over wireless LAN, as shown in Figure 6-5. Thread 1 schedules an SV stream of WLAN data at 480 Hz and registers the QNX CLK time of SV messages corresponding to fault inception (T1). Thread 2 captures WLAN messages and filters for IEC 61850 GOOSE. Upon reception of GOOSE (Trip) message from protection IED, the MU gets the

GOOSE reception time (T2) from hard-real time clock, which is used to calculate the total time of protection operation (which also includes communication network delays of SV and GOOSE)

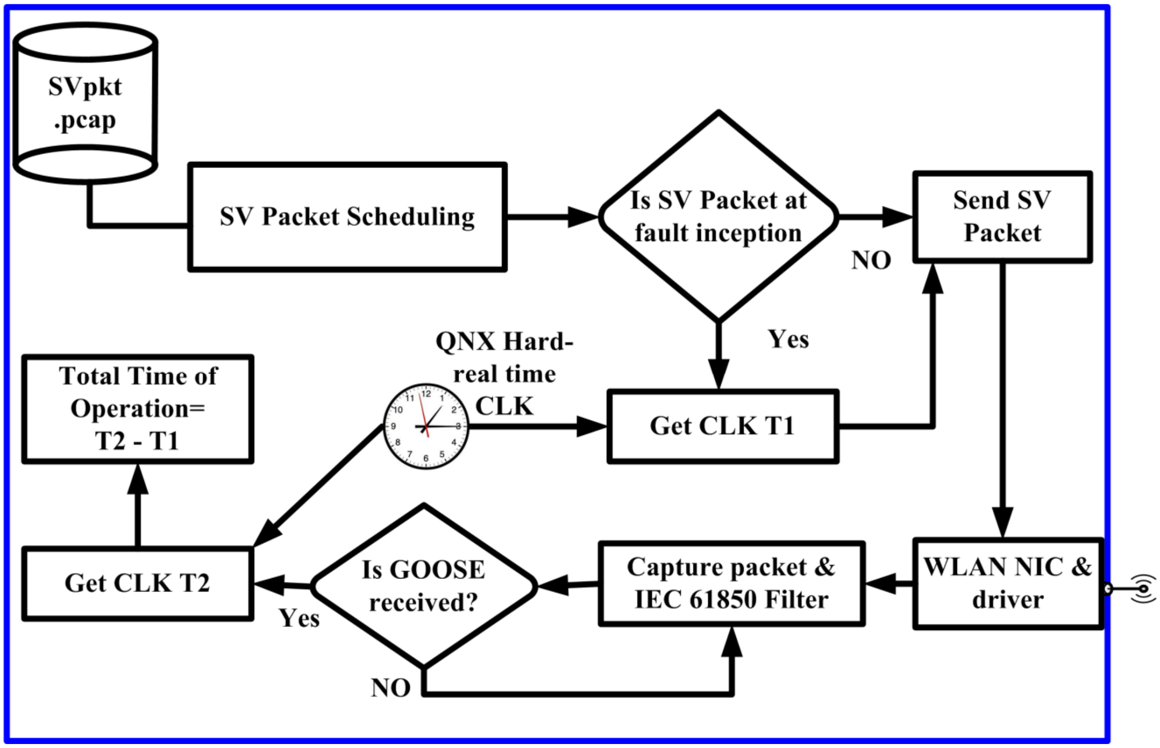


Figure 6-5 Functional block diagram of the developed wireless MU

6.2.4 Development of Protection and Control (P&C) IED

The P&C IED developed for distribution feeder protection is illustrated in Figure 6-6. Once the protection IED opens the communication port with the WLAN NIC driver using libpcap, it starts capturing packets over the WLAN network, and it filters the packets for IEC 61850 SV messages. The current signal value is dissected from each SV message and stored in a buffer. The short-circuit condition is detected, and time of operation is determined by a time-over-current (TOC) protection function (meaning PTOC Logical Nodes of IEC 61850) as discussed in the Appendix. The IEC 61850 GOOSE message is configured to send a TRIP signal to the MU.

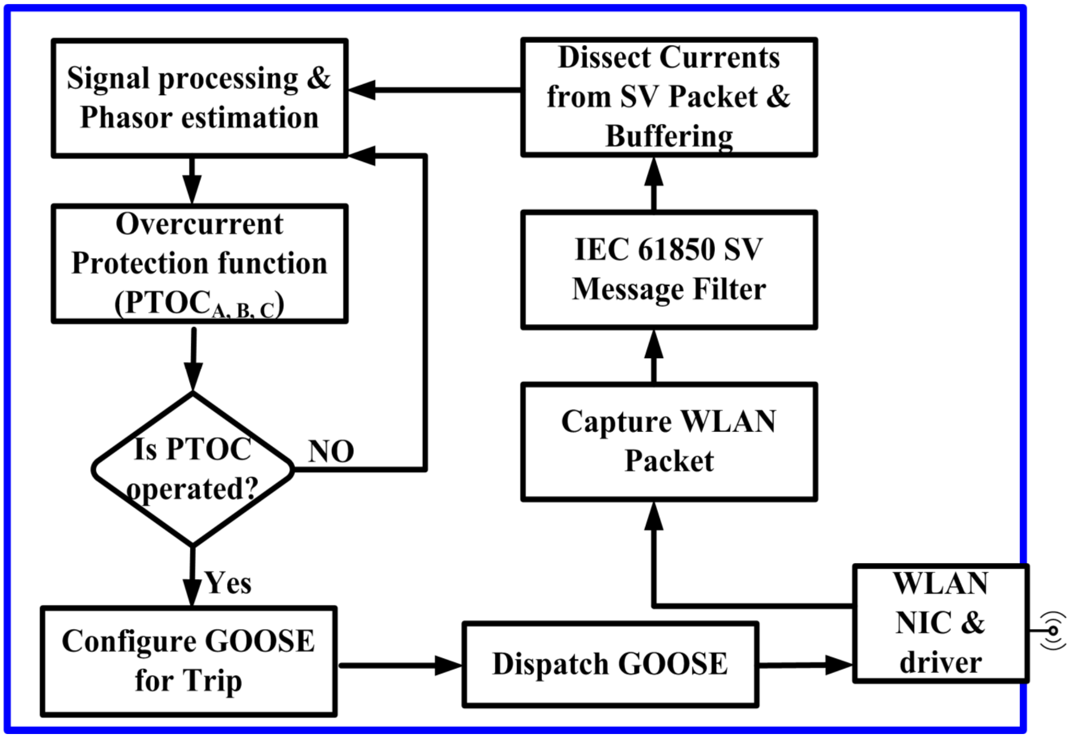
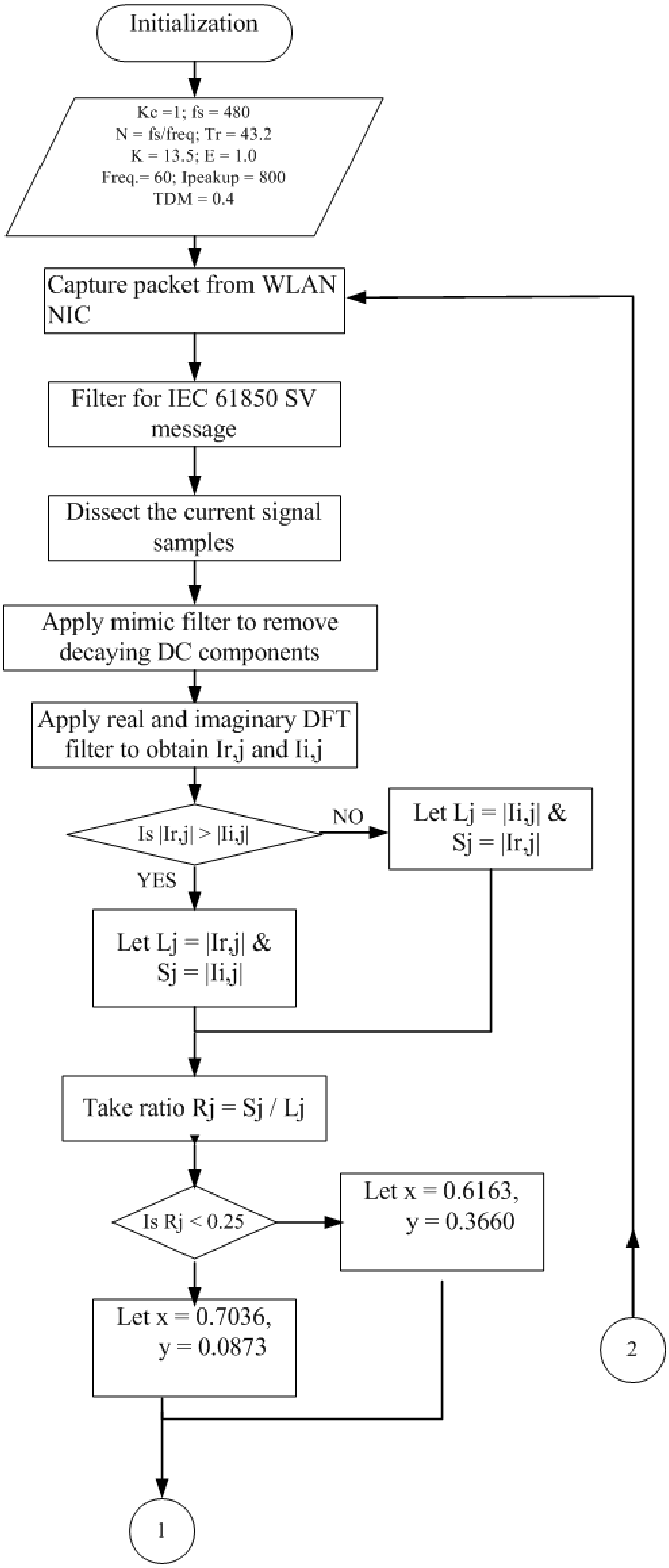


Figure 6-6 Functional flowchart of wireless P&C IED

The functional flowchart of digital over-current protection element (PTOC) implemented in the wireless P&C IED is shown in Figure 6-7. The digital over-current protection algorithm is developed based on [83]. When starting, the device initializes the settings and constants of the algorithm, mainly related to over-current characteristic and filtering values. Once the protection IED opens the communication port with the WLAN NIC driver using libpcap, it starts capturing packets from the NIC buffer, and filters the packets for IEC 61850 SV messages. The digital values of all three phase and neutral current signals are dissected from SVs, and a mimic (differentiator) filter is applied on these raw data streams to remove decaying DC components from current signals. The RMS values of the currents are estimated from real and imaginary components of the phasors (obtained using Discrete Fourier Transformation (DFT) filters for real and imaginary parts) using the piecewise linear approximation technique [85] as well as two region approximation coefficients [83]. As shown in Figure 6-7, the values of coefficients (x and y) for two region approximations are multiplied with large (L) and small (S) components of the current phasors. And, the multiple of pickup (M_j) is calculated by taking the ratio of current RMS with its pickup (that is, settings of the over-current element), which is part of the protection operating time (t_j) equation of inverse-time-over-current characteristics. To determine the time delay corresponding to the current in the protected equipment, the integration/sum of all instants of operating time (t_j) at sampling frequency (time difference) needs to be carried out [86]. Finally, if this summation/integration is higher than operating area (Kc), then the over-current element picks up. This pickup of the over-current protection element is communicated to the MU over wireless LAN using IEC 61850 GOOSE. Therefore, the over-current trip bit is set to high in the GOOSE message, and it is retransmitted several times using the WLAN NIC.


Initialization
Kc =1; fs = 480
N = fs/freq; Tr = 43.2
K = 13.5; E = 1.0
Freq.= 60; Ipeakup = 800
TDM = 0.4
Capture packet from WLAN NIC
Filter for IEC 61850 SV message
Dissect the current signal samples
Apply mimic filter to remove decaying DC components
Apply real and imaginary DFT filter to obtain Ir,j and Ii,j
Is |Ir,j| > |Ii,j|
NO
Let Lj = |Ii,j| & Sj = |Ir,j|
YES
Let Lj = |Ir,j| & Sj = |Ii,j|
Take ratio Rj = Sj / Lj
Is Rj < 0.25
Let x = 0.6163, y = 0.3660
Let x = 0.7036, y = 0.0873
2
1

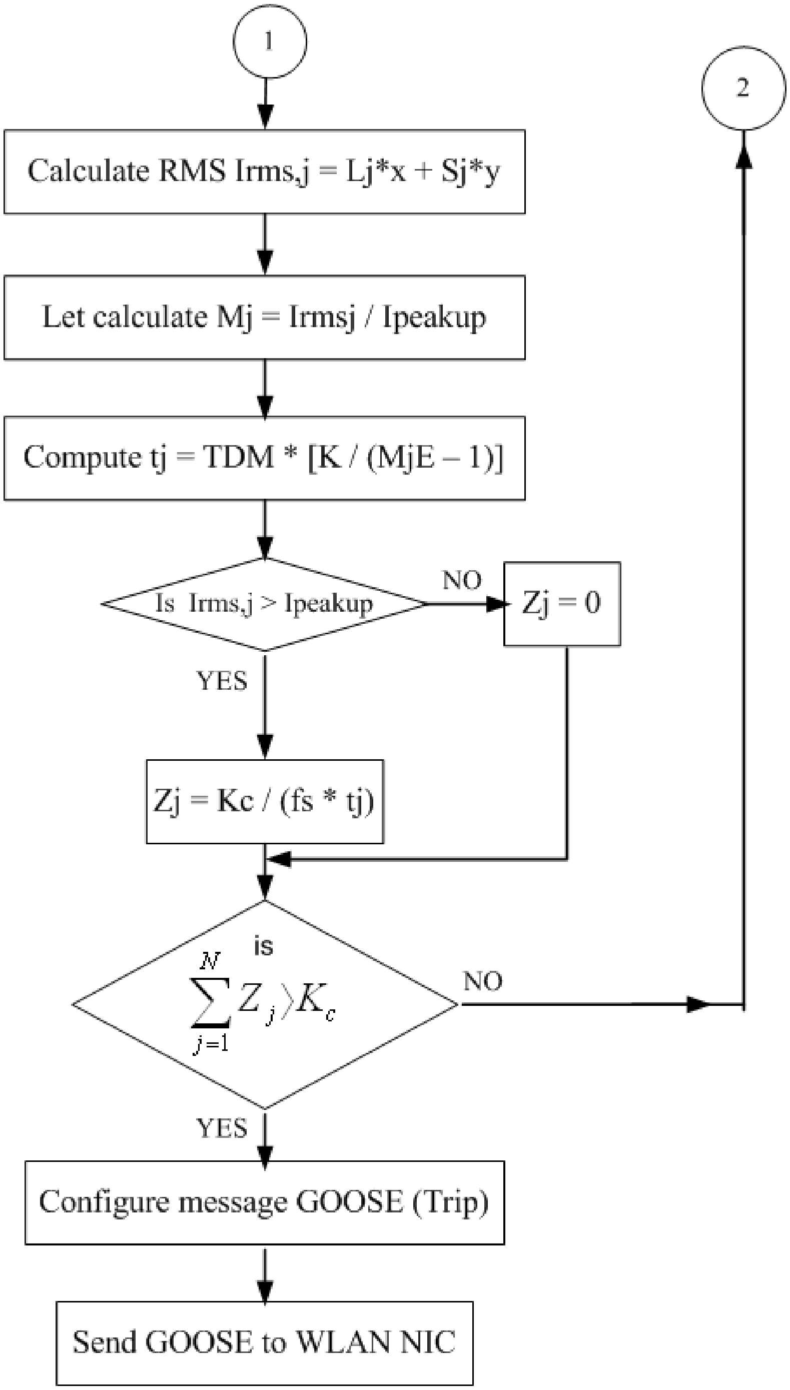


Figure 6-7 Functional flowchart of over-current protection element

These developed devices can be used to playback the IEC 61850 messages in real-time and calculate RTT accurately. Further details are discussed in the next section.

6.3 Distribution Automation Laboratory Setup

Figure 6-8 shows the laboratory test set-up to investigate the performance of wireless LAN for the IEC 61850 based distribution substation. The substation protection and automation devices (as a part of substation control room) were deployed in the laboratory, and included wireless IEDs, wireless access point, spectrum analyzer, network analyzer, and traffic generator, as shown. The field devices, such as two MUs and radio noise sources, were installed outside the laboratory at a distance of 45 feet.

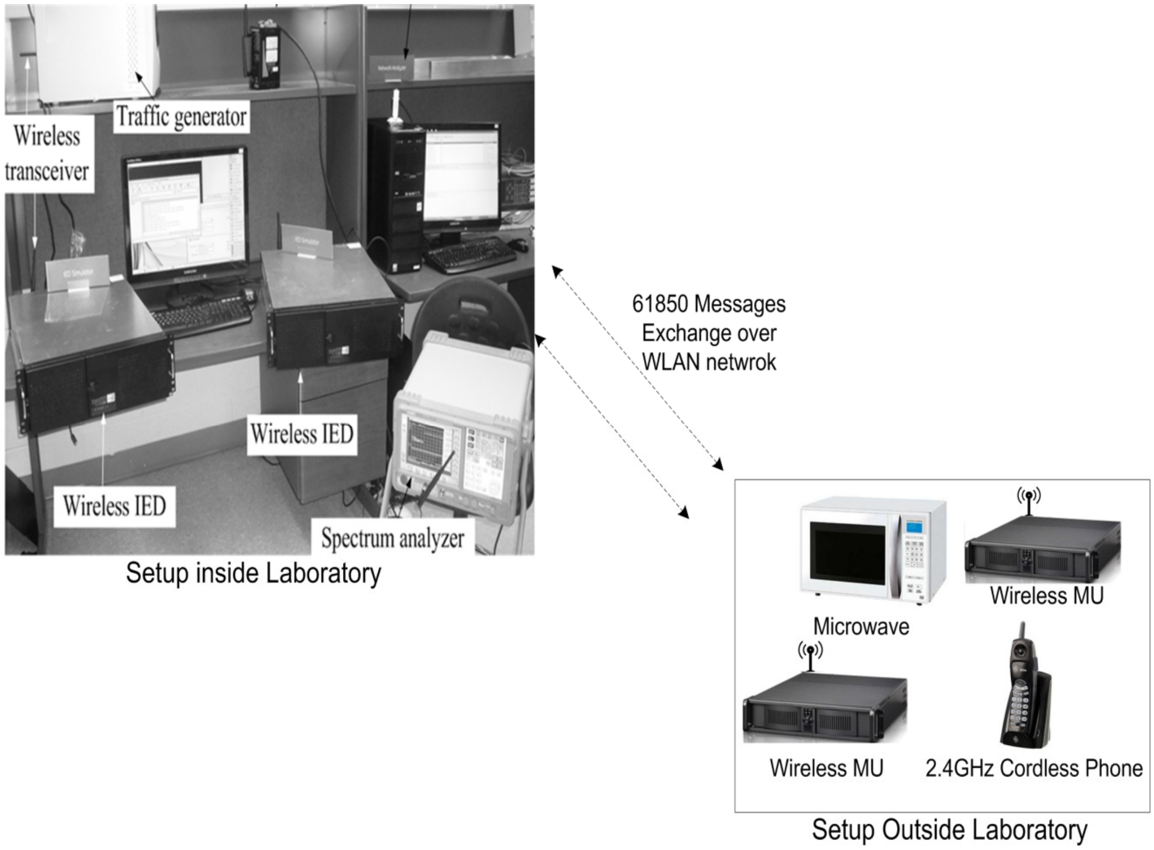


Figure 6-8 Wireless LAN setup within laboratory

6.3.1 Configuring the Wireless AP Network

Wireless IEDs, MUs, and traffic generators were developed using industrial embedded computers with real-time platforms as discussed in the previous section. A commercial wireless AP designed for the substation environment was used in this setup, as shown in Figure 6-9. The wireless AP [87] facilitates the communication among wireless IEDs within the wireless LAN. Moreover, wireless AP also allows security networks based on IEEE 802.11i [70], plus IEEE 802.1X/RADIUS for wireless user traffic and distribution of dynamic encryption keys, and QoS based on IEEE 802.1Q.

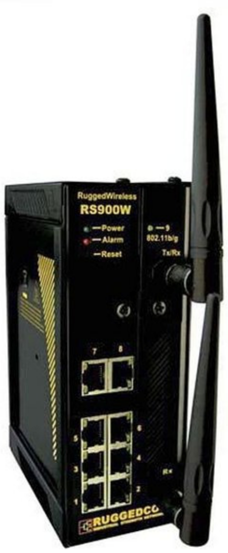


Figure 6-9 Industrial wireless LAN access point

The developed industrial-harden WLAN in the laboratory not only enhanced network security, but also facilitated reliable communication links and additional noise attenuation features, which are very promising for next-generation communication infrastructure for the smart grid.

6.3.2 **Radio Noise and Traffic Generator**

Various levels of electro-magnetic interferences were generated using a microwave oven and a cordless phone, while radio frequency interferences from other wireless LAN devices were obtained using a wireless traffic generator that can inject various types of messages over different WLAN channels.

6.3.3 Spectrum and Network Analyzers

A spectrum analyzer was used to measure radio noise and interference levels within the setup. AirPcap with the Pilot tool was used as a network analyzer to monitor and analyze the substation wireless LAN. The network analyzer was configured in promiscuous mode to sniff all the packets from the entire IEEE 802.11 based wireless LANs. It captured all the data packets from the network, and it displayed all statistics of network traffic, signal, and noise strength at each wireless transceiver, and so on.

Using this laboratory setup, testing of various scenarios was carried out to investigate the performance of wireless LAN for various smart distribution substation applications. In order to examine performance of the smart distribution substation applications, the round-trip-time of messages and throughput were evaluated. Each message was tagged with a unique 32-bit identification number in the message field; therefore the sending-end wireless device was able to differentiate messages in order to calculate RTT. This RTT included message formation, queuing, transmission, propagation delay over the air medium, communication delay over the wireless AP, receipt time, message dissection, change of address, and same delays while communicating the same message back to the sending-end device.

6.4 Laboratory Results for Distribution Control and Monitoring Applications

To study the performance of IEC 61850 based WLAN for control and monitoring applications, the RTT of the GOOSE message was measured by setting up processing and echo IEDs in the described laboratory.

IEEE 802.11 technologies offer various data rates and spread spectrum as well as OFDM encoding technologies, as discussed in Chapter 2. For this study, the technologies and their data rates considered for this analysis were: 1) IEEE 802.11b at 1 Mpbs data rate; 2)

IEEE 802.11b at 11 Mpbs data rate; 3) IEEE 802.11g at 54 Mpbs data rate; and 4) IEEE 802.11a at 54 Mpbs data rate.

Figure 6-10 shows the RTT delay of IEEE 802.11b technology at the 1 Mbps data rate. Average delay of GOOSE was 4.1 ms, while maximum delay was around 15.2 ms.

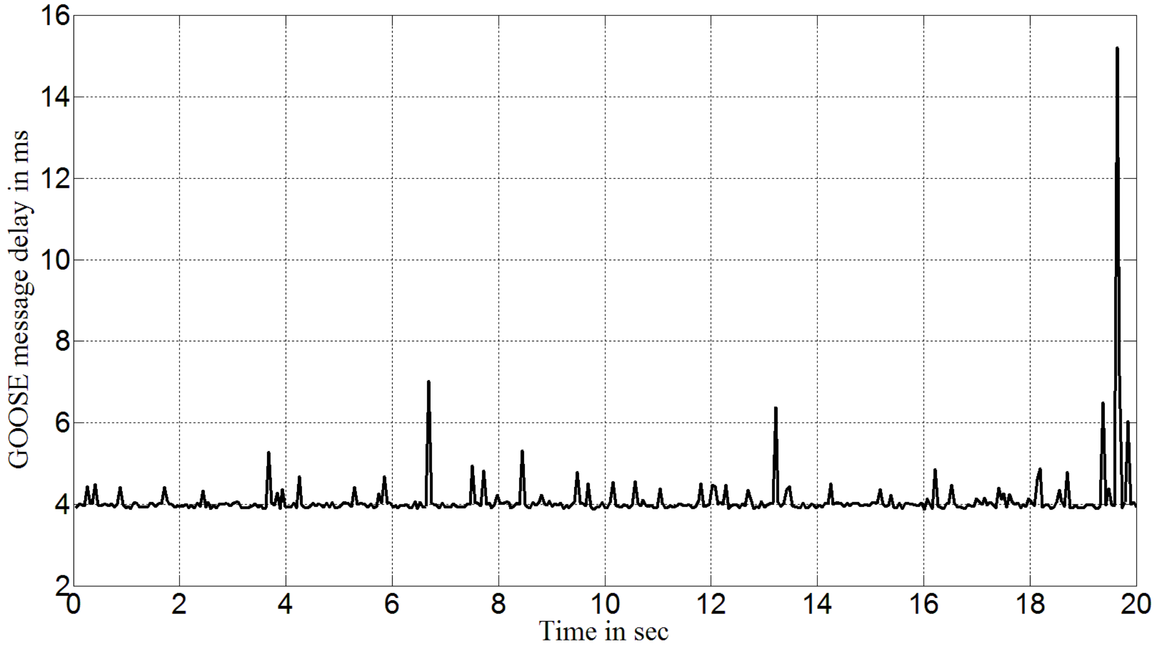


Figure 6-10 GOOSE message delay of IEEE 802.11b technology with 1 Mbps data rate

The delay of GOOSE messages with the IEEE 802.11b technology at the highest data rate possible (11Mpbs) is shown in Figure 6-11. The average and maximum GOOSE RTTs were reduced to 3.8 ms and 6.7 ms respectively due to the increased data rate.

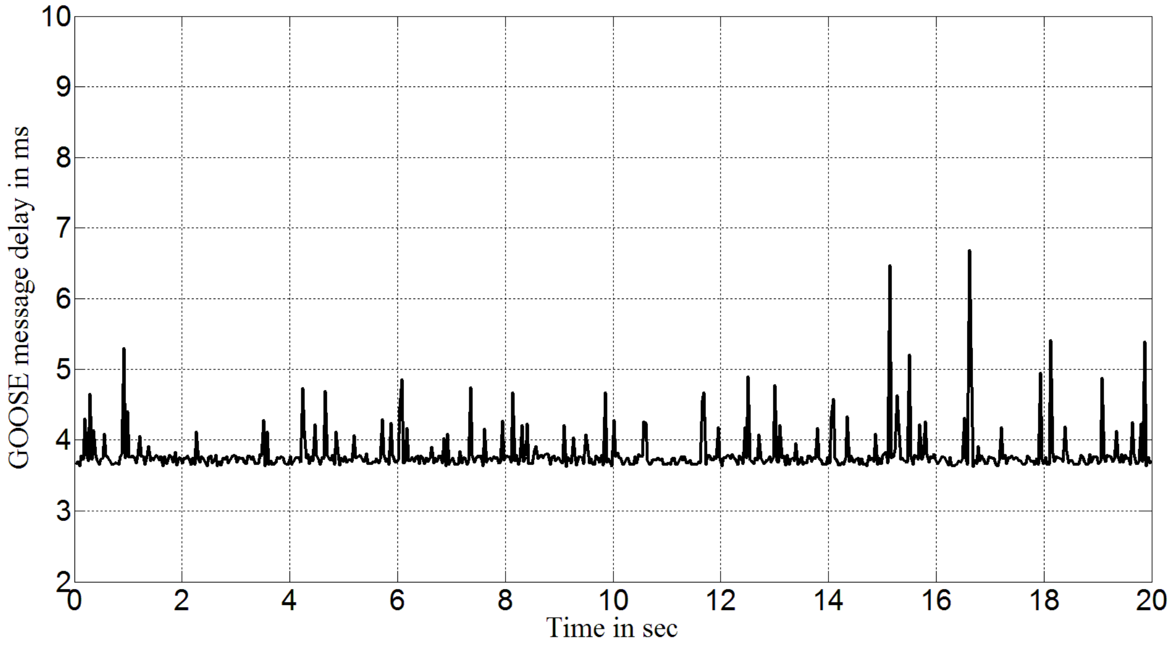


Figure 6-11 GOOSE RTT delay of IEEE 802.11b technology with 11 Mbps data rate

Figure 6-12 illustrates the GOOSE RTT delay of IEEE 802.11g technology with the highest available data rate of 54 Mpbs. With this higher data rate, the maximum delay reduced to 4.2 ms, and average delay was around 3.5 ms.

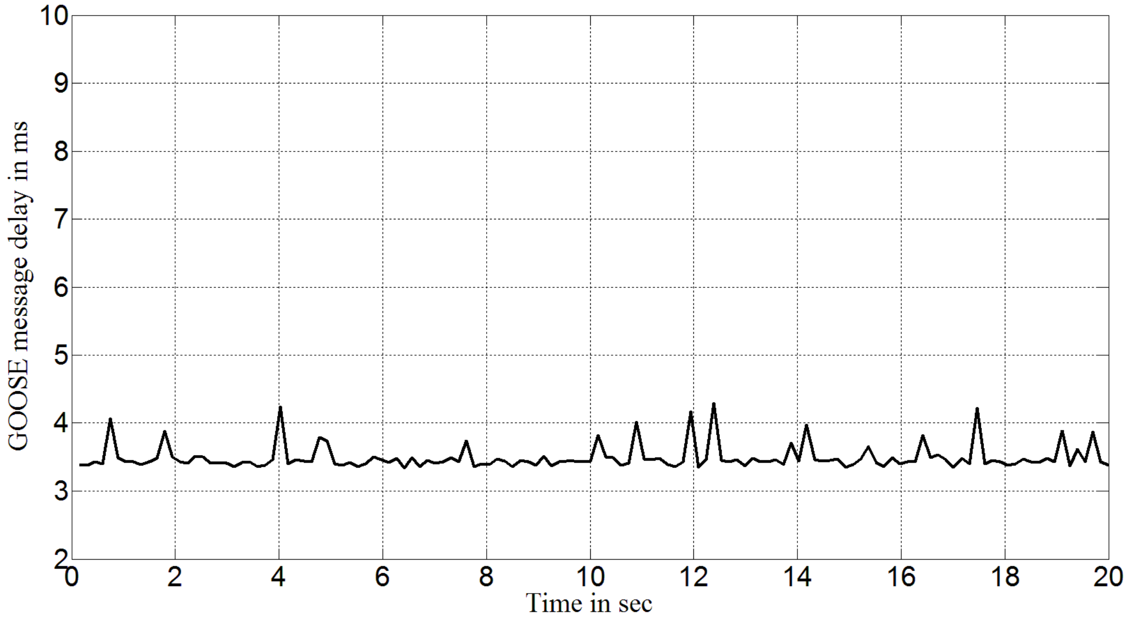


Figure 6-12 GOOSE RTT delay of IEEE 802.11g technology with 54 Mbps data rate

The effect of IEEE 802.11a technology with a 54 Mbps data rate on GOOSE RTT delay is shown in Figure 6-13. This technology significantly improves the GOOSE RTT average delay to 1.43 ms and maximum delay to 1.48 ms.

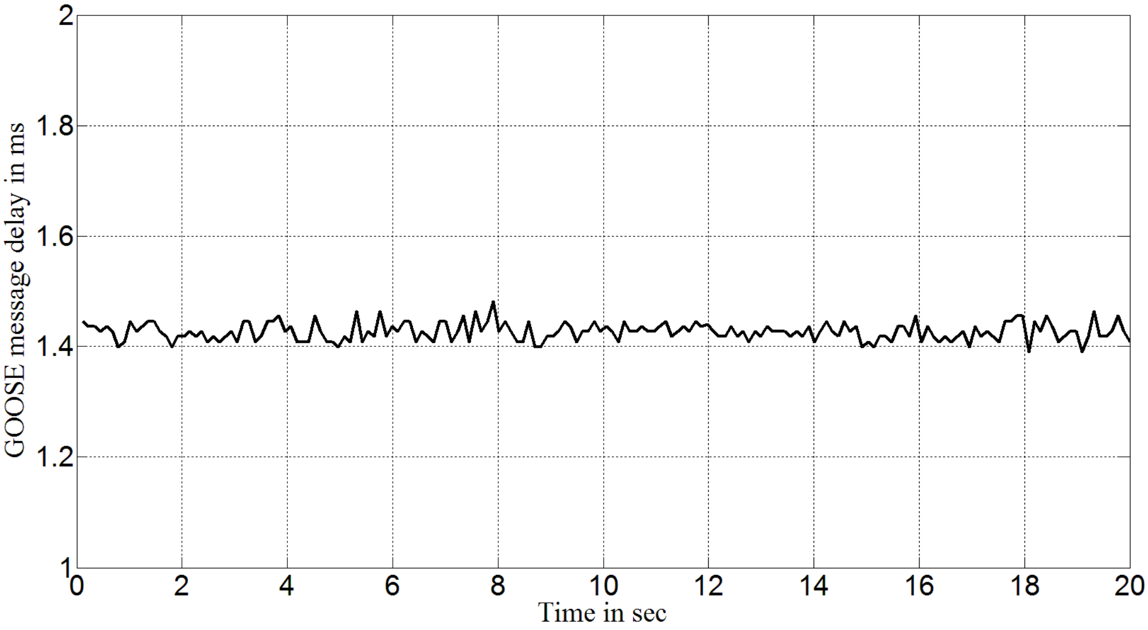


Figure 6-13 GOOSE RTT delay of IEEE 802.11a technology with 54 Mbps data rate

6.5 Laboratory Results for Distribution Automation and Metering Applications

Testing of RTT delay for client/server (IP message) applications is discussed in this section. IEEE a/b/g technologies with various data rates were used.

The RTT of IP messages is shown in Figure 6-14 for IEEE 802.11b technology at 1 Mbps data rate. The average delay of the message communication was 96 ms, while maximum delay was 320 ms. Moreover, client/server messages experienced a jump in communication delay due to the limited data rate. This behavior indicates insufficient availability of bandwidth (1 Mbps).

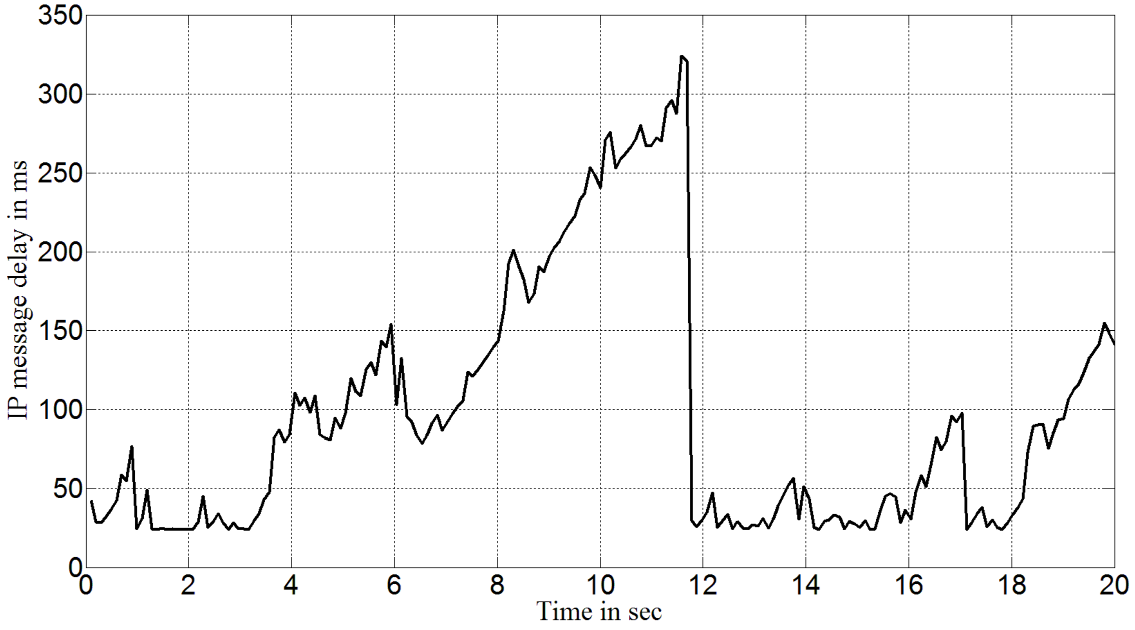


Figure 6-14 IP RTT delay of IEEE 802.11b technology with 1Mbps data rate

The IP RTT delay from IEEE 802.11b technology with an 11Mbps data rate is illustrated in Figure 6-15. The maximum delay of the IP message was around 104 ms, and average RTT delay calculated as 45 ms. At the same time, the delay locus shows some gradual rise in delay, which occurred due to the lower data rate offered by this technology.

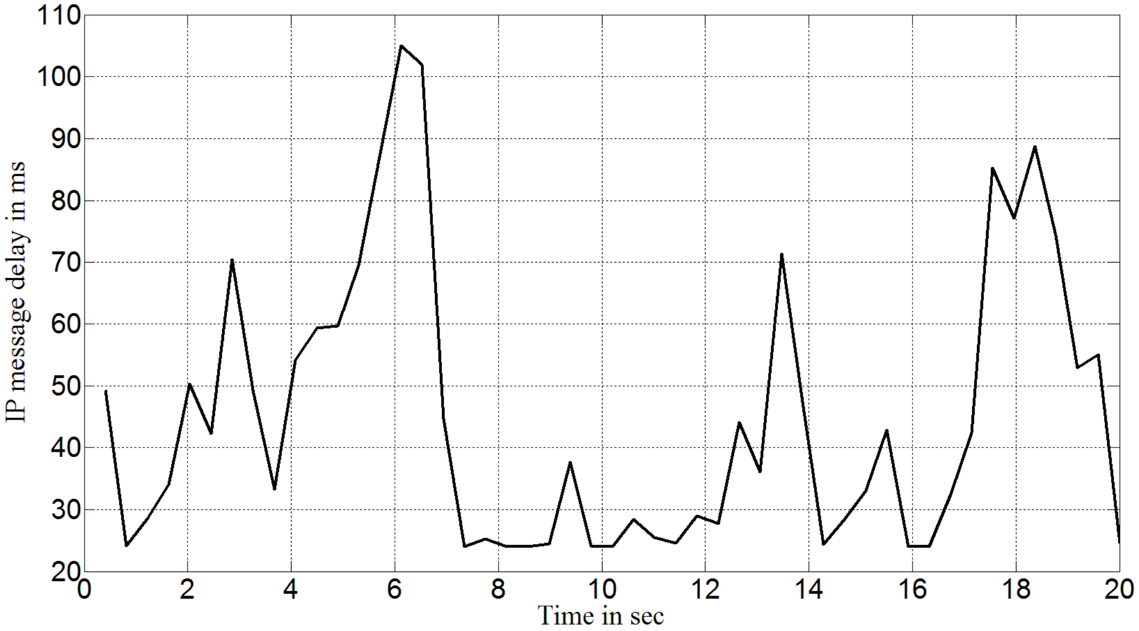


Figure 6-15 IP RTT delay of IEEE 802.11b technology with 11 Mbps data rate

Figure 6-16 shows the RTT delay of IP messages for IEEE 802.11g technology with 54 Mbps data rate. The maximum delay was 26 ms, and average delay was 24 ms. The network delay was more stable and smooth compared to the IEEE 802.11b technology.

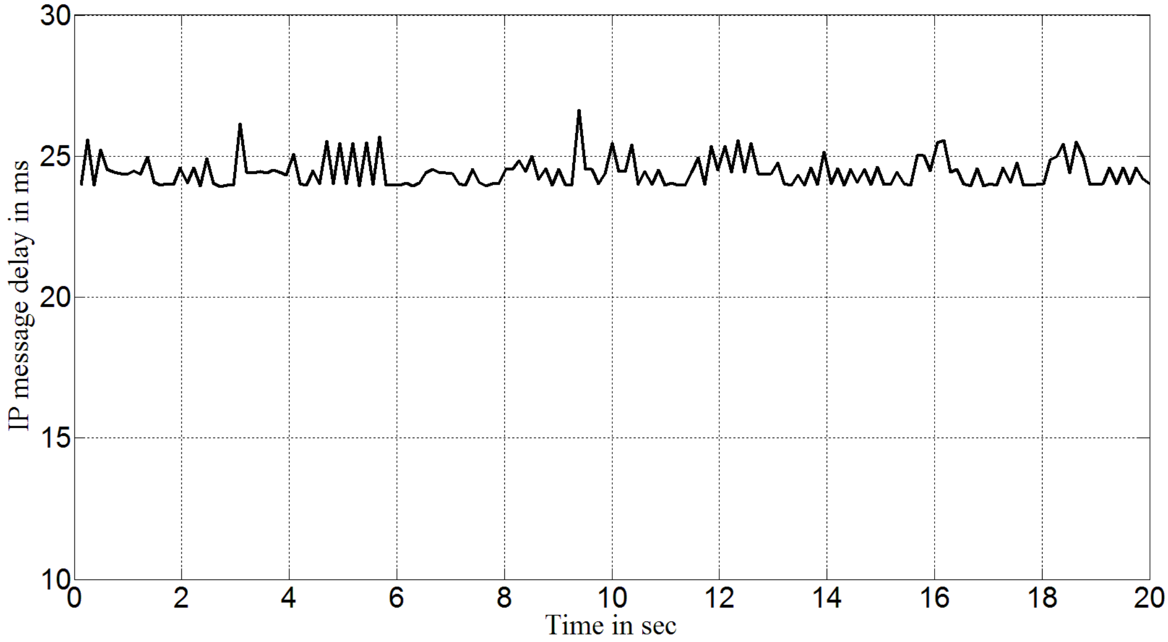


Figure 6-16 IP RTT delay of IEEE 802.11g technology with 54 Mbps data rate

The RTT delay of IP messages with IEEE 802.11a technology at the 54 Mbps data rate is shown in Figure 6-17. A significant reduction in delay was observed. IEEE 802.11a offered an average delay of 8.3 ms and 8.7 ms maximum delay.

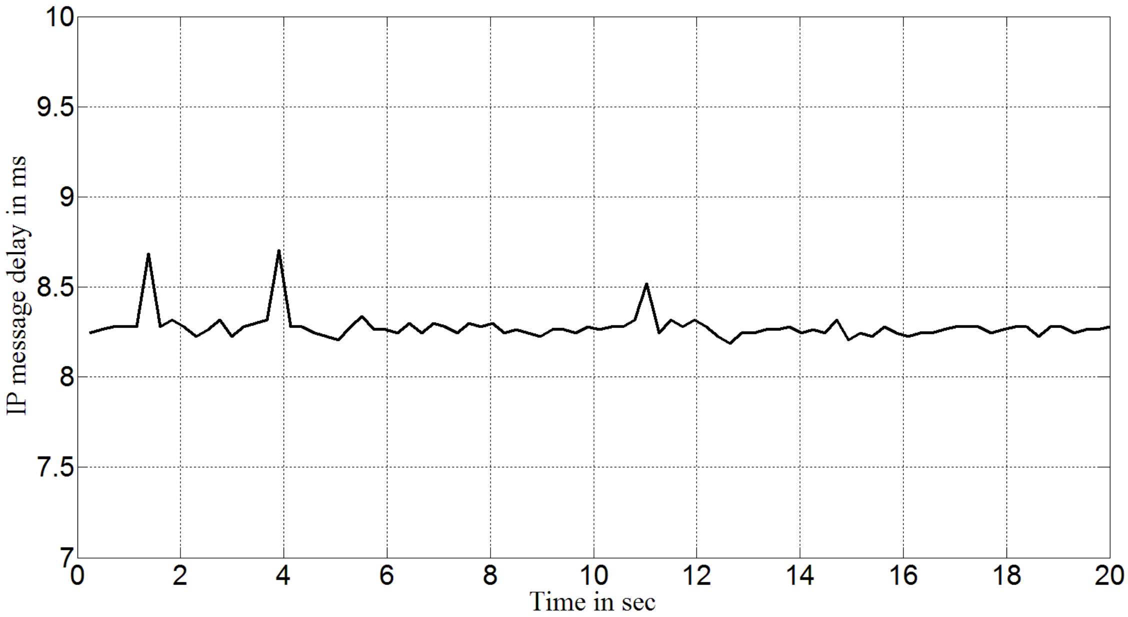


Figure 6-17 IP RTT delay of IEEE 802.11a technology with 54Mbps data rate

6.6 Laboratory Results for Distribution Feeder Protection Applications

Performance of distribution substation over-current protection using wireless LAN communication network was tested in the laboratory. The wireless protection IED and the merging unit device developed in the laboratory were used for testing. Performance results of the over-current element are discussed.

The results for the over-current element operation for different values of M (multiple of pick-up) are tabulated in Table 6-1 for the AG (A-phase to Ground) fault element. The maximum difference between time of operation obtained from MATLAB (which does not include any communication delay) and the WLAN field setup (including WLAN communication delay) was 4.71% (14.52 ms), which is not significant for distribution substation protection.

Table 6-1 Performance of WLAN for over-current protection applications

TDM	Over-current Relay Operating Time (AG Fault)

	MATLAB simulation (no comm. delay) (in sec)	From hardware testing (in sec)	Difference (comm. delay) (in sec)	Difference (%)
0.05	0.19373	0.201	0.00727	3.75
0.10	0.30833	0.3228	0.01452	4.71
0.20	0.5375	0.561	0.0235	4.37
0.40	0.995833	1.012	0.01616	1.62
0.60	1.4521	1.472	0.02002	1.37
0.80	1.91041	1.925	0.01459	0.76
1.00	2.531	2.55	0.01938	0.77

6.7 Effect of Noise Level

Testing was done to analyze the time-critical GOOSE message delays for various noise levels. The signal-to-noise ratio (SNR) was measured using the AirPcap network analyzer in the laboratory. Noise levels were generated using a microwave oven, cordless phones, and a traffic generator. It can be observed from Figure 6-18 that the GOOSE message delay increased from 5 ms to 10.2 ms, and that the throughput of WLAN reduced to 6930 Kbps as the SNR reduces from 23 dB to 11 dB. The noisy environment caused higher bit-error-rate in a message, and therefore the message may have been discarded at the receiver. Thus, the same message had to be retransmitted over the network, which can cause higher delays. Nevertheless, the delays obtained for the GOOSE messages were still within the allowable time delay requirements (10 ms ETE delay or 20 ms RTT).

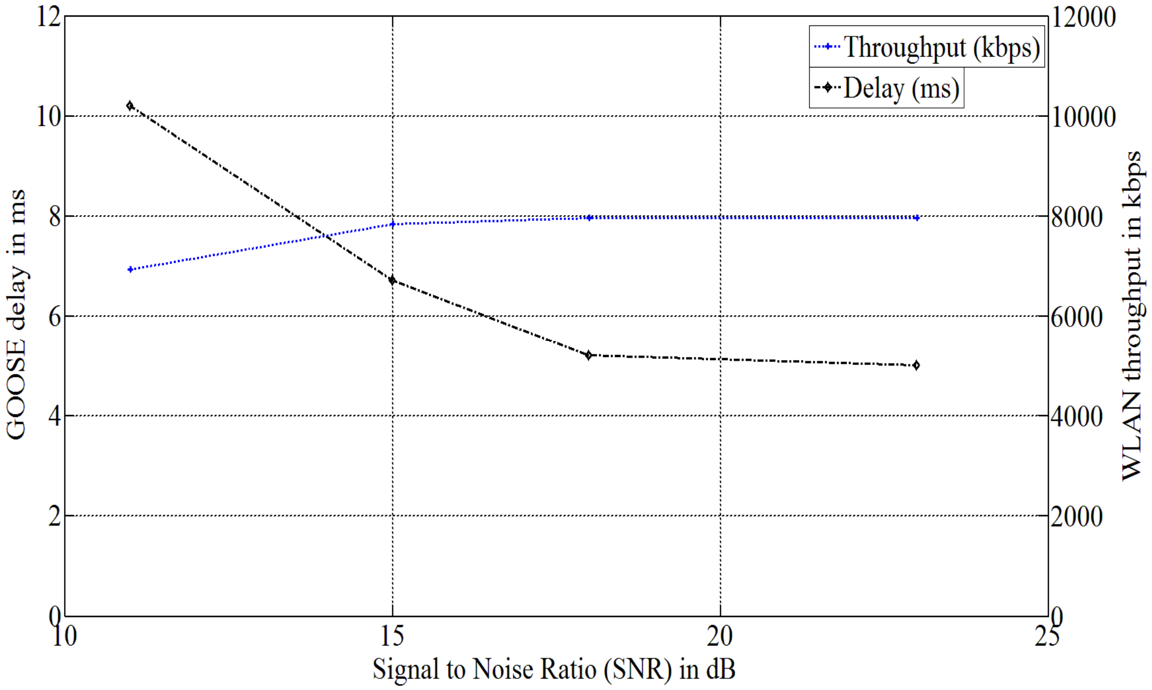


Figure 6-18 GOOSE delays with various noise level and throughput.

6.8 Summary

The prototype development of four WLAN-enabled IEC 61850 devices, meaning 1) the processing IED; 2) echo IED; 3) merging unit; and 4) protection and control IED were proposed in this chapter in order to study performance of substation control, monitoring, and protection applications. In addition to IEC 61850 prototype IEDs, the laboratory setup also utilized a network analyzer, spectrum analyzer, traffic generator, and WLAN access point. Different WLAN technologies, such as IEEE 802.11 (1 Mbps), IEEE 802.11b (11 Mbps), IEEE 802.11g (54 Mbps), and IEEE 802.11a (54 Mbps), were considered for this analysis, by installing switchyard devices (MU and echo IEDs) 45 feet from the laboratory. Smart distribution control and monitoring applications were deployed using GOOSE messages, whereas automation and metering applications utilized IP messages. The protection applications were employed using SV (from MU to protection IED) as well as GOOSE (from protection IED to MU). For control and monitoring applications with higher data rate (54 Mbps), the maximum GOOSE delay was reduced from 15.2 ms to 4.2 ms, and average delay fell from 4.1 ms to 3.5 ms. The maximum and average delays using IEEE 802.11a technology (54 Mbps) were 1.48 and 1.43 ms respectively. Similarly, for automation and metering application, the maximum delays were 26 ms and 8.7 ms with IEEE 802.11g (54 Mbps) and IEEE 802.11a (54 Mbps) technologies respectively. For the distribution feeder protection application, the maximum difference between time of operation obtained from MATLAB and WLAN field setup was 4.71% (14.52 ms), which can be tolerated for distribution substation protection. Furthermore, the qualitative match in values was observed by comparing results obtained using OPNET simulation and the laboratory setup. Some minor differences in the results (between hardware setup and OPNET simulations) were possibly due to various parameters related to QNX processing time for delay measurements, throughput processing delay of the network analyzer, QNX task priority, and/or hardware buffering and processing, which were difficult to account.

Chapter 7

7. Field Setup and Testing in Distribution Substations

This chapter presents assessment of WLAN-enabled devices in a harsh environment of a distribution substation. Five substation site visits were conducted at 13.8 and 27.6 kV distribution voltage levels in London, Ontario, owned by London Hydro and Hydro One. The field testing was carried out using wireless LAN IEDs installed in a substation switchyard at one end and in a control room at another end, with switching of the circuit breaker (CB) at full load current. The performance of distribution substation applications, such as control and monitoring (IEC 61850 GOOSE messages), automation and metering (client/server communication using IP messages), and over-current protection (using SV and GOOSE messages) is presented in this chapter.

7.1 Distribution Substation Setup for Field Testing

As explained in Chapter 2, the smart distribution substation applications are classified in three types of IEC 61850 defined messages, these being GOOSE, IP (client/server), and sampled values. Figure 7-1 shows the on-site measurement setup at the London Hydro distribution substation. A remote MU (close to switchgear) communicated SVs and client/server messages to the wireless P&C IED within the corresponding BSS (Basic Service Set, which is established by WLAN AP). A P&C IED sent GOOSE messages to the MU. Processing and echo IEDs exchanged client/server IP and GOOSE messages using wireless AP. The distance between the control room to the switchyard was approximately 12 meters for 13.8 kV substations and around 75 meters for 27.6 kV substations. The performance of distribution control and monitoring, automation and metering, and protection applications is demonstrated in following sections.

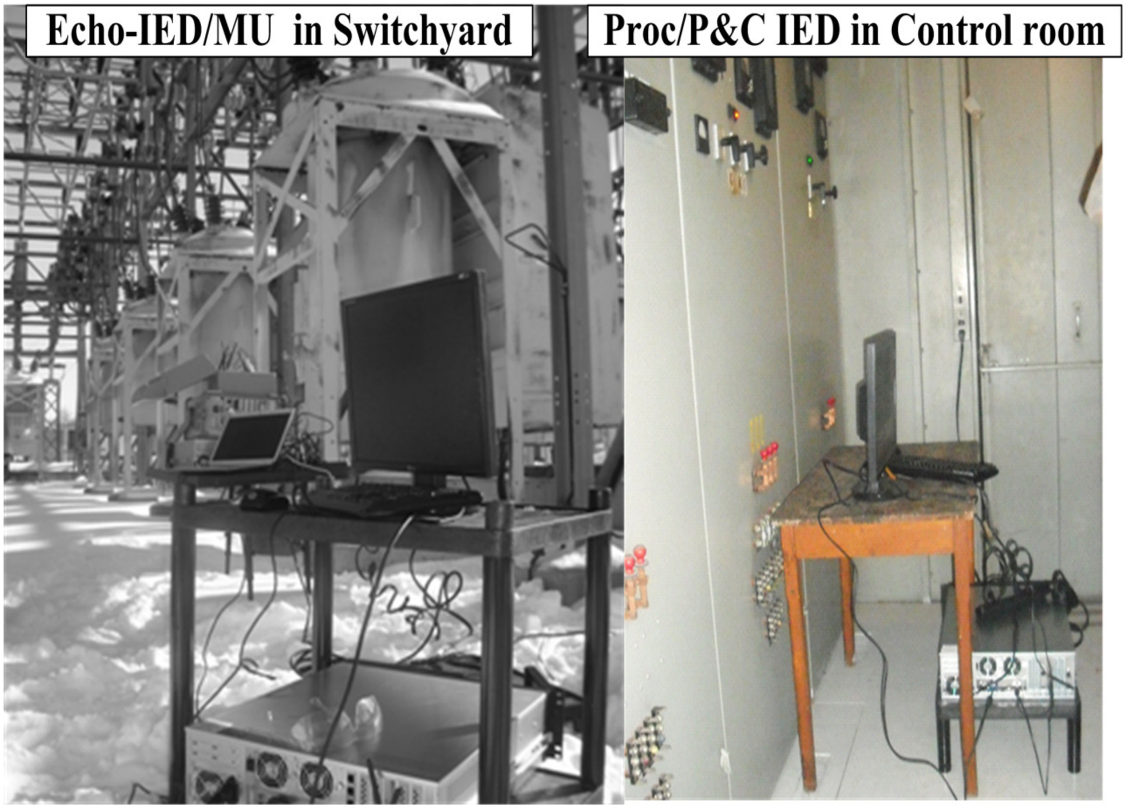


Figure 7-1 Substation field setup

7.2 Field Testing of Control and Monitoring Applications in 13.8 kV Substations

Figure 7-2 illustrates the peer-to-peer GOOSE message delay measurement setup. Industrial embedded systems with wireless LAN features were developed to test delay of IEC 61850 GOOSE messages for peer-to-peer applications. The processing IED sent GOOSE message with sequence number stamped on it and registered the GOOSE sending time using hard real-time timers of the QNX real-time operating system. The echo IED received the GOOSE messages, reversed the source and destination MAC addresses, and sent the same GOOSE messages. The processing IED received the GOOSE-echo messages, registered the receipt times, and matched the sequence numbers. Round-trip-time of the GOOSE messages was calculated by subtracting the receipt times of GOOSE-echo messages with sending times of GOOSE messages, for the messages with the identical sequence numbers. If a GOOSE message with a particular sequence number was not received by the end of the testing duration, it was declared to be lost.

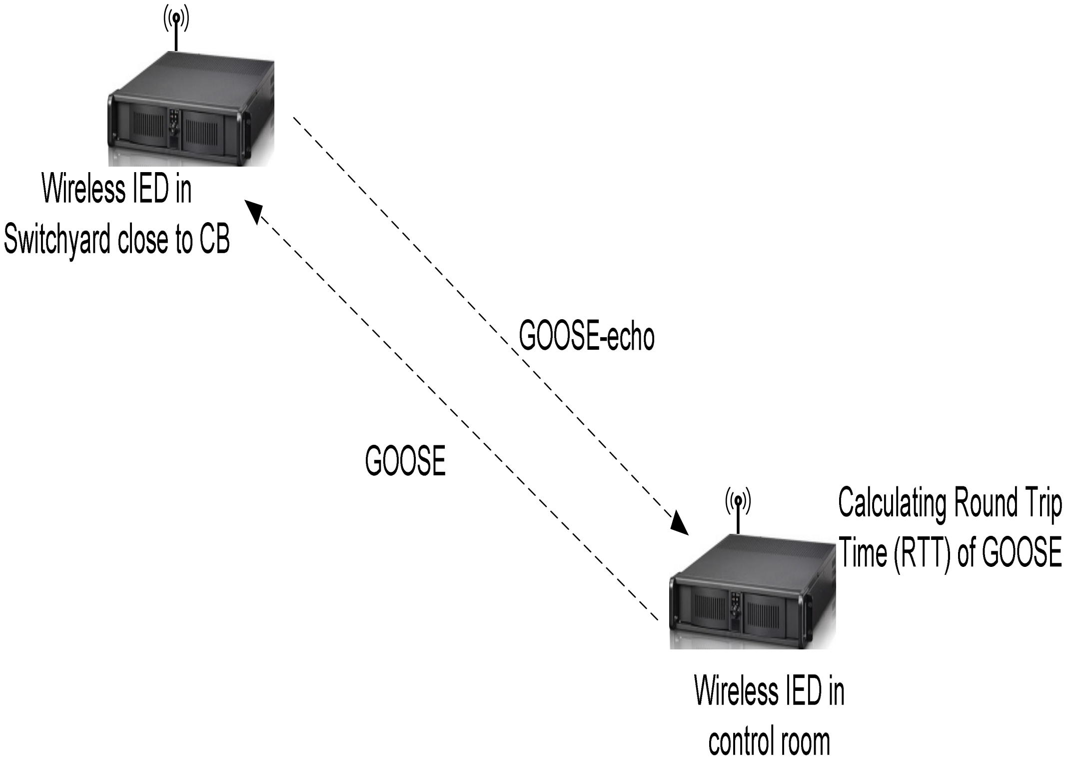


Figure 7-2 Peer-to-peer GOOSE RTT measurement setup

The results obtained from field testing of peer-to-peer GOOSE application are discussed in this chapter. Two 13.8 kV and two 27.6 kV substations were visited for this analysis. The wireless LAN IEDs developed using an industrial computer with QNX real-time operating system were used in this setup. The RTT of GOOSE messages was obtained for various switching scenarios.

7.2.1 **13.8 kV Substation 1**

Figure 7-3 shows the wireless IED, which was near the 13.8 kV circuit breaker enclosure. A second wireless IED was installed at another end of the substation (approximately 12 meters). The GOOSE messages were sent from the processing IED to the echo IED installed at the circuit breaker. The RTT of GOOSE messages was observed with and without circuit breaker switching operation (open/close).

Figure 7-3 Wireless IED near 13.8 kV circuit breaker

Figure 7-4 and Figure 7-5 show the end-to-end delay of the GOOSE signal at the 13.8 kV distribution substation during normal operation and during load disconnection. In both the cases, average GOOSE RTT was around 3.35 ms, while maximum RTT was around 8 ms, which was well within the allowed GOOSE delay time requirements. Thus, the switching operation of the circuit breaker did not have any impact on the GOOSE delay values.

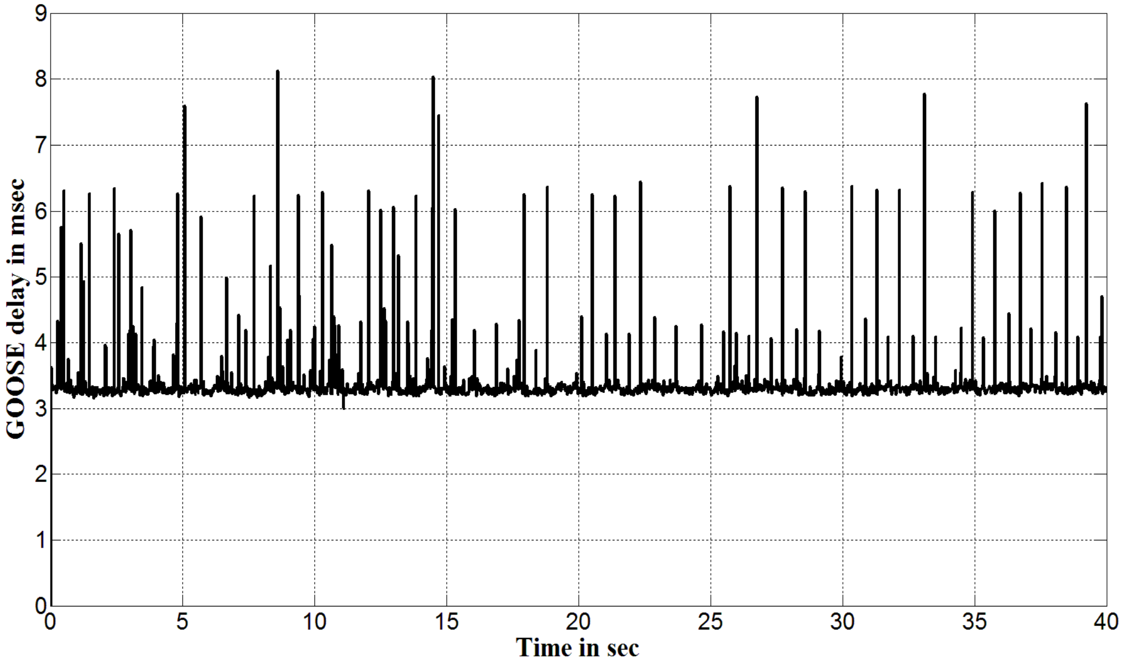


Figure 7-4 GOOSE RTT without CB switching

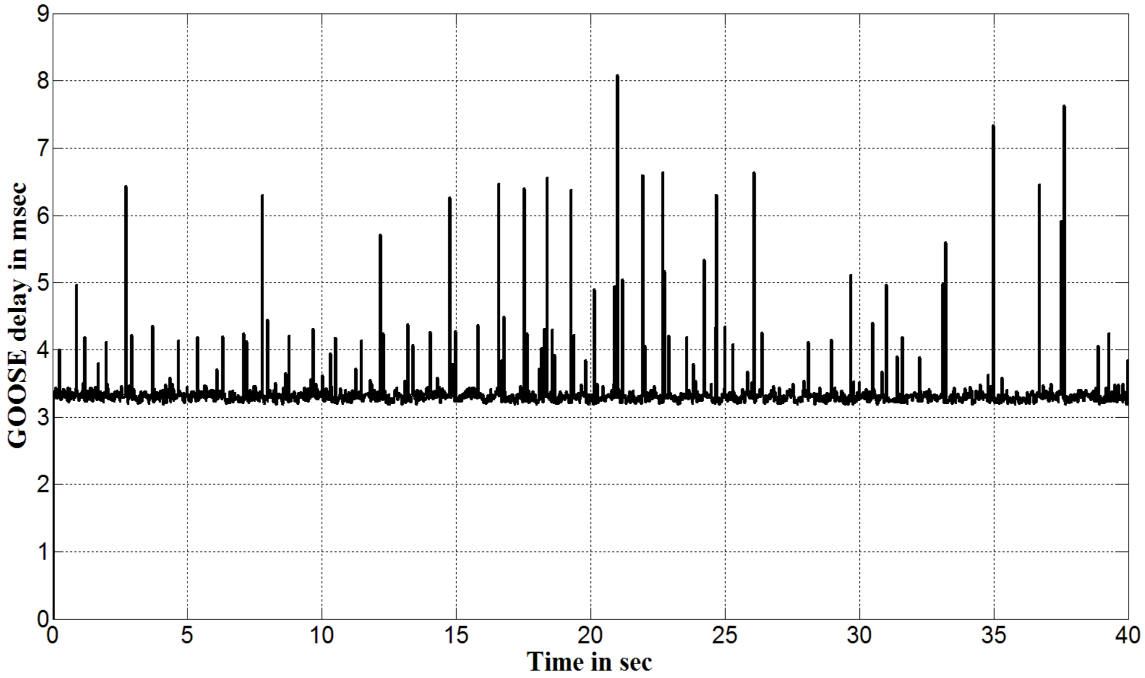


Figure 7-5 GOOSE RTT during CB switching at 13.8 kV distribution substation

7.2.2 **13.8 kV Substation 2**

The RTT communication delay was measured during one-to-one communication between the processing IED and the echo IED. With approximately 12 meters distance, the maximum delay was around 4.97 ms, with average delay of around 3.3 ms, as shown in Figure 7-6 (without CB switching). On the other hand, Figure 7-7 shows GOOSE RTT with CB switching (at full load current), for which the maximum delay was 4.57 ms and the average delay was 3.31 ms. Average delay was almost the same and well within the range allowed for distribution substation control and monitoring applications. It is clear from the figure that there was no impact of EMI from CB switching on the WLAN communication delay. Figure 7-8 shows GOOSE RTT over IEEE 802.11a based WLAN. The maximum and average delays were 4.45 ms and 1.71 ms respectively, which was less than half of the delays registered for the IEEE 802.11g technology.

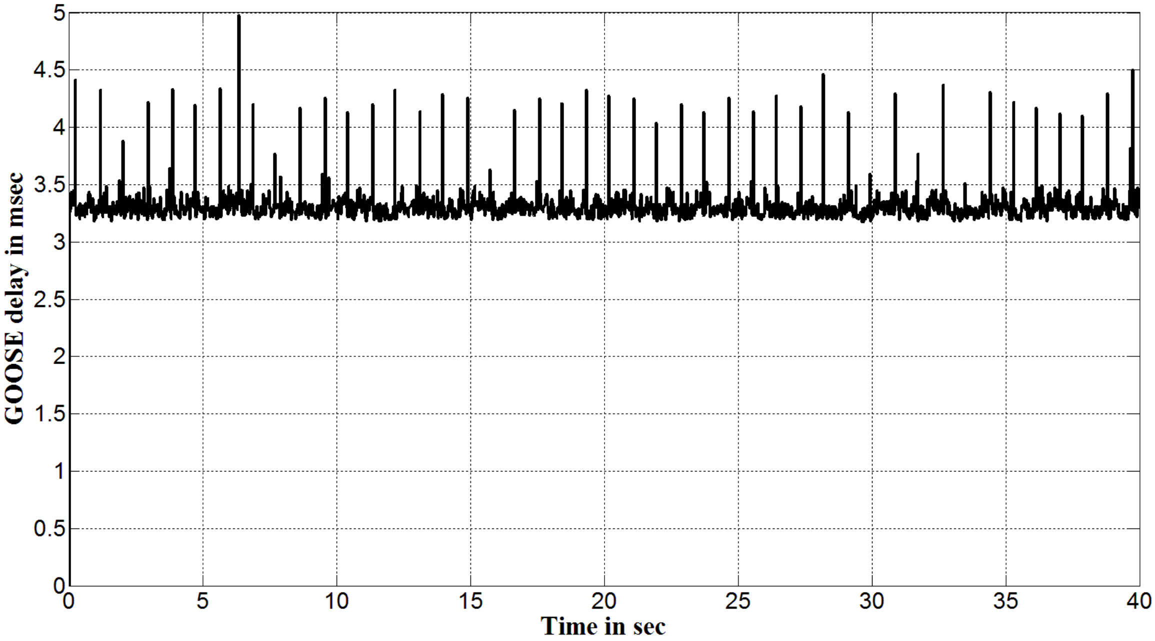


Figure 7-6 RTT of GOOSE without switching

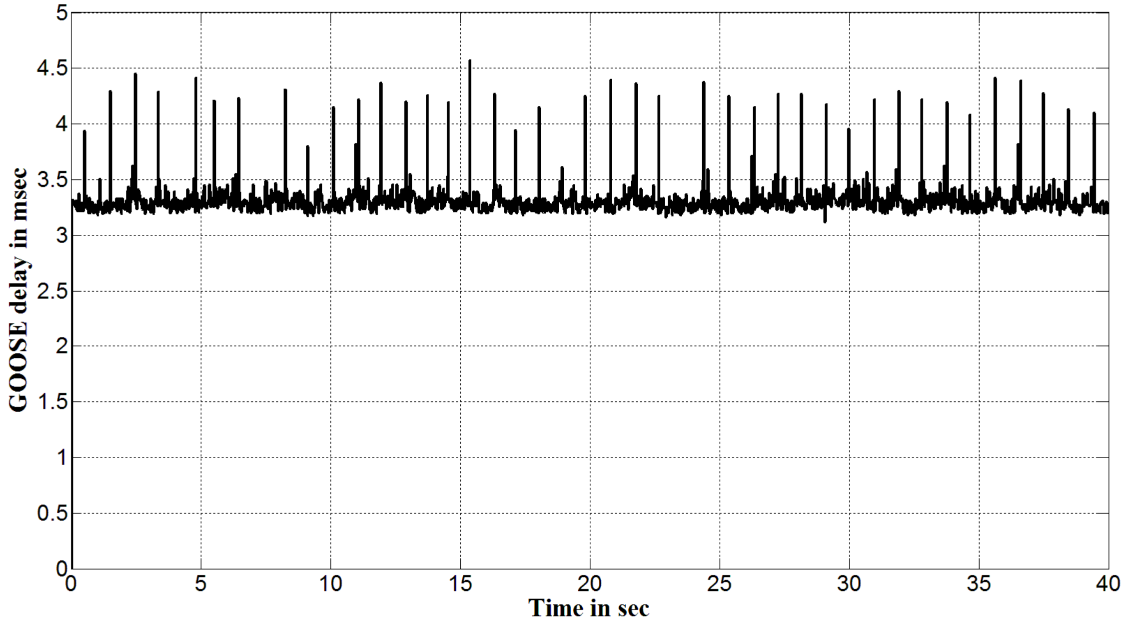


Figure 7-7 RTT of GOOSE with switching

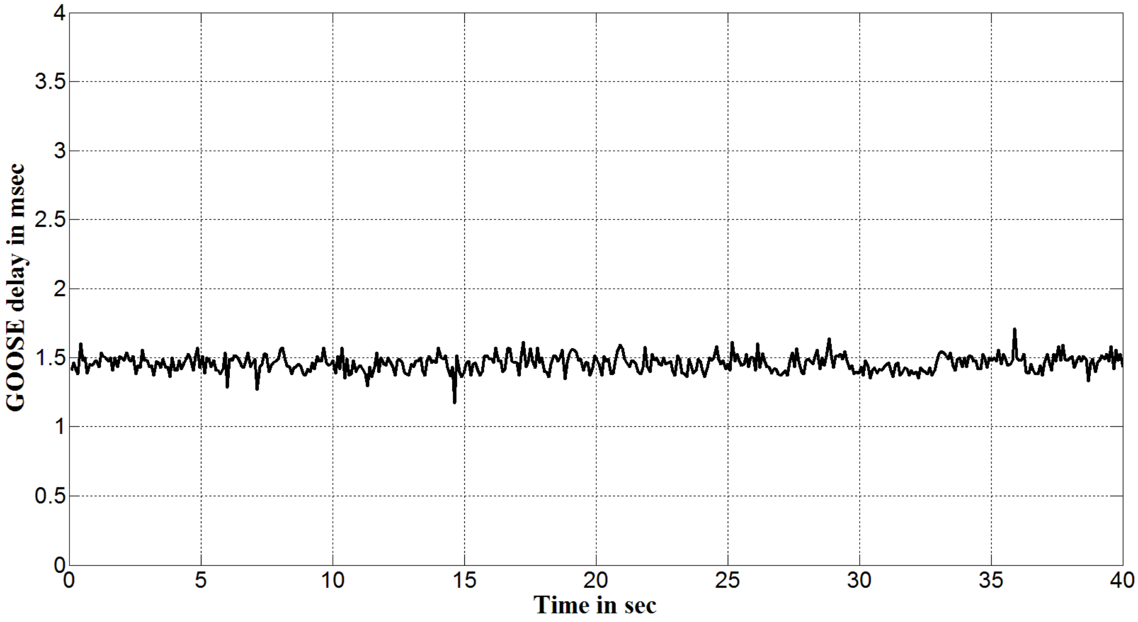


Figure 7-8 RTT of GOOSE with switching over IEEE 802.11a

Table 7-1 summarizes the GOOSE RTT in two 13.8 kV distribution substations of London Hydro. The overall average RTT of GOOSE over IEEE 802.11g WLAN technology at 54 Mbps was between 3.3 and 3.4 ms. The maximum RTT for substation 1 was higher than substation 2 because substation 1 is located in downtown London. The surrounding WLAN networks detected at substation 1 were large in number. It can also be observed from the results that there was no significance difference in delay due to CB switching (which occurred at full load current around 15 to 20 seconds in most of the cases). Using GOOSE over IEEE 802.11a WLAN (at 54 Mbps), the average and maximum RTTs were 1.45 ms and 1.71 ms respectively. This was due to the fact that: 1) there was clear line of sight between the processing IED and the echo IED at the 13.8 kV substation; 2) the distance between these IEDs was only 12 meters; 3) there was no WLAN AP on IEEE 802.11a detected surroundings this substation (since residential WLAN are mainly on IEEE 802.11g AP).

Table 7-1 Summary of GOOSE RTT in 13.8 kV substations

Scenario	**Avg. Delay (ms)**	**Max. Delay (ms)**
13.8 kV substation 1 without any switching operations	3.4	8.13
13.8 kV substation 1 with switching	3.36	8.08
13.8 kV substation 2 without switching	3.31	4.97
13.8 kV substation 2 with switching	3.3	4.57
13.8 kV substation 2 over IEEE 802.11a	1.45	1.71

7.3 Field Testing of Control and Monitoring Applications in 27.6 kV Substations

7.3.1 27.6 kV Substation Site 1

Figure 7-9 shows the on-site measurement setup at one of the 27.6 kV Hydro One distribution substations, close to a 27.6 oil-tank CB (which was subjected to switching).

Figure 7-9 Wireless IED installed at 27.6 kV circuit breaker

Figure 7-10 and Figure 7-11 show the GOOSE RTT without any switching operation and with (SF_6 CB) switching at full load current. In both the cases, average delay was around 3.4 to 3.5 ms. Maximum delay was around 7.5 ms. Moreover, there was no significant impact of switching events on the GOOSE message delay (which occurred approximately 25-30 sec into the result window).

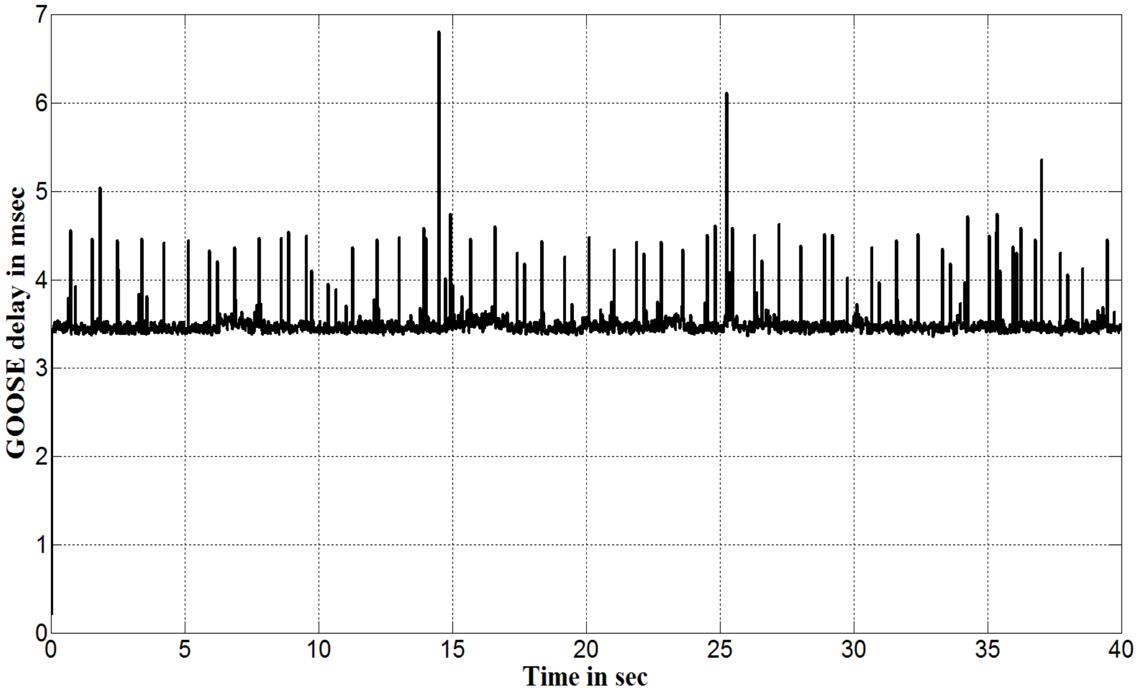


Figure 7-10 RTT GOOOSE delay without switching at 27.6 kV substation

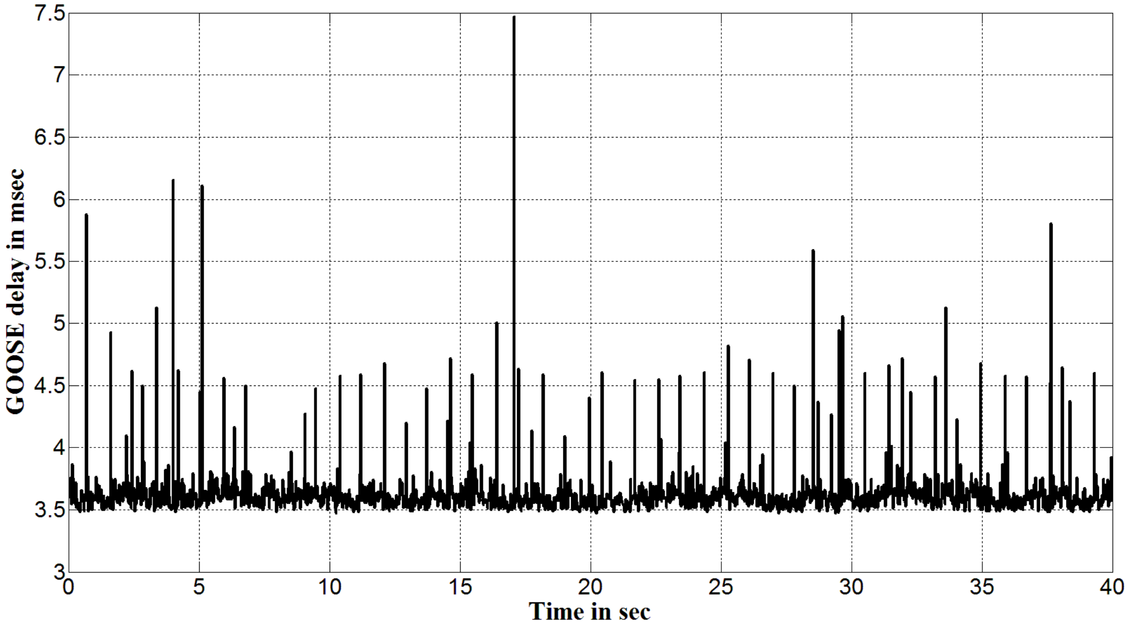


Figure 7-11 RTT GOOSE delay with switching at 27.6 kV substation

7.3.2 **27.6 kV Substation Site 2**

Figure 7-12 and Figure 7-13 show the RTT of the GOOSE message during normal and (oil-tank CB) switching operations respectively. For both cases, average delay was around 3.5 ms, while the maximum delay was around 6.8 ms and 7.47 ms respectively.

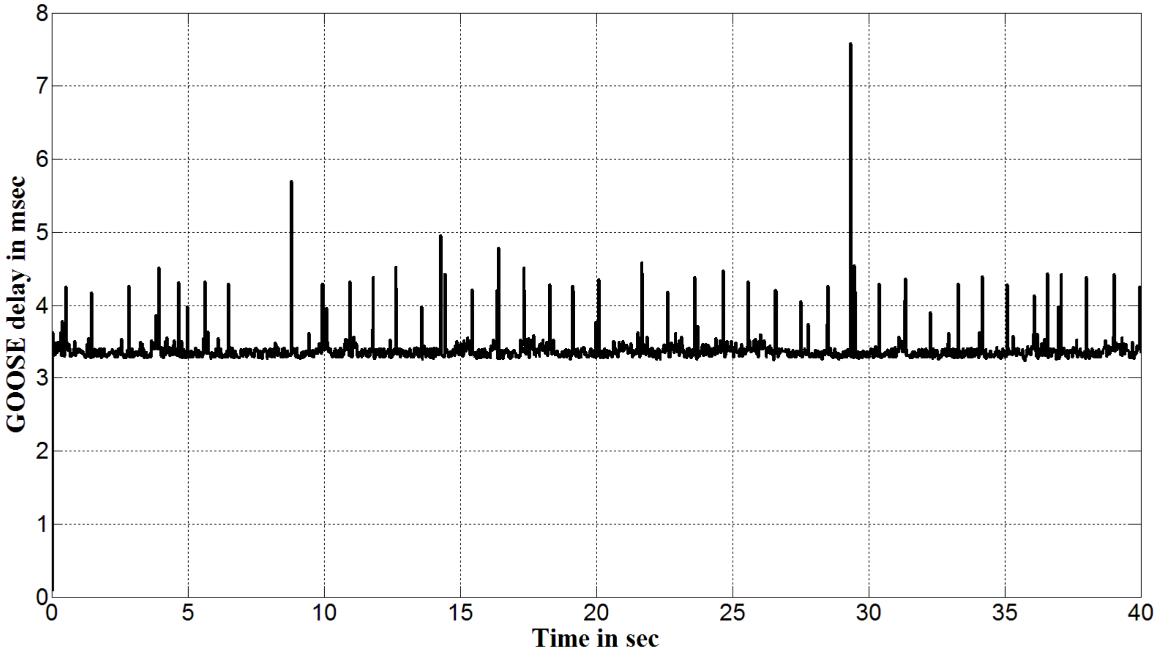


Figure 7-12 RTT GOOSE delay without switching at 27.6 kV substation

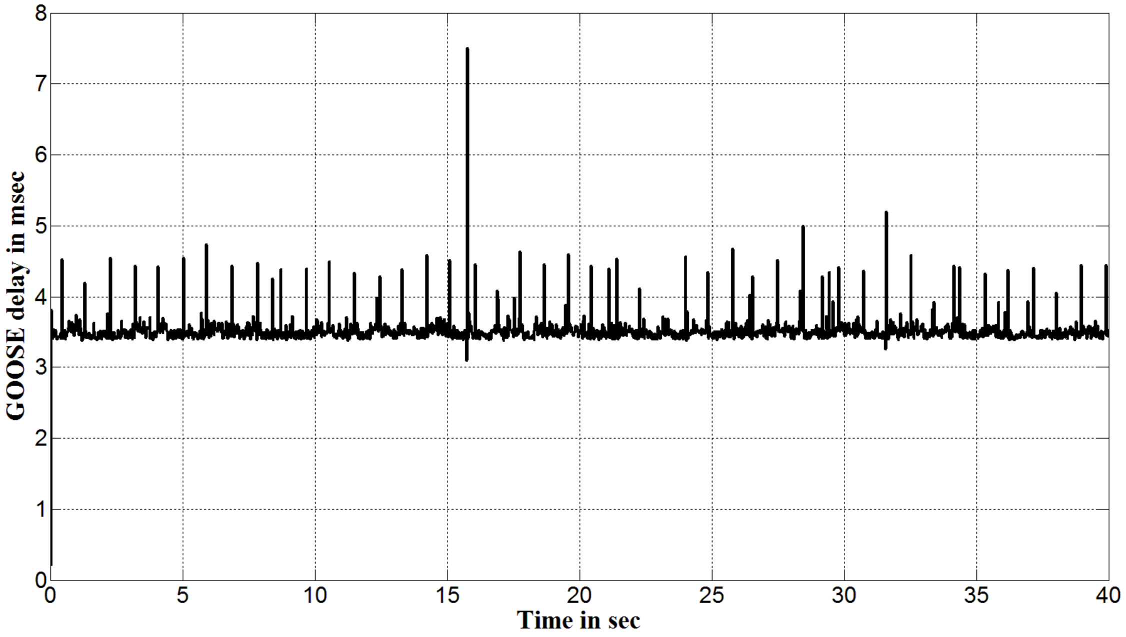


Figure 7-13 RTT GOOSE delay with switching at 27.6 kV substation

7.3.3 27.6 kV Transformer Isolator Switch Operation

Figure 7-14 shows the GOOSE delay observed during isolator switching operation at the 27.6 kV side of a 230/27.6 kV transformer. The average RTT of GOOSE was around 3.7 ms, while maximum RTT delay was 6.91 ms. In addition, GOOSE RTT was also measured over IEEE 802.11a WLAN technology without any switching operation, as illustrated in Figure 7-15. There was less difference in average delay between IEEE 802.11g and IEEE 802.11a, however, there was a difference in maximum delay. The average delay of IEEE 802.11a was not significantly less due to the higher distance between the IEDs (75 meters), and at the same time, the maximum delay was lower because there was no radio interference from surrounding WLAN devices (no IEEE 802.11a based AP detected at the 27.6 kV substation).

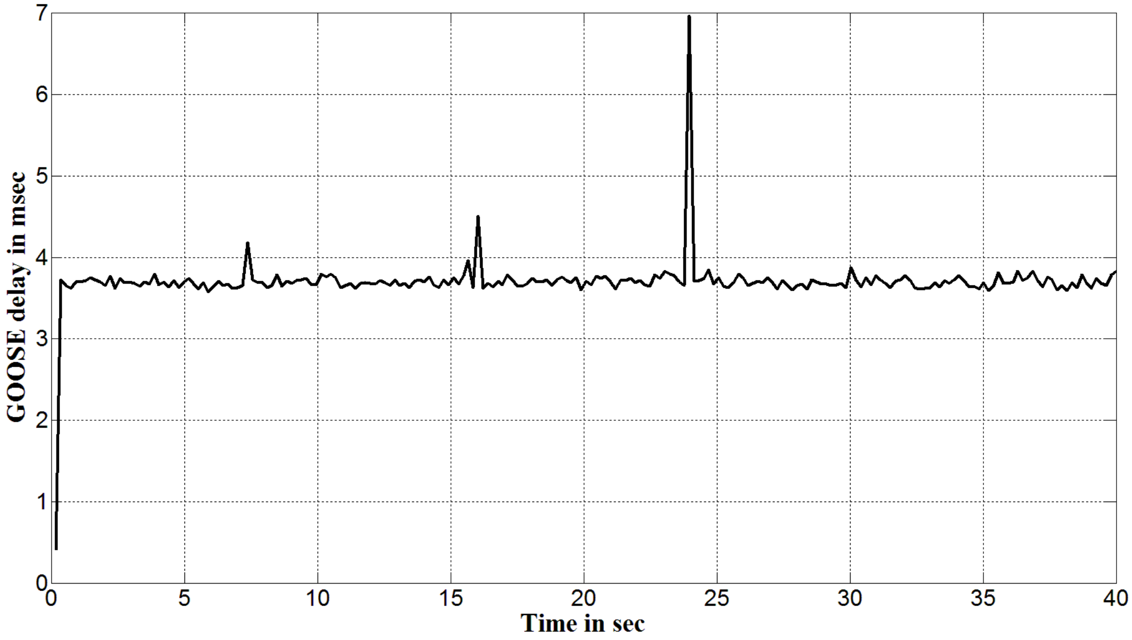


Figure 7-14 RTT GOOSE delay during switching

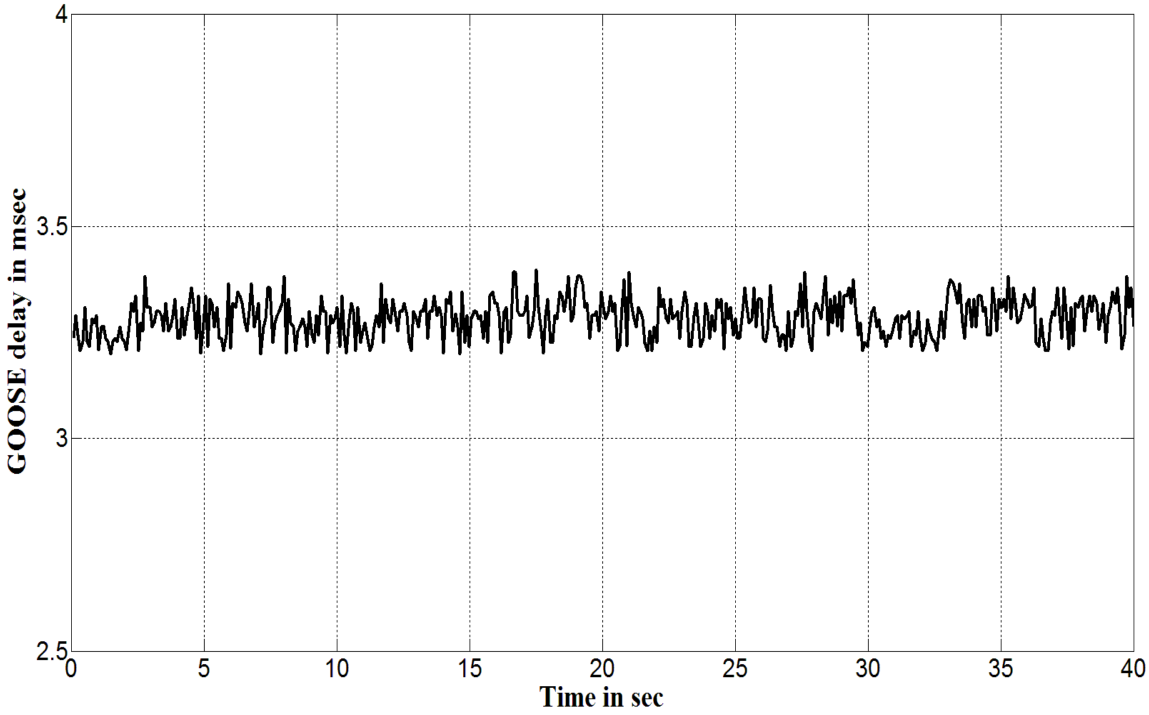


Figure 7-15 RTT GOOSE delay over IEEE 802.11a

Table 7-2 shows the average and maximum RTT for GOOSE messages used for various applications in the 27.6 kV distribution substations. It can be observed that switching of (SF6 and oil tank) circuit breakers did not have significant impact on the average delay of GOOSE message (CB switching at full load current occurred approx. 25-30 seconds while running communication). Moreover, the maximum RTT registered for this substation was around 7.52 ms, which was within allowable range of IEC 61850 standard. Further it can be inferred from the result table that GOOSE RTT over IEEE 802.11a WLAN technology (at 54 Mbps) had almost same average delay 3.2 ms (and less maximum delay 3.39 ms) with respect to other IEEE 802.11g results. Unlike, 13.8 kV substation, the average GOOSE RTT in 27.6 kV substation was not significantly less since the distance in 27.6 kV was higher (75 meter) compared to 13.8 kV (13 meter).

Table 7-2 Summary of GOOSE RTT in 27.6 kV substations

Scenario	**Avg. Delay (ms)**	**Max. Delay (ms)**
27.6 kV substation 1 without any switching operations	3.5	6.8
27.6 kV substation 1 with SF6 CB switching	3.6	7.47
27.6 kV substation 2 without switching	3.4	7.52
27.6 kV substation 2 with oil-tank CB switching	3.5	7.51
27.6 kV substation 2 with isolator switching	3.7	6.91
27.6 kV substation 2 over IEEE 802.11a	3.2	3.39

7.4 Field Results for Automation and Metering Applications in 27.6 kV Substation

In order to evaluate performance of WLAN for automation and metering applications, the RTT was measured for IP messages between the switchyard and control room at a 27.6 kV substation. The processing IED was set up in the control room, and the echo IED was configured close to a 27.6/13.8 kV transformer (as shown in Figure 7-16). Streaming of IP packets was performed between the substation control room and the switchyard over two different 54 Mbps wireless LAN technologies, that is, IEEE 802.11g and IEEE 802.11a.

Figure 7-16 wireless IED installed close to 27.6/13.8 kV transformer in a substation

Figure 7-17 shows the RTT of IP messages between the control room and switchyard. The IP messages (for client/server applications) had average delay of 24.2 ms, and maximum delay was around 25.24 ms with IEEE 802.11g technology, while over IEEE 802.11a based WLAN technology, the IP message average and maximum delays were 22.18 ms and 22.46 ms, respectively.

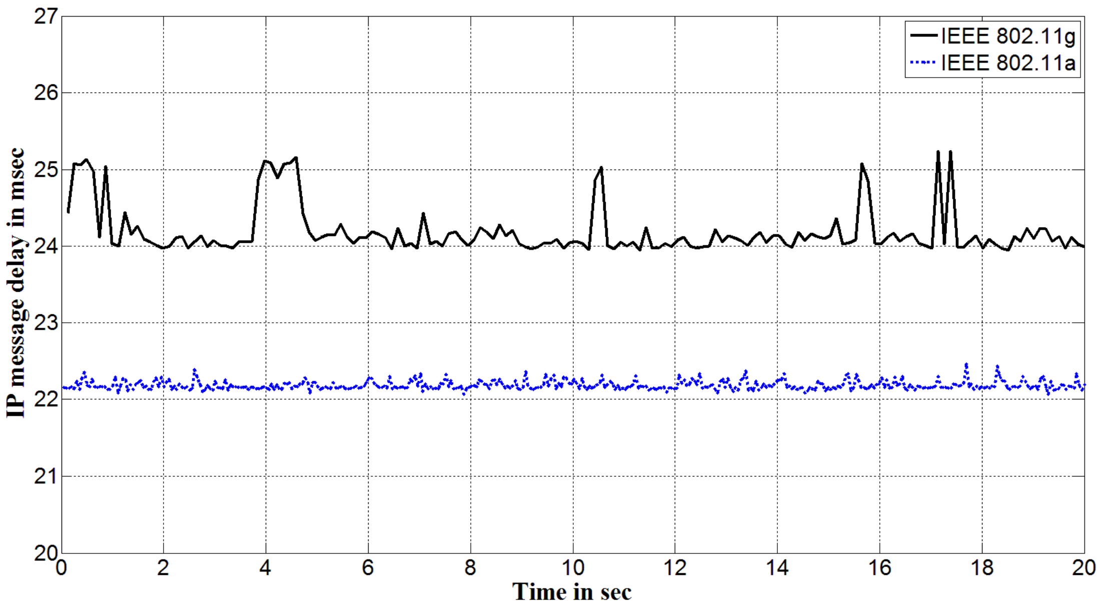


Figure 7-17 RRT IP delay with switching

7.5 Field Results for Over-current Protection Element in 27.6 kV Substation

Figure 7-18 shows the wireless protection IED with over-current element, installed in a control room of a 27.6 kV substation. On the other side, Figure 7-19 shows the installation of the wireless MU that sent sampled-value packets to the protection IED. The distance between these two WLAN devices was approximately 75 meters. The MU streamed data packets with digitized voltage and current signals at 480 Hz (8 samples per cycle), which is specified as the preferable sampling rate in distribution substations according to the IEC 61850-5 standard. The over-current protection IED obtained instantaneous values of three-phase current signals and executed the inverse-time over-current protection algorithm specified in the previous chapter. On the event of protection element pick-up, it transmitted GOOSE packets immediately to the wireless MU. Upon receipt of a GOOSE/trip message over wireless LAN, the wireless MU computed the time difference between fault inception and reception of the GOOSE message. The results of this field test are tabulated in Table 7-3.

Figure 7-18 Wireless IED installed close to relay panel in 27.6 kV substation

Figure 7-19 Wireless MU installed in switchyard of 27.6 kV substation

Table 7-3 demonstrates the results of over-current protection element performance over wireless LAN. The difference between the over-current relay operating time, from MATLAB simulation and from WLAN hardware testing in terms of ms, was considerable, because over-current relay operating time is in terms of seconds. And, the maximum percentage difference due to WLAN communication delay was 5.75% (17.73 ms), which should be acceptable at less critical LV distribution level applications.

Table 7-3 Performance of over-current protection element

TDM	**Over-current Relay Operating Time (AG Fault)**			
	From MATLAB simulation (in sec)	**From WLAN hardware testing (in sec)**	**Difference between hardware and simulation (in sec)**	**Difference (%)**
0.05	0.19373	0.194727	0.000997	0.51
0.10	0.30833	0.326058	0.017728	5.75
0.20	0.5375	0.555076	0.017576	3.26
0.40	0.995833	1.01176	0.015927	1.6
0.60	1.452083	1.500	0.047191	3.25
0.80	1.910411	1.9634	0.052987	2.77
1.00	2.513360	2.544776	0.031416	1.25

7.6 Summary

This chapter presented the field testing carried out in 13.8 and 27.6 kV substations owned by London Hydro and Hydro One in London, Ontario, Canada. The round-trip time of smart distribution substation applications, such as control and monitoring, automation and metering, and total operation time of protection applications, were measured between the switchyard and control room during various circuit breaker switching operations at full load current. The small 13.8 kV substation situated downtown had higher radio interferences on IEEE 802.11g WLAN, and hence, more spikes were observed. On the other hand, IEEE 802.11a WLAN had almost 50% RTT compared to IEEE 802.11g with smooth delay since there was no IEEE 802.11a WLAN AP detected at the time of the experiments. With the 27.6 kV substations, the RTTs were measured for two different types of CBs, SF_6 and oil-tanks. Again, there was no significant impact observed on RTT of any applications due to CB switching operation. Compared to laboratory results (in

Chapter 6), the average RTT of smart distribution substation applications (over IEEE 802.11g) was in the same range. On the other hand, the IP message delay of IEEE 802.11a technology rises from 8.3 ms to 22.18 ms due to increased distance as well as lack of line of sight.

Chapter 8

8. Summary and Conclusions

This research work focused on investigating wireless LAN technology for IEC 61850 based smart distribution substation automation applications. The detailed substation noise measurements and performance analysis of various distribution substation automation applications was presented. The major contributions from this work, as well as summary and conclusion of the research work are discussed in this chapter.

8.1 Major Contributions from the Research

Specific contributions of this research to the area of power system protection are as follows:

1. **Noise measurements and models of distribution substation:** Noise measurements from switching operations and other radio devices were made in the range of wireless LAN at several 13.8 kV and 27.6kV distribution substations. Moreover, the measured noise of distribution substations was modeled, and parameters were obtained for further use.
2. **Dynamic models of WLAN enabled IEC 61850 devices:** The proposed dynamic models of IEC 61850 based WLAN devices can facilitate a platform to analyze wireless LAN networks for desired smart grid applications in the IEC 61850 based substation networks during the planning stage itself. WLAN performance analysis was presented using these developed models for a typical smart distribution substation.
3. **Laboratory development of wireless LAN for IEC 61850 application studies:** A laboratory setup was developed at the University of Western Ontario, which

included wireless LAN enabled IEC 61850 devices, such as wireless protection and control IEDs and the wireless merging unit. The lab was also equipped with an industrial WLAN access point, noise sources, spectrum analyzer, and network analyzer for detailed analysis. This developed laboratory setup can be utilized for studying various wireless applications in a smart grid environment.

4. **Field testing of developed devices for distribution substation applications:** The developed prototypes of WLAN enabled IEC 61850 devices were also tested in the harsh environment of distribution substations of London Hydro and Hydro One. The performance of various smart distribution substation applications based on the IEC 61850 standard was carried out, and the field investigation presented considering switching of distribution substation switchgears at full load currents.

8.2 Summary and Conclusions

Development of smart distribution substations based on the IEC 61850 standard is crucial for the future smart grid infrastructure due to the interconnection of distributed energy resources. With recent advancements in industrial-hardened wireless LAN technologies, it is considered one of the technologies for the future smart grid communication infrastructure. Therefore, an extensive literature survey was carried out to explore the applications of WLAN for power substations. From the survey, various applications of WLAN were identified for the smart distribution substation, which can enhance the distribution substation control, monitoring, automation, and protection with comparatively lower expenses. Further investigation of these applications was carried out using simulation packages, laboratory setup, and field testing.

To examine the performance of wireless LAN for various smart distribution substation applications, the work commenced with substation noise measurements in five London Hydro 27.6 and 13.8 kV substations. The measured substation noise profile was mapped with the generalized extreme value distribution model for 2.4 to 2.5 GHz (IEEE 802.11b/g) bands and normal Gaussian model for 5.7 to 5.9 GHz (IEEE 802.11a) bands.

The observed noise in WLAN radio bands due to switching was insignificant. This may have been due to the fact that the switching noise/EMI in distribution switchyard did not have significant value in GHz bands or because the switching operations were only allowed at load currents (200-300 A) through the breaker, not at the fault currents. Moreover, the radio frequency interference from other WLAN devices was considerable in the downtown area, and comparatively less significant for the remote distribution substation. Hence, it was recommended to study the noise profile of a distribution substation in the vicinity of a residential or industrial neighborhood. The measured noise from the spectrum analyzer was modeled using the MATLAB tool.

Thereafter, the performance analysis of WLAN enabled IEC 61850 distribution substations was carried out using the industry-trusted OPNET simulation tool. These developed noise models were incorporated in OPNET to simulate the distribution substation environment. Furthermore, the detailed dynamic models of IEC 61850 based substation automation devices, such as wireless IED and MUs, were developed using Proto-C language of the OPNET tool. In addition, the modeling of IEC 61850 messages, and priority tagging based quality of service was implemented.

Using these models, a detailed performance evaluation was carried out for a typical 27.6/13.8 kV distribution substation in OPNET for various identified smart distribution substation applications. The end-to-end delays of IEC 61850 messages for distribution substation applications were observed within the allowable limits with 54 Mbps WLAN networks. In addition, the effect of various parameters, such as QoS, data rate, sampling frequency, and signal-to-noise ratio on the delays of time critical (GOOSE and SV) and client/server messages, as well as throughput of wireless communication network, was evaluated. While studying the entire distribution substation applications over WLAN, the average delay of SVs at 11 Mbps (IEEE 802.11b) data rate was higher than the allowable 10 ms, as well as throughput reduced to 3600 Kbps. Conversely, with 54 Mbps (IEEE 802.11 g) network, the delays of time-critical messages (SV and GOOSE) were well within the required delays, with the throughput up to 8000 Kbps. The results showed that QoS (priority tagging) has to be implemented in the WLAN for the time-critical messages. The WLAN network based on IEEE 802.11g with 54 Mbps data rate provided delays within the allowable range of 10 ms for 480 Hz and 960 Hz sampling frequency. For this sampled substation automation system, with SNR less than 20 dB, the delay of time critical messages increased significantly. Also, BER (Bit-Error-Rate) of more than $4.5x10^{-3}$ caused time delays of sampled value messages more than the acceptable limit. Similarly, the distance of more than 200 m between protection and control IEDs (control room) and merging unit (switchyard) may have resulted in higher delays of time-critical messages. This analysis showed that with the proposed wireless substation automation device models, it was possible to carry out the dynamic performance assessment of any wireless IEC 61850 based substation automation system by simulating certain conditions in OPNET. This chapter presented the performance evaluation of various communication systems between the IEC 61850 based distribution automation system and DERs.

Further investigation was carried out in a laboratory by developing hardware prototypes of four WLAN enabled IEC 61850 devices (processing IED, echo IED, protection IED, and MU) using an industrial embedded computer with hard real-time operating system. The processing IED and echo IED were developed to analyze RTT of IEC 61850 based communication message/information exchange for control and automation applications, using IEC 61850 messages. Moreover, the protection and control IED and merging unit playback were developed to investigate delay incurred over WLAN for LV feeder over current protection. In order to assess WLAN performance, further laboratory setup included a commercial wireless access point, traffic generator, noise sources, network analyzer, and spectrum analyzer. From a laboratory setup at 45 feet (13 meters) between IEDs, the average RTT of smart distribution substation control applications (GOOSE message) was 3.5 ms, while for automation applications (IP messages), it was 24 ms at a 54 Mbps data rate. The maximum percentage of operating time of over-current protection was 4.71%, and corresponding delay was 14.52 ms. The average radio noise level should be higher than the threshold that can result in low throughput and higher delay, which was identified as 16 dB in this study. From the thorough investigation, wireless LAN with 54 Mbps data speed is suitable for implementing various smart distribution substation applications up to throughput of 8000 Kbps.

Finally, field testing of 54 Mbps WLAN was carried out by installing the developed prototype devices in harsh-environment 13.8 kV and 27.6 kV substations at 12 meters and 75 meters distance respectively. The smart distribution substation applications were tested between switchyard and control room during switching operations of substation switchgears. It was concluded from the field analysis that the 13.8 kV substation situated downtown had higher radio interferences on IEEE 802.11g WLAN, and hence, more peaks were observed in the results. Moreover, the maximum GOOSE message delays were higher for the 13.8 kV substations (with 12 meters distance) than the 27.6 kV substations (with 75 meters distance) due to higher surrounding noise. In addition, for the 13.8 kV substation, IEEE 802.11a WLAN had almost 50% RTT compared to IEEE 802.11g with smooth delay since there was no IEEE 802.11a WLAN AP detected at the time of experiments. However, for 27.6 kV substations, since the distance was greater than 13.8 kV as well as a lack of line-of-sight between the control room IED and switchyard IED, the application delays over IEEE 802.11a were close with IEEE 802.11g. Therefore, IEEE 802.11a is more suitable for short distances and higher surrounding noise applications where cost and complexity of this technology is justified. With 27.6 kV substations, the RTT were measured for two different types of CBs, SF_6 and oil-tank. Again, there was no significant impact observed on RTT of any applications due to substation switchgear switching operations.

Furthermore, the results obtained in this work from various analysis (e.g. i) dynamic IEC 61850 models development and simulation analysis using OPNET; ii) hardware investigation using laboratory setup, and iii) field setup in distribution substation) are comparable qualitatively. The overall throughput of WLAN setup in a typical distribution substation is obtained around 8000 Kbps (at 17 dB SNR) from the simulation as well as hardware laboratory setup. The OPNET simulation tool allows application performance results in terms of End-To-End delays, whereas, these results using hardware setup (laboratory and field) has to be obtained using Round-Trip-Time (during network stable operation, average ETE ≈ (average RTT)/2). For IEEE 802.11g network setup, the average GOOSE delay (control & monitoring application) obtained from OPNET in terms of ETE is 1.73 ms (at 15 meter distance); and observed RTT from hardware laboratory setup is 3.5 ms (≈ 1.75 ms ETE) at 13 meter distance; whereas, RTT from field installation at 13.8 kV substation is 3.3 ms (≈ 1.65 ms ETE) at 12 meters. Similar qualitative result mapping is observed for other applications with minor differences. The possible reasons behind this differences (between hardware setup and OPNET simulations) could be one or more these parameters: QNX processing time for delay measurements; throughput processing delay of the network analyzer; QNX task priority; kernel procedures differences between hardware and simulation platform, etc. which are difficult to account into the results.

8.3 Future Work Recommendations

Some potential topics for further research are as follows:

- Investigation of other wireless technologies, such as WiMAX and ZigBee, in a smart grid environment.
- Study the wireless LAN against the upcoming IEEE 802.11n protocol that has even higher data rates, once it is made available in OPNET and industrial WLAN APs in the future.

References

[1]. V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, “Smart Grid Technologies: Communication Technologies and standards,” IEEE Transaction on Industrial Informatics, vol. 7, no. 4, pp. 529-539, 2011.

[2]. S. S. Venkata, and H. Rudnick, “Distribution system-past, future and present,” IEEE Power and Energy Magazine, vol. 5, No. 4, pp. 16-22, July/August 2007.

[3]. S. S. Venkata, “Smart Distribution Grid”, Tutorial at NPSC 2008, Mumbai, India. [Online]. Available: http://www.ee.iitb.ac.in/~npsc2008/NPSC_CD/Data/Tutorial%201/SmartDistributionGrid.pdf.

[4]. S. S. Venkata, A. Pahwa, R. E. Brown and R. D. Christie, “What future distribution engineers need to learn,” IEEE Trans. On Power Systems, vol. 19, no. 1, pp. 17-23, Feb. 2004.

[5]. D.E Nordell, "Communication systems for distribution automation,” in Proc. 2008 IEEE T&D Conf. and Expo., pp. 1-14.

[6]. T. S. Sidhu, and P. K. Gangadharan, “Control and Automation of Power System Substation using IEC 61850 Communication,” in Proc. IEEE Control and Applications, pp.1331-1336, Aug. 2005.

[7]. IEC Standard for Communication Network and Systems in Substations, IEC 61850, 1st ed., 2003-04.

[8]. K. P. Brand, V. Lohmann, and W. Wimmer, Substation Automation Handbook, 1st ed., Utility Automation Consulting Lohmann, pp. 301-312, 2003.

[9]. National Institute of Standards and Technology, Standards Identified for Inclusion in the Smart Grid Interoperability Standards Framework, Release 1.0, Sept. 2009, [Online]. Available: http://www.nist.gov/smartgrid/standards.html.

[10]. Electric Power Research Institute Tech. Rep., “The Smart Grid Interoperability Standards Roadmap,” Aug. 2009, [Online]. Available:http://collaborate.nist.gov/twikisggrid/pub/SmartGridInterimRoadmap/InterimRoadmapFinal/Report_to_NISTl August10.pdf

[11]. B. Buchholz, and Z.Styczynski, "New tasks create new solutions for communication in distribution systems,” in Proc. IEEE Power and Energy General Meeting, June 2006.

[12]. B. Hadzi- Kostova, Z. Styczynski, and R. Krebs, "New protection concepts for distribution systems with dispersed generation,” in Proc. IEEE Power Tech. Conf., pp. 1-6, June 2005.

[13]. IEEE P1777 Tech. Rep., "Recommended Practice for Using Wireless Data Communications in Power System Operations,” July 2001.

[14]. F. Cleveland, "Use of wireless data communications in power system operations," in Proc. IEEE Power System Conf. and Expo., pp. 631-640, 2006.

[15]. M. Gast, “802.11 wireless networks: the definitive guide”, Sebastopol, CA: O’Reilly, 2002.

[16]. W. Stallings, “Local and metropolitan area networks”, Upper Saddle River, N.J., Prentice Hall, 5th ed.1997.

[17]. IEEE Standard for Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE Std. 802.11, 2007.

[18]. C. Cena, A. Valenzano, and S. Vitturi, “Hybrid Wired/Wireless Networks for Real-Time Communications,” IEEE Industrial Electronics Mag., vol. 2, no. 1, pp. 8–20, March. 2008.

[19]. P. Kaveh, “Principles of wireless network: a unified approach”, Upper Saddle River, N.J.,Prentice Hall, 2000.

[20]. Stallings William, “Wireless communication and networks”, Upper Saddle River, N.J.,Prentice Hall, 2nd ed.2005.

[21]. Cooklev Todor, “Wireless communication standards: a study of IEEE 802.11, 802.15 and 802.16”, Standards information network, New York, IEEE Press, 2004.

[22]. Ruggedcom, Rugged Wireless Applications, [Online]. Available: http://www.ruggedcom.com/applications/wireless/index.php

[23]. EPRI Tech. Rep., "Wireless Connectivity for Electric Substations," Feb. 2008.

[24]. EPRI Tech. Rep., "Assessment of Wireless Technologies in Substation Functions Part-II: Substation Monitoring and Management Technologies," Mar. 2006.

[25]. IEEE PSRC Tech. Rep., "Using Spread Spectrum Radio Communication for Power System Protection Relaying Applications," july 2005.

[26]. D. K. Holstein, “Wi-Fi Protected Access for Protection and Automation a work in progress by CIGRE Working Group B5.22,” in Proc. 2006 IEEE Power System Conf. and Expo., pp. 2004-2011.

[27]. K.M. Abdel-Latif, M.M. Eissa, A.S. Ali, O.P. Malik, and M.E. Masod, “Laboratory investigation of using Wi-Fi protocol for transmission line differential protection,” IEEE Trans. Power Delivery, vol. 24, no. 3, pp. 1087-1094, July. 2009.

[28]. D.R. Brown, J.A. Slater, and A.E. Emanuel, “A wireless differential protection system for air-core inductors,” IEEE Trans. Power Delivery, vol. 20, no. 2, pp. 579-586, April. 2005.

[29]. M. Adamiak, R. Hunt, A. King, and S. McCreery," Application of digital radio for distribution pilot protection and other applications,” in Proc. IEEE Protective Relay Conf., pp. 310-333, 2008.

[30]. G. Thonet, and B.Deck, “A new wireless communication platform for medium-voltage protection and control,” in IEEE workshop on factory communication system, pp. 335-338, Sept. 2004.

[31]. A. Timbus, M. Larsson and C. Yuen, “Integration of wind energy resources in the utility control and information technology infrastructures,” in Proc. IEEE International Symposium on Industrial Electronics, pp. 2371-2376, Jul. 2008.

[32]. P. Palensky, and D. Dietrich, "Demand Side Management: Demand Response Intelligent Energy Systems, and Smart Loads,” IEEE Transaction on Industrial Informatics, vol. 7, no. 3, pp. 381-388, 2011.

[33]. L.K. Siow, P.L. So, H.B. Gooi, F.L. Luo, C.J. Gajanayake, and Q.N. Vo, “ Wi-Fi based server in microgrid energy management system,” in Proc. IEEE TENCON Conf. 2009,pp. 1-5, Jan. 2009.

[34]. GE Digital Energy, [Online]. Available: http://www.gedigitalenergy.com/Communications/catalog/dgt.htm, Aug. 2011.

[35]. T. Smith, J. Vico, and C. Wester, “Advanced Distribution Reclosing using Wireless Communications,” in proc. Georgia Tech Protective Relaying Conference, Apr. 2012.

[36]. SEL Inc. [Online]. Available: http://www.seling.com/sel-3022.htm, Aug. 2011.

[37]. Beckwith, [Online]. Available: http://www.beckwithelectric.com/powerlines/powerlines-38.html, Aug. 2011.

[38]. RUGGEDCOM – Industrial Strength Network [Online]. Available: http://www.ruggedcom.com/applications/smart-grid/, Aug. 2011.

[39]. Tropos GridCom™, "A Wireless Distribution Area Network for Smart Grids," Whitepaper [Online]. Available: www.tropos.com/pdf/whitepapers/GridComWP_052709.pdf

[40]. Carlson wireless, SwiftGrid products, [Online]. Available: http://www.carlsonwireless.com/products/SwiftGrid.php, Aug. 2011.

[41]. MOXA, [Online]. Available: http://www.moxa.com, Aug. 2011.

[42]. CIGRE WG 36, IEEE Radio Noise Subcommittee Working Group No. 1, "CIGRE/IEEE Survey On Extra High Voltage Transmission Line Radio Noise," CIGRE/IEEE Report, Nov. 1971.

[43]. C. M. Wiggins, D. E. Thomas, F. S. Nickel, and S. E. Wright, "Transient electromagnetic interference in substations," IEEE Trans. On Power Delivery, vol. 9, no. 4, pp. 1869-1884, Oct. 1994.

[44]. W.H Siew, Y.C. Liu, B. Musa, F. Mir and Y. Wang, "Basis for a Wireless Network for EMC Measurements in Electric Substations," in IEEE international symp. on electromagnetic compatibility,pp.1-5, July 2007.

[45]. W.H Siew, Y. Wang, and M. Faheem, "Wireless digital data acquisition system for EMI measurement in power substations," 17th International Zurich symposium on electromagnetic compatibility, 2006.

[46]. PSERC (Power System Engineering Research Center) Tech. Rep., "Wireless Communications in Substations", Nov. 2002.

[47]. A. Shapoury, and M. Kezunovic, "Noise profile of wireless channels in high voltage substations," in proc. IEEE Power Engineering Society General Meeting, pp: 1- 8, June 2007.

[48]. Q. Shan , I.A. Glover, R. Rutherford, S. Bhatti, R. Atkinson, I.E. Portugues, and P.J. Moore, "Detection of ultra-wide-band impulsive noise in a 400 kV air insulated electricity substation," in proc. 20th international conference on electricity distribution, Jun. 2009.

[49]. Q. Shan, S. Bhatti, I.A. Glover, R. Atkinson, I.E. Portugues, P.J. Moore, and R. Rutherford, "Characteristics of impulsive noise in electricity substations," EUSIPCO 2009.

[50]. Q. Shan , I.A. Glover, P.J. Moore, I.E. Portugues, R.J. Watson, R. Rutherford, R. Atkinson, and S. Bhatti, "Laboratory Assessment of WLAN Performance Degradation in the Presence of Impulsive Noise," Wireless Communications and Mobile Computing Conference, pp. 859 –863, Aug. 2008.

[51]. H. Jashnani, and T. S. Sidhu, "Study of Radio Noise in Electrical Substation in IEEE 802.11 wireless bands," M.Engg. Project Report, Dec. 2008.

[52]. V. C. Gungur, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid – a case study of link quality assessments in power distribution systems," IEEE Transactions on Industrial Electronics, Vol. 57, No. 10, October 2010, pp. 3557-3564.

[53]. IEC 61850-5, "Communication Networks and Systems in Substations, Part 5: Communication Requirements for Functions and Device Models", First Edition, 2003.

[54]. B. Dimitri and R. Gallager, "Data networks", Englewood Cliffs, N.J.,Prentice Hall, 2nd ed.1992.

[55]. OPNET Modeler - OPNET Technologies Inc. [Online]. Available: http://www.OPNET.com 2011.

[56]. NS-2 - The Network Simulator [Online]. Available : isi.edu/nsnam/ns.

[57]. R. O. Baldwin, N. J. Davis, and S. F. Midkiff, “Implementation of an IEEE 802.11 Wireless LAN model using OPNET,” in Proc. OPNETWORK 2002, Washington D.C., USA, Aug. 2002.

[58]. B. Van den Broeck, P. Leys, J. Potemans, J. Theunis, E. Van Lil, and A. Van de Capelle, "Validation of Router Models in OPNET," in Proc. OPNETWORK 2002, Washington D.C., USA, Aug. 2002.

[59]. P. Rathod, S. Perur, and R. Rangarajan, "Bridging the Gap between Reality and Simulations: An Ethernet Case Study," in Proc. International Conf. on Information Technology (ICIT'06), Bhubaneswar, Orissa, India, pp.52-55, Dec.18-21, 2006.

[60]. Zaki Maged, “IEEE 802.11 wireless LANs carrying integrated traffic, quality of service policies and performance analysis,” Master’s Thesis, University of western ontario, 2000.

[61]. G. Cena, I. C. Bertolotti, A. Valenzano, and C. Zunino,“Evaluation of Response Times in Industrial WLANs,” IEEE Transaction on Industrial Informatics, vol. 3, no. 3, pp. 191-201, 2007.

[62]. T. S. Sidhu and Y. Yin, “Modelling and simulation for performance evaluation of IEC 61850 based substation communication systems,” IEEE Trans. Power Delivery, vol. 22, no. 3, pp. 1482-1489, Jul. 2007.

[63]. C. Wang, and Y. J. Fang, “Channel model simulation for underwater acoustic sensor networks using OPNET,” in Proc. Of IEEE Communication Technology conference, China, pp. 141-144, Nov. 11-14, 2010.

[64]. M. Kanabar, and T. S. Sidhu, “Performance of IEC 61850-9-2 Process Bus and Corrective Measure for Digital Relaying,” IEEE Transaction on Power Delivery, vol. 26, no. 2, pp. 725-735, Apr. 2011.

[65]. T. Skeie, Svein Johanessen and Christoph Brunner, “ETHERNET in Substation Automation,” IEEE Control Systems Magazine, vol. 22, no. 3, Page(s): 43 – 51, June 2002.

[66]. M. S. Thomas, and I. Ali, “Reliable, Fast, and Deterministic Substation communication network architecture and its performance simulation,” IEEE Transactions on Power Delivery, vol. 25, No. 4, Oct. 2010.

[67]. Yujie Yin, M.E.Sc. Thesis, “Performance Evaluation of IEC 61850 based substation automation communication networks,” 2006.

[68]. IEEE Std. 802.11b, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-speed Physical Layer Extension in the 2.4 GHz Band,” 2001.

[69]. IEEE Std. 802.11g, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band,” 2003.

[70]. IEEE Std. P802.11i, “Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: medium access control (MAC) Security Enhancements, April, 2004.

[71]. Siemens White Paper, “WLAN Security Today: more secure than wired,” July 2008.

[72]. IEEE PSRC WG H5 Report on “Application of peer-to-peer communications for protective relaying,” Mar. 2001.

[73]. G. Brunello, and B. Kasztenny, “An application of a protective relaying scheme using ICA/MMS standard,” in Proc. IEEE PES T&D Latin America conference, Brazil, Mar. 2002.

[74]. N. Hatziargyriou, H. Asano, R. Iravani, and C. Marnay, “Microgrids,” IEEE power & energy magazine, vol. 5, no. 4, 2007.

[75]. Communication networks and systems for power utility automation - Part 7-420: Basic communication structure - Distributed energy resources logical nodes, International Standard IEC 61850-4-720, Feb. 2003.

[76]. P. Parikh, M. G. Kanabar, W. El-Khattam, T.S. Sidhu, and A. Shami, “Evaluation of Communication Technologies for IEC 61850 Based Distribution Automation System with Distributed Energy Resources,” Proc. of the IEEE PES General Meeting, Calgary, July 26-30, 2009.

[77]. IEEE Std. 802.11e, “Wireless LAN medium access control (MAC) and Physical Layer (PHY) Specifications: medium access control (MAC) enhancement for quality of service (QoS),” 2002.

[78]. G. Cena, L. Seno, A. Valenzano, and C. Zunino, “On the Performance of IEEE 802.11e Wireless Infrastructure for Soft- Real –Time Industrial Applications,” IEEE Transaction on Industrial Informatics, vol. 6, no. 3, pp. 425-437, 2010.

[79]. ANTEC Inc, [Online]. Available: http://www.antec.com/Believe_it/

[80]. CISCO Inc. Linksys WMP600N, wireless LAN transceiver PCI network adapter, [Online]. Available: http://www.linksysbycisco.com/UK/en/products/WMP600N, 2011.

[81]. QNX Real Time Operating System (RTOS), [Online]. Available: http://www.qnx.com/products/neutrino-rtos/neutrino-rtos.html, 2011.

[82]. M. R. Dadash Zadeh, T.S. Sidhu and A. Klimek, “Suitability analysis of Practical Directional Algorithms for Use in Directional Comparison Bus Protection based on IEC61850 Process Bus,” in IET Generation, Transmission & Distribution, vol. 5, Issue. 2, pp. 199-208, 2011.

[83]. M. R. Dadash Zadeh, T.S. Sidhu and A. Klimek, “Implementation and Testing of Directional Comparison Bus Protection Based on IEC61850 Process Bus,” IEEE Transaction on Power Delivery, vol. 26, Issue. 3, pp. 1530-1537, 2011.

[84]. T. S. Sidhu, M. S. Sachdev, and H. C. Wood, “Design of a microprocessor based overcurrent relay,” IEEE Western Canada Conference on Computer, Power and Communications Systems in a Rural Environment, pp. 41-46.29-30 May 1991.

[85]. T. S. Sidhu, M.Sc. thesis, “Computer aided design and performance evaluation of digital relays,” University of Saskatchewan, Saskatoon, Canada, 1985.

[86]. J. Singh, M. S. Sachdev, R. J. Fleming, and A. Krause, “Digital IDMT directional overcurrent relays,” in proc. IEE conf. on developments in power system protection, no. 185, pp. 152-157, Apr. 1980.

[87]. Ruggedcom Inc, RS900W, industrial strength RuggedWireless, [Online]. Available: http://www.ruggedcom.com/products/ruggedwireless/rs900w/

[88]. IEEE Std.802.16, “IEEE Standard for Local and metropolitan area networks,” 2009.

[89]. EPRI Tech. Rep., "Wireless Connectivity for Electric Substations," Feb. 2008.

[90]. V. C. Gungor, F. C. Lambert, “A survey on communication networks for electric system automation,” [Online]. Available: http://www.sciencedirect.com/science.

[91]. International Telecommunication Union. [Online] Available: http://www.itu.int/home/imt.html

[92]. P. K. Lee, and L. L. Lai, “A Practical Approach to Wireless GPRS On-Line Power Quality Monitoring System,” Proc. of the IEEE PES General Meeting, June 2007.

[93]. T. Choi, K. Y. Lee, D. R. Lee, and J. K. Ahn, “Communication system for distribution automation using CDMA,” IEEE Trans. On Power Delivery, vol. 23, no. 2, pp. 650-656, Apr. 2008.

[94]. X. Zhang, Y. Gao, G. Zhang, and G. Bi, “CDMA2000 cellular network based SCADA system,” in an international conf. on Power system technology, pp. 1301-1306,Vol. 2, 2002.

[95]. L.Kong, J. Jin, and J. Cheng, “Introducing GPRS technology into remote monitoring system for prefabricated substations in China,” in an international conf. of mobile tech., application and systems, Nov. 2005.

[96]. IEEE Std. 802.15, “Standard for Information Technology - telecommunications and information exchange Systems between systems - Local and metropolitan area networks,”2006.

[97]. J. Cheng, M. Hung, and J. Cheng, “A ZigBee-Based Power Monitoring System with Direct Load Control Capabilities,” in an international conf. of networking, sensing and control, pp. 895-900, April 2007.

[98]. P. Kadar, “ZigBee Controls the Household Appliances,” Proc. of the IEEE PES General Meeting, Calgary, July 26-30, 2009.

[99]. IEEE Std.802.20, “IEEE Standard for Local and Metropolitan Area Networks,” 2008.

[100]. H. Zhang, G. Guan, and X. Zang, “The design of insulation online monitoring system based on Bluetooth technology and IEEE1451.5,” in an international conf. on Power Engineering, pp.1287-1291, Dec. 2007.

[101]. Agilent Spectrum Analyzer, [Online]. Available: http://www.home.agilent.com/agilent/

[102]. AirPcap & CACE pilot Network Analyzer, [Online]. Available: http://www.cacetech.com/

Appendix A Wireless Applications

A.1 WiMAX

Worldwide inter-operability for Microwave Access (WiMAX) technology is a part of 802.16 series standards for Wireless Metropolitan Area Network (WMAN) [88]. Main objective of WiMAX is to achieve worldwide interoperability for microwave access. In 2001, when the first draft of IEEE 802.16 standard was released, it defined the wide operating range of 10-66GHz for communication infrastructure. WiMAX forum has published a subset of the range for interoperability. For fixed communication 3.5 and 5.8 GHz bands have been dedicated, while for mobile communication frequency bands 2.3, 2.5 and 3.5 GHz have been assigned. The spectrums 2.3, 2.5, 3.5 GHz are licensed; whereas 5.8GHz is unlicensed spectrum. It provides data rate up to 70Mbps and distance up to 48km [89]. However, distance and network speed are inversely proportional to each other. Licensed spectrums allow higher power and longer distance transmission, which is more suitable for long distance communication. The bandwidth and the range of WiMAX provide the alternative of cable, DSL and T1 communication channel for last-mile access. WiMAX for smart grid applications are discussed below:

A.1.1 Wireless Automatic Meter Reading (WMAR)

Large distance coverage and sufficiently high data rates make WiMAX technology more suitable for Wireless Automatic Meter Reading (WMAR) as a part of utility Automatic Metering Infrastructure (AMI). Fig. A-1 shows the WAMR system based on WiMAX. Implementation of WAMR for revenue metering offers several advantages to electric utilities and/or service provider in the smart grid environment by reducing the need for human meter readers.

A.1.2 Real-time pricing

WiMAX network for AMI can be used to provide real-time pricing models based on real-time energy consumption of the customers. Real-time pricing capability of WAMR systems can also be beneficial to the customers by shifting their loads during off-peak times [90].

A.1.3 Outage Detection and Restoration:

Currently, distribution network has almost negligible outage detection mechanism especially for residential customers, which result into low reliability of power supply. With the help of two-way communication using WiMAX, fast outage detection and restoration can be implemented. Challenges and solutions of WiMAX technology are discussed below:

Radio frequency hardware for WiMAX tower is comparatively expensive, and therefore, the placement of WiMAX tower should be done optimally to reduce infrastructure costs and meet Quality of Service (QoS) requirements.

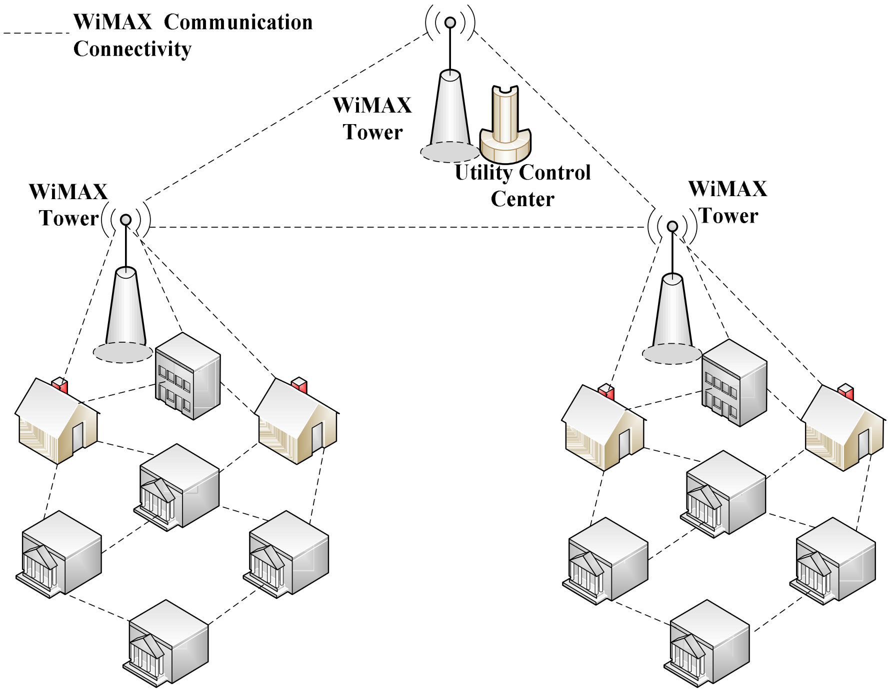


Fig. A-1 WiMAX communication for WAMR

Moreover, WiMAX frequency above 10 GHz cannot penetrate through obstacles; therefore, lower frequencies are the most practical for AMI applications especially in urban area. However, the lower frequency bands are already licensed, and hence, the most likely way of utilizing WiMAX is by leasing it from the third party.

A.2 Cellular

The 3G (3rd Generation) / 4G (4th Generation) cellular technology operates on the spectrum range of 824-894MHz/1900MHz [91]. These are the licensed frequency bands. Data transmission rate of this technology is 60-240Kbps, and distance converge is depend upon the availability of cellular service [89]. This cellular network topology consists of cells, which are formed by many low power wireless transmitters. With the moment of mobile devices having cellular modem, transmission of data is also exchanged between cell to cell, which facilitates non interrupted data flow. This way it forms a point to point architecture. It can also receive data from serial or Ethernet interface and transmit data on a second interface over cellular network, to enable normally wired components to become wireless. This technology offers extensive data coverage, no maintains costs and network fully maintained by carrier [92], [93].

Cellular technology for smart grid applications:

The advantage with cellular technology is that the existing infrastructure can be used at some extent. Also, with the recent growth in 3G / 4G cellular technology, the data rate and Quality of Service (QoS) are improving very fast.

A.2.1 SCADA interface for remote distribution substation

Due to mobile phone users, cellular coverage is available even in very remote locations. Reference [94] has demonstrated use of Code Division Multiple Access (CDMA) technology for power system Supervisory Control And Data Acquisition (SCADA), by providing cellular communication between substation Remote Terminal Unit (RTU) and

SCADA server. Fig. A-2 shows the application of cellular technology for SCADA interface of remote distribution substation site.

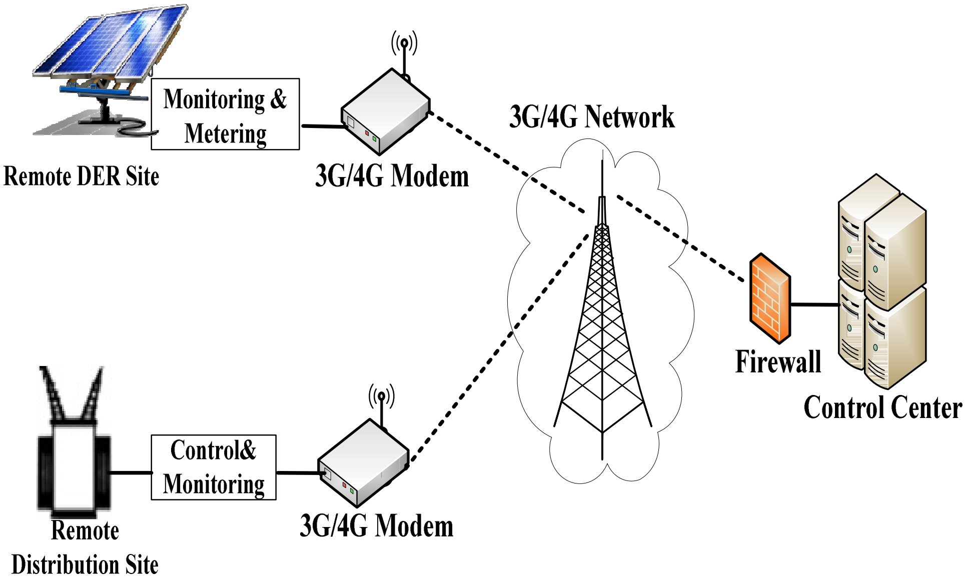


Fig. A-2 Cellular technology for SCADA and power grid monitoring

A.2.2 Monitoring and metering of remote DERs

As shown in Fig.5, the cellular technology can be used for monitoring and metering of remotely installed DERs. Non-critical information exchange can be carried out in the form of SMS, which is cheap solution comparatively. The monitoring application of remote substation using General Packet Radio Service (GPRS) technology is explained in [92], [95].

Challenges and solutions of cellular technology:

Call establishment takes indefinite time delay, and moreover, call dropout can affect the large data exchange. Due to high monthly fees for individual connection and expensive call costs, cellular technology may not be economical for larger group of remote sites or regular data transfer [89].

A.3 ZigBee

ZigBee is reliable, cost effective, and low power home area wireless network developed by ZigBee Alliance based on an open global standard. It provides compatibilities with IEEE 802.15.4 standard. ZigBee operates on the unlicensed frequency range of 868MHz, 915MHz and 2.4GHz with DSSS modulation technique. It offers a data rate of 20-250 Kbps. It provides coverage of 10-100m. ZigBee supports the star, tree and Mesh topologies. Transmission reach and battery life of the ZigBee devices vary depending upon the topology adopted. ZigBee employs 128-bit AES encryption for security [96].

ZigBee is widely used for building automation, security systems, remote control, remote meter reading and computer peripheral applications. ZigBee technology for smart grid applications:

A.3.1 Control of home appliances

ZigBee is very suitable for Wireless Sensor Networks (WSN), due to low power consumption, low cost, and low data rate. Smart Home Area Network (HAN) can be formed using advanced ZigBee network consist of Full Function Node (FFN) and Reduced Function Node (RFN). Only the FFN has the full ZigBee functionality and hence, one of the FFN becomes a network coordinator. The RFN has limited resources and does not allow some advanced functions, e.g. routing, as it is a low cost end device solution. Fig. A-3 shows the star configured ZigBee HAN for home appliances control. As illustrated in the figure, ZigBee end devices are connected with relay which can control the power supply switch of home appliances. ZigBee coordinator manages the ZigBee network configuration, as well as, exchanges the information between each home appliances and local HAN control.

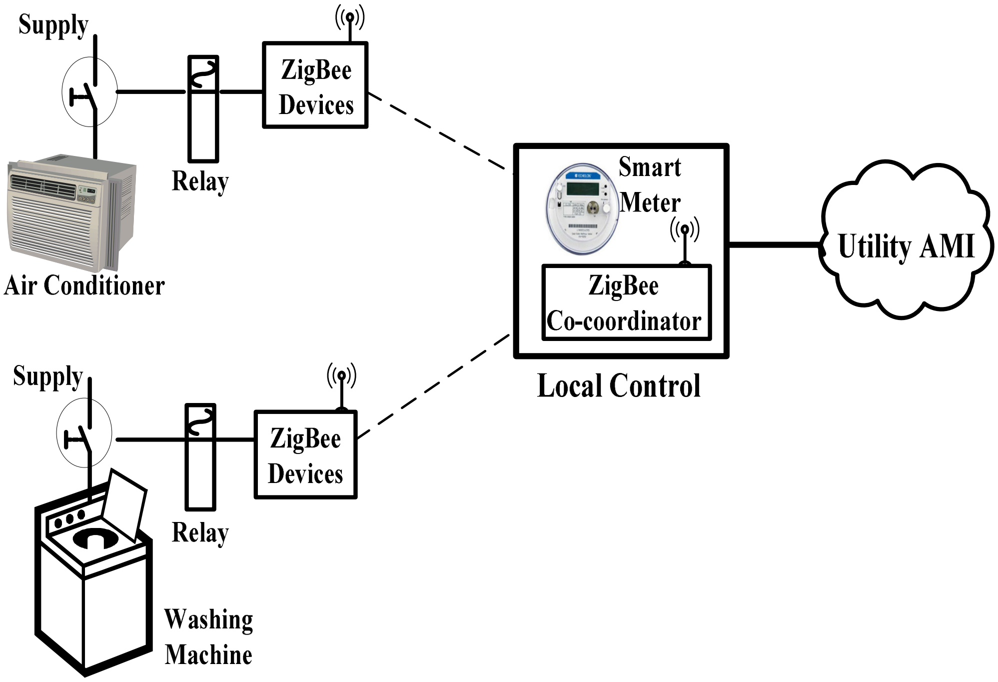


Fig. A-3 ZigBee technology for smart home area network

A.3.2 Direct load control

The local HAN can be automatically controlled locally with the help of controller or remotely using utility AMI infrastructure. References [97], [98] present implementation of direct load control for home appliances. Challenges and solutions of ZigBee technology are discussed below:

Due to limited physical size, ZigBee devices have limited battery energy supply, internal memory and processing capacity. The use of ZigBee in industrial environments is not well document [89], and hence this technology may be limited for residential automation system.

A.4 Other Potential Wireless Technologies

A.4.1 Mobile Broadband Wireless Access (MBWA):

IEEE 802.20 standard for MBWA provides high bandwidth, high mobility and low latency in the licensed frequency bands below 3.5 GHz, by utilizing the positive features of both IEEE 802.11 WLANs and IEEE 802.16 WMANs. It is also known as MobileFi. It offers real time peak data rate of 1Mbps to high speed data rate of 20Mbps. This standard is optimized for full mobility up to vehicular speed of 250km/h [99].

IEEE 802.20 may be used for smart grid applications, such as broadband communication for plug-in electric vehicles, wireless backhaul for electric grid monitoring and SCADA systems. IEEE 802.20 (MBWA) is new emerging technology, and hence, communication infrastructures for this technology are not readily available. Currently, use of this technology may be costly solution compare to cellular technology.

A.4.2 Digital Microwave Technology:

Digital microwave operates on licensed frequency band of 2-40GHz, and provides the data rate up to 155Mbps. Microwave technology provides very long distance coverage up to 60 kilometers. It accepts data from Ethernet or ATM port and transmits it to the other as microwave radio.

Digital microwave can support point to point communication for smart grid applications, e.g. transfer trip between DER and distribution substation feeder protection relay. Microwave radio is susceptible to two types of signal fading, precipitation and multi-path interference. Encryption for security may result in to additional latency as it takes larger message sizes [89].

A.4.3 Bluetooth

Bluetooth is part of wireless personal area network standard, IEEE 802.15.1. It is low power, short range radio frequency communication standard. It operates on 2.4–2.4835GHz unlicensed ISM band. It offers a data rate of 721Kbps [96]. Devices with Bluetooth configuration consist of complete OSI 7 layer communication stack. It can facilitate both point to point, and point to multipoint communication configuration.

Depending upon the communication configuration it offers distance coverage between 1m – 100m.

Bluetooth technology can be used for local online monitoring applications as a part of substation automation systems [100]. These devices are highly influenced by surrounding communication link and may interfere with IEEE 802.11 based wireless LAN network. The Bluetooth offers weak security compare to other standards.

The wireless applications discussed in this section are summarized in Table A-1.

Table A-1 Comparison of wireless technologies used in power industry

Wireless Technologies	Data Rate	Approx. Coverage	Potential Smart Grid Applications
Wireless LAN	1-54 Mbps	100-200 m	distribution automation, monitoring, and protection
WiMAX	70 Mbps	48 km	Wireless Automatic Meter Reading (WMAR)
Cellular (3G/ 4G)	60-240 Kbps	10-50 km	SCADA and monitoring for remote distribution
ZigBee	20-250 Kbps	10-100 m	Direct load control of home appliances
MobileFi	20 Mbps	Vehicular Std.	communication for PEVs and remote monitoring
Digital Microwave	155 Mbps	60 km	transfer trip (point-to-point)
Bluetooth	721 Kbps	100 m	local online monitoring applications

Appendix B EMI Measurement in Substation

B.1 Site plan for BUCHANAN Substation

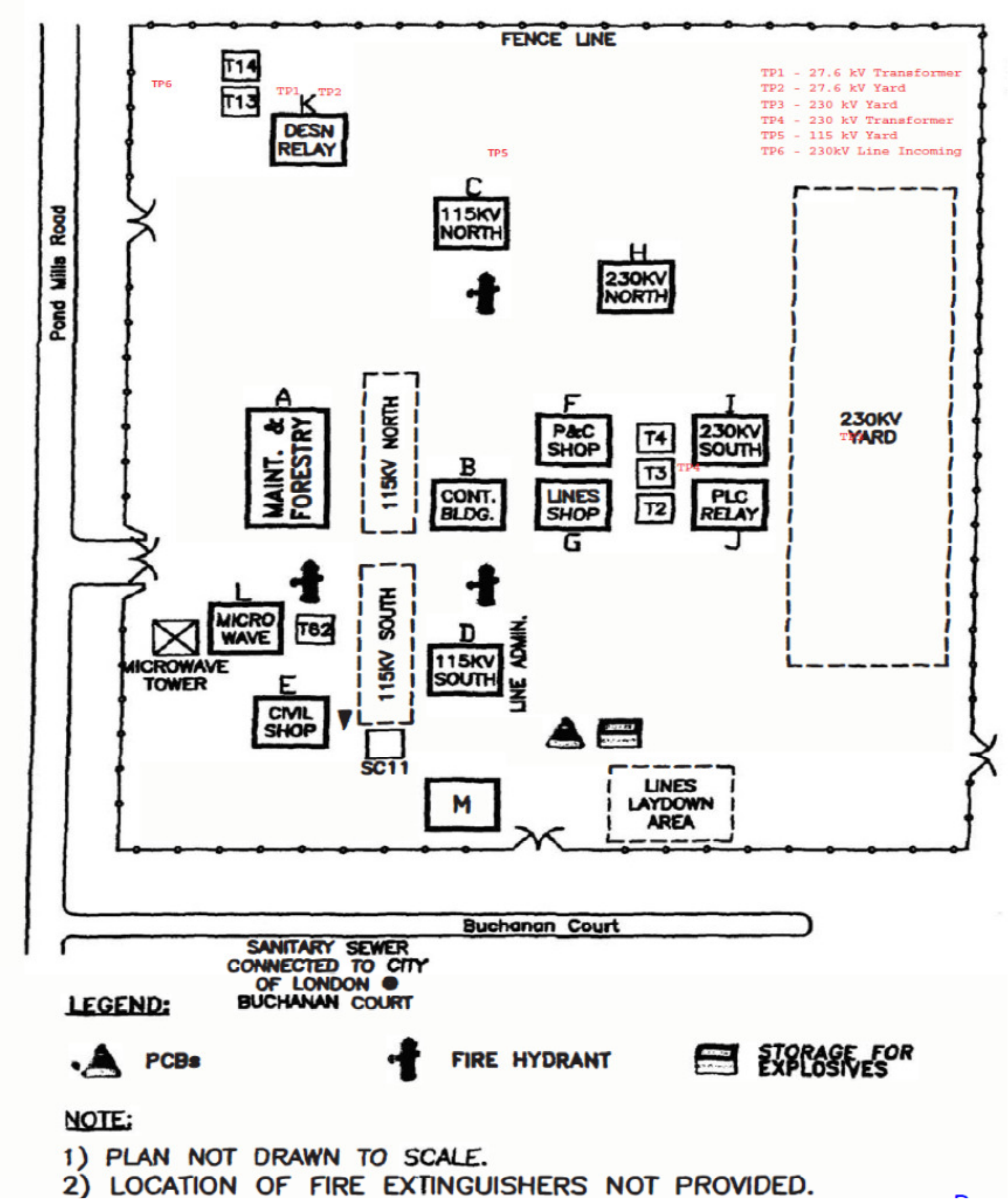


Fig. B-1 Substation layout of Buchanan distribution substation, London, ON

B.2 Instruments of Measurement Set-up

B.2.1 Agilent Spectrum Analyzer

The spectrum analyzer, like an oscilloscope, is a basic tool used for observing signals. Where the oscilloscope provides a window into the time domain, the spectrum analyzer provides a window into the frequency domain. In this work, Agilent made E4404B spectrum analyzer is used for the EMI measurement in distribution substation [101]. E4404B can measure EMI between 9 kHz to 6.7 GHz range. Fig. B-2 shows the ESA-E series Agilent spectrum analyzer with GPIB interface to computer.

Fig. B-2 Agilent Spectrum Analyzer

B.2.2 Critical parameter selection in Agilent Spectrum Analyzer

The critical parameter selection of spectrum analyzer for EMI measurements in distribution substation is discussed as below:

1) Frequency range or span: It is one of the key setting parameters of a spectrum analyzer. It depends upon in which range of the frequency, noise should be measured. In spectrum analyzer, first center frequency is tuned to the signal of interest, and then span or range of frequency is adjusted to zoom in on the signal of interest. There is a trade-off in setting frequency span of the spectrum analyzer,

as higher span will take more time to measure the EMI over the entire range. Table B-1 list-out the frequency ranges used for EMI measurement study.

Table B-2 Frequency range for noise measurement

Experiment Set-up	**Frequency**
Experiment 1	2.4-2.5 GHz band (IEEE 802.11 b, g)
Experiment 2	5.75-5.85 GHz band (IEEE 802.11a)
Experiment 3	0-2.5 GHz band

2) Sweep speed: It indicates how fast the trace (or EMI measurement) can sweep across the entire frequency span of interest. Generally, it is given in msec. Since, the EMI measurement should be done during switching operation of circuit breaker; the sweep speed of 16 msec (every power cycle of 60Hz) is selected for this set-up.
3) Resolution Bandwidth (RBW): The resolution bandwidth (RBW) setting must be considered when concerned with separating spectral components, setting an appropriate noise floor and demodulating a signal. Advantages of using a narrow RBW are: improves sensitivity, reduces Display Average Noise Level (DANL), and increases dynamic measurement range. DANL is the internal noise floor level of the instrument, and it should be lower than expected noise level amplitude. Lower DANL can be achieved by narrowing RBW. However, the narrowest RBW setting is not always ideal, as it increases the sweet time. Moreover, it is important to set the RBW wide enough to include the sidebands of the signal. The narrow RBW selected for the distribution substation EMI measurement is between 1 kHz to 10 kHz, in order to achieve sweep speed of 16 msec.
4) Display detection mode: The spectrum analyzer digitizes the signal, and the choice of which digitized data to display depends on the display detector following ADC. It is as if the data is separated into buckets, and the choice of which data to display in each bucket becomes affected by the display detection mode. The display detection modes available in Agilent spectrum analyzer are

positive peak, negative peak, and sample detectors. Peak detection mode detect the highest level in each bucket, and is good choice for analyzing sinusoids, but tend to over-respond to noise measurements. Whereas, sample detection mode displays the center point in the each bucket. Sample detection is good for noise measurements, and accurately indicates the true randomness of noise. Therefore, it is recommended by Agilent technical support team to use sample detection mode for EMI measurements in distribution substation.

The spectrum analyzer provides ways to soften the tradeoffs to achieve accuracy, fast and high dynamic range of measurements. By utilizing digital signal processing, the spectrum analyzer provides for a more accurate measurement, while at the same time allowing faster measurements even when using narrow RBW.

B.3 GPIB interface with computer

As shown in Fig. B-3, the Agilent 82357B USB/GPIB interface provides a direct connection from the USB port on your desktop and laptop computers to GPIB instruments. Once the software is loaded, your computer automatically detects the 82357B when it is connected to the USB port of the computer. With this GPIB port, computer directly connects spectrum analyzer to Microsoft Excel software. This way, the data capturing can be done automatic during substation switching events. GPIB supports more than 1.15 Mbps data transfer rate.

Fig. B-3 GPIB interface with computer

B.3.1 AirPcap adapter with Wireless LAN analyzer (CACE Pilot)

Multi-channel AirPcap Nx adapters are used with wireless LAN analyzer (CACE Pilot) is used to measure radio frequency interferences from other WLAN devices in the vicinity of the distribution substation [102]. Fig. B-4 shows the AirPcap adapter connected to computer with CACE Pilot analysis tool. Multiple AirPcap adapters can be plugged into a laptop or a USB hub and provide industry-leading capability for simultaneous multi-channel capture and traffic aggregation. The AirPcap driver provides support for this operation through CACE Multi-channel Aggregator technology that exports capture streams from multiple AirPcap adapters as a single capture stream. Even when more than one BSS shares the same channel, the AirPcap adapter will capture the data, control, and management frames from all of the BSSs that are sharing the channel within range of the AirPcap adapter. CACE Pilot tool connected with multiple AirPcap adapters, provides a seamless distributed network analysis, recording, visualization, monitoring, and reporting system. Three multi-channel adapters hop to various IEEE 802.11 defined channels and obtains data from all WLAN channels.

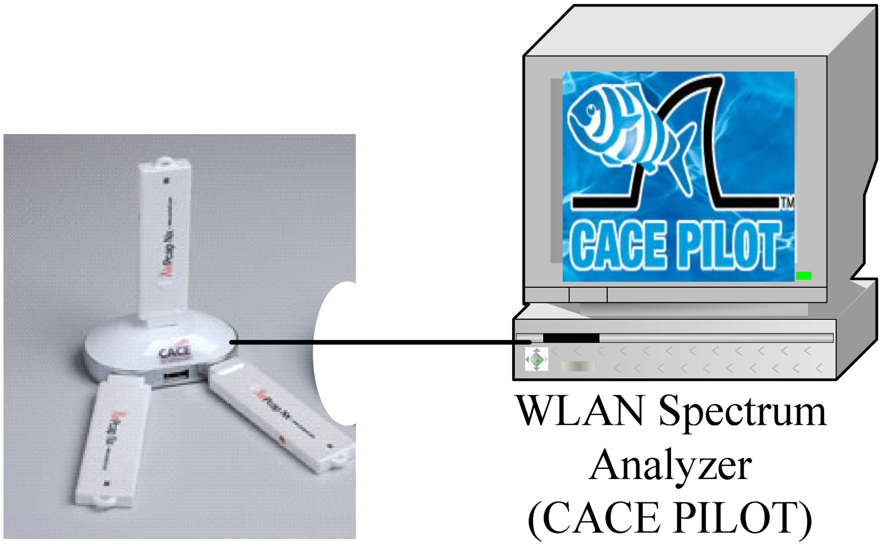


Fig. B-4 AirPcap setup to measure RFI

Appendix C Used Probability Distribution Functions

C.1 Gaussian Normal Distribution

The normal distribution curve is based on two-parameter. The first parameter, μ, is the mean. The second, σ, is the standard deviation. The standard normal distribution sets μ to 0 and σ to 1. Mean and Standard deviation can be calculated using the maximum likelihood estimates (MLEs) estimator or minimum variance unbiased estimator (MVUE) technique. However, an MLE might be biased, which means that its expected value of the parameter might not equal the parameter being estimated. While, the MVUE has the minimum variance of all unbiased estimators of a parameter.

The MVUEs of parameters μ and σ for the normal distribution are the sample mean and variance. The sample mean is also the MLE for μ.

C.2 Generalized Extreme Value Distribution

The probability density function for the generalized extreme value distribution with location parameter μ, scale parameter σ, and shape parameter $k \neq 0$ is for

$$f(x|k,\mu,\sigma) = \left(\frac{1}{\sigma}\right) exp\left(-\left(1 + k\,\frac{(x-\mu)}{\sigma}\right)^{\frac{-1}{k}}\right)\left(\left(1 + k\,\frac{(x-\mu)}{\sigma}\right)^{-1-\frac{1}{k}}\right)$$

where,

μ = Location Parameter

σ = Scale Parameter

k = Shape parameter

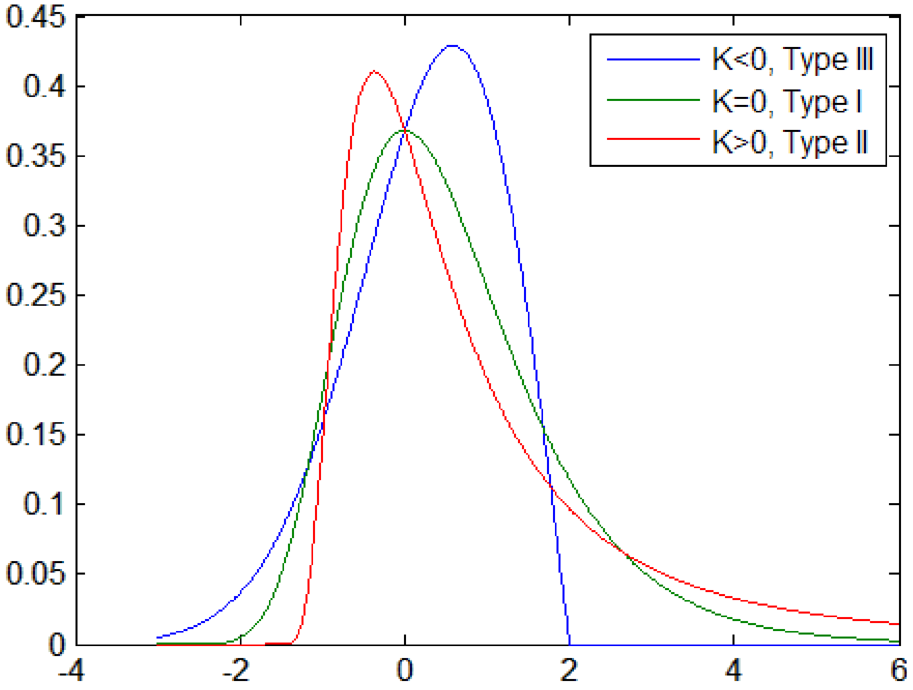


Fig. C-1 Generalized Extreme Value Distribution

Based on this description and formulas, most suitable distribution for the measured noise data at different substation level and location is decided. Also, standard deviation error is also calculated based on the estimated parameter.

Appendix D Development of IEC 61850 Enabled Devices Using OPNET Tool

In this appendix, some of the major C/C++ codes for the development of IEC 61580 based wireless devices using OPNET, are presented.

D.1 wlan_mac_hcf_Function Block_GOOSE_Final

```
static WlanT_HCF_Access_Category
wlan_hcf_higher_layer_data_arrival (void)
	{
	Packet*						hld_pkptr;
	OpT_Packet_Size					data_size, frag_size;
	OpT_Int64					dest_addr;
	int							protocol_type;
	int							up;
	WlanT_HCF_Access_Category	ac;
	Ici*						ici_ptr;
	WlanT_HCF_Peer_Info*		dest_info_ptr = PRGC_NIL;
	const IpT_Dgram_Fields*		ip_header_fields_ptr;
	int							in_strm;  /*defined by Palak*/

	/** Queue the packet as it arrives from higher layer. Also, store		**/
	/** the destination address of the packet in the queue and the		**/
	/** arrival time. Return the access category of the higher layer **/
	/** packet if it is successfully queued, otherwise return				**/
	/** WlanC_AC_None.
								**/
	FIN (wlan_hcf_higher_layer_data_arrival (void));
	/*************Modified by Palak on 12th march 2009**************/
	/* Determine the interrupt type and the stream index in the case of	*/
/* stream interrupt, since this information will be	in the next if	*/
/* statement condition.							*/
intrpt_type = op_intrpt_type ();
if (intrpt_type == OPC_INTRPT_STRM)
	{
	in_strm = op_intrpt_strm ();
	if(in_strm == instrm_from_source)
	{
	/* Get packet from the incoming stream from higher layer and obtain	*/
	hld_pkptr = op_pk_get (instrm_from_source);
	}
	else
	{
```

```
		/* Get packet from the incoming stream from higher layer and obtain	*/
		hld_pkptr = op_pk_get (instrm_from_mac_if);
		}
		}
		/*cnt=cnt+1;
		op_stat_write (counter, cnt);		*/

		/* If we are in a bridge/switch node, then we don't accept any		*/
		/* higher layer packet unless we are AP enabled.				*/
		if ((wlan_flags->bridge_flag == OPC_TRUE) && (ap_flag == OPC_BOOLINT_DISABLED))
			{
			op_pk_destroy (hld_pkptr);
			FRET (WlanC_AC_None);
			}
		/* Read ICI parameters at the stream interrupt.				*/
		ici_ptr = op_intrpt_ici ();
		/* Get the destination address from the ICI.				*/
		op_ici_attr_get_int64 (ici_ptr, "dest_addr", &dest_addr);
		/* Get the protocol information of the higher layer data from ICI.	*/
		op_ici_attr_get_int32 (ici_ptr, "protocol_type", &protocol_type);
		/* Check for an AP bridge whether the destined station exists in	*/
		/* the BSS or not. If not then no need to broadcast the packet.	*/
		if (wlan_flags->bridge_flag == OPC_TRUE && ap_flag == OPC_BOOLINT_ENABLED)
			{
			/* If the destination station doesn't exist in the BSS then no	*/
			/* need to broadcast the packet.				*/
			if (dest_addr >= 0)
				{
				dest_info_ptr = (WlanT_HCF_Peer_Info *) prg_bin_hash_table_item_get
(peer_info_hash_tbl, (void *) &(dest_addr));
				if (dest_info_ptr == PRGC_NIL)
					{
					op_pk_destroy (hld_pkptr);
					FRET (WlanC_AC_None);
					}
				}
			}
		/* Get the size of the packet arrived from higher layer.			*/
		data_size = op_pk_total_size_get (hld_pkptr);
		/* Find out the UP information. If the higher layer packet is an */
		/* IP packet, then retrieve the information from the IP header,  */
		/* otherwise obtain it from the ICI.					*/
		if (wlan_flags->nqsta_operation == OPC_FALSE)
			{
			if (protocol_type == OMSC_PROTOCOL_TYPE_IP)
				{
				/* Obtain the UP information from the ToS field of the IP	*/
				/* header. Shift the number to right by 5 bits to skip the	*/
				/* DSCPbits.						*/
				op_pk_nfd_access_read_only_ptr (hld_pkptr, "fields", (const void **)
&ip_header_fields_ptr);
				up = (ip_header_fields_ptr->tos >> 5);
				}
			else if (op_ici_attr_exists (ici_ptr, "type_of_service"))
```

```
            op_ici_attr_get_int32 (ici_ptr, "type_of_service", &up);
        else
            /* For higher layer packets that don't carry any ToS          */
            /* information, assume their UP 0 (best effort).              */
            up = 0;
        /* Make sure we have a valid user priority value.                 */
        if (up < MIN_UP_VALUE || up > MAX_UP_VALUE)
            wlan_error_print ("Incorrect UP (user priority) value associated with the higher
layer packet.", "", "");
        /* Determine the AC corresponding to the packet's UP.             */
        ac = WLANC_UP_TO_AC_MAPPING_ARRAY [up];
        }
    else
        {
        /* Since we belong to an nQBSS, we will use the DCF access  */
        /* methods. Use the "best effort" AC to buffer the higher layer */
        /* packet.                                                          */
        ac = WlanC_AC_BE;
        /* If there is a UP information within the ICI of the event,     */
        /* then obtain that information. Although we belong to an nQBSS      */
        /* currently, at the time when we transmit this higher layer     */
        /* packet, we may be in a QBSS and need that information.            */
        if (op_ici_attr_exists (ici_ptr, "type_of_service"))
            op_ici_attr_get_int32 (ici_ptr, "type_of_service", &up);
        else
            up = WLANC_nQSTA_DATA_UP;
        }
    /* If this is the very first higher layer packet of this AC, then   */
    /* register the outgoing traffic related statistics of this AC.       */
    if (!(wlan_ac_flags->stats_registered & WLANC_AC_BITMAP_ARRAY [ac]))
    wlan_hcf_ac_statistics_register (ac, OPC_TRUE);

    /* Update all the load statistics, local and global, general and   */
    /* AC specific.                                                        */
    op_stat_write (packet_load_handle, 1.0);
    op_stat_write (packet_load_handle, 0.0);
    op_stat_write (bits_load_handle,   (double) data_size);
    op_stat_write (bits_load_handle,   0.0);
    op_stat_write (global_load_handle, (double) data_size);
     op_stat_write (global_load_handle, 0.0);
    op_stat_write (ac_load_pkts_shndl_arr [ac], 1.0);
    op_stat_write (ac_load_pkts_shndl_arr [ac], 0.0);
    op_stat_write (ac_load_bits_shndl_arr [ac], (double) data_size);
      op_stat_write (ac_load_bits_shndl_arr [ac], 0.0);
    op_stat_write (ac_gb_load_shndl_arr [ac],   (double) data_size);
     op_stat_write (ac_gb_load_shndl_arr [ac],   0.0);
    /* Determine the size of the MPDUs of the MSDU.                        */
    if ((data_size > frag_threshold) && (frag_threshold != -1))
        frag_size = frag_threshold;
    else
        frag_size = data_size;
    /* Destroy packet if it is more than max msdu length or its size*/
    /* zero. Also, if the size of the higher layer queue will exceed  */
    /* its maximum after the insertion of this packet, then discard the      */
```

```
        /* arrived packet. The higher layer is responsible for the                    */
        /* retransmission of this packet.                                                     */
        if    ((data_size    >    WLANC_MAXMSDU_LENGTH    &&    accept_large_packets    ==
OPC_BOOLINT_DISABLED) ||
                frag_size > WLANC_MAXMSDU_LENGTH || data_size == 0 || total_hlpk_size +
data_size > hld_max_size)
                {
                /* Drop the higher layer packet.                                    */
                wlan_hcf_hl_packet_drop (hld_pkptr, data_size, ac);
                FRET (WlanC_AC_None);
                }
        /* Stamp the packet with the current time. This information will            */
        /* remain unchanged even if the packet is copied for                                */
        /* retransmissions, and      eventually it will be used by the                */
        /* destination MAC to compute the end-to-end delay.                    */
        op_pk_stamp (hld_pkptr);
        /* Enqueue the packet for transmission.                                              */
        wlan_hcf_hlpk_enqueue  (hld_pkptr,  ac,  dest_addr,  my_address,  up,  protocol_type,  data_size,
dest_info_ptr);
        /* Return the access category of the enqueued higher layer packet.        */
        FRET (ac);
        }
```

Part 2:

```
static void
wlan_hcf_physical_layer_data_arrival (void)
        {
        char                                                            msg_string [128];
        int                                                             accept;
        OpT_Int64                                                       dest_addr, remote_sta_addr;
        OpT_uInt8                                                       tid;
        OpT_uInt16                                                      prev_seq_num;
        OpT_Packet_Id                                       data_pkt_id;
        const WlanT_Data_Header_Fields*             pk_dhstruct_ptr;
        const WlanT_Control_Header_Fields*          pk_chstruct_ptr;
        const WlanT_QoS_Control_Fields*                     qos_info_ptr;
        WlanT_HCF_Peer_Info*                        src_sta_info_ptr;
        WlanT_HCF_Hld_Info*                         hld_info_ptr;
        WlanT_HCF_BA_State*                         ba_state_info_ptr;
        WlanT_Mac_Frame_Type                        rcvd_frame_type;
        WlanT_Phy_Char_Code                                         rcvd_frame_phy_char;
        WlanT_HCF_Ack_Policy                        ack_policy;
        Packet*                                     wlan_rcvd_frame_ptr;
        Packet*                                     seg_pkptr;
        const WlanT_Beacon_Body_Fields*                     pk_bbstruct_ptr;
        int                                                             rcvd_sta_bssid;
        int                                                             i;
        Boolean                 disable_signal_extension = OPC_FALSE;
        double                                                          rcvd_pk_size, rx_start_time;
        double                                                          total_retries;

        /** Process the frame received from the lower layer. This          **/
        /** routine decapsulate the frame and set appropriate flags        **/
        /** if the station needs to generate a response to the    **/
```

```
        /** received frame.                                        **/
        FIN (wlan_hcf_physical_layer_data_arrival (void));
        /*  Access received packet from the physical layer stream.      */
        wlan_rcvd_frame_ptr = op_pk_get (i_strm);
        /* Get the type of the received WLAN frame and check          */
        /* whether it is marked as a bad packet in the pipeline        */
        /* stages. Consider the possibility that we may receive a     */
        /* noise packet from a powerful jammer, which we need         */
        /* simply discard.                                            */
        if (op_pk_encap_flag_is_set (wlan_rcvd_frame_ptr, OMSC_JAMMER_ENCAP_FLAG_INDEX)
== OPC_FALSE)
                {
                op_pk_nfd_get_int32 (wlan_rcvd_frame_ptr, "Accept", &accept);
                op_pk_nfd_get_int32 (wlan_rcvd_frame_ptr, "Type", (int *) &rcvd_frame_type);
                }
/* this is modified my Palak on 3rd Nov. 2008*********************************/
        else
                {
                accept          = OPC_FALSE;
                rcvd_frame_type = WlanC_None;
                }

        /* If this is an ERP-OFDM packet and if we support 802.11g   */
        /* PHY, then it is received with 6 usec signal extension       */
        /* delay. Hence, reset the delay attribute of the packet*/
        /* stream from the receiver.                                  */
        if (accept && phy_type == WlanC_11g_PHY)
                {
                op_pk_nfd_get_int32 (wlan_rcvd_frame_ptr, "PHY Info", (int *)
&rcvd_frame_phy_char);
                if (rcvd_frame_phy_char == WlanC_ERP_OFDM_11g)
                        {
                op_ima_obj_attr_set (rx_state_info_ptr->mac_strm_objid, "delay", 0.0);
                        /* If the packet will be rejected due to a                  */
                        /* collision, then update the receiver idle time        */
                        /* accordingly, since the packet could not be           */
                        /* decoded, which disables the signal extension.        */
                        if (wlan_flags->rcvd_bad_packet == OPC_TRUE)
                                disable_signal_extension = OPC_TRUE;
                        }
                }
                /* ***************END of Modification *********************/
```

Part 3:

```
/* Make sure that the received packet is transmitted with a                 */
/* physical layer technology that is supported by us so that we can       */
/* decode and process the packet. Get the PHY info unless it is          */
/* already obtained (in case of 802.11g operation).                       */
        if (phy_type != WlanC_11g_PHY)
                op_pk_nfd_get_int32 (wlan_rcvd_frame_ptr, "PHY Info", (int *)
&rcvd_frame_phy_char);

        /***************This is modified by Palak on *********/
        /* Check for the support.*/
```

```
	if (!(rcvd_frame_phy_char == phy_char_flag || (phy_type == WlanC_11g_PHY &&
rcvd_frame_phy_char == WlanC_Direct_Sequence)))
		{
		/* It is an mismatching/unsupported PHY. Drop the packet and		*/
		op_pk_destroy (wlan_rcvd_frame_ptr);
		FOUT;
		}
	/* If we are in "scanning" mode, discard any packet received from		*/
	/* the physical layer, unless it is a beacon message. The packet is		*/
	/* not expected to be destined to this MAC anyway, since it is not		*/
	/* registered in a BSS that it is currently evaluating.			*/
	if (wlan_flags->scanning == OPC_TRUE && rcvd_frame_type != WlanC_Beac)
		{
		/* Printing out information to ODB.					*/
		if (wlan_trace_active == OPC_TRUE)
			{
			op_prg_odb_print_major ("Discarding the packet received from physical layer
during scanning process.", OPC_NIL);
			}
		/* Destroy the packet and quit the function.				*/
		op_pk_destroy (wlan_rcvd_frame_ptr);
		FOUT;
		}
```

Part 4:

```
static void
wlan_hcf_completed_frame_forward (Packet* seg_pkptr, OpT_Int64 src_addr, OpT_Int64 dest_addr,
OpT_Int64 final_dest_addr, int protocol_type,
 OpT_Packet_Id pkt_id, int tid)
	{
	Packet*								copy_pkptr;
	Boolean								send_to_higher;
	WlanT_HCF_Access_Category			tx_ac
	= WLANC_UP_TO_AC_MAPPING_ARRAY [tid];
	OpT_Packet_Size							pkt_size;
	char								msg_string [128];
	/** This function processes MSDUs that are fully received through		**/
	/** the physical layer, reassembled, and destined to this MAC. **/
	/** Based on their final destinations, such packets are either			**/
	/** forwarded to the MAC client, enqueued for transmission to its		**/
	/** final destination in the BSS (by APs) or both (in case of			**/
	/** broadcast).								**/
	FIN (wlan_hcf_completed_frame_forward (seg_pkptr, src_addr, dest_addr, final_dest_addr,
protocol_type, pkt_id, tid));
	if (ap_flag == OPC_BOOLINT_ENABLED)
		{
		/* If the address is not found in the address list then access		*/
		/* point will sent the data to higher layer for address			*/
		/* resolution. Note that if destination address is same as AP's	*/
		/* address then the packet is sent to higher layer for address	*/
		/* resolution. If the destination address is broadcast address	*/
		/* then the packet is both transmitted within the BSS and also	*/
		/* forwarded to the higher layer.					*/
```

```
                if (final_dest_addr == MAC_BROADCAST_ADDR ||
                        (final_dest_addr        !=        my_address        &&        prg_bin_hash_table_item_get
(peer_info_hash_tbl, (void *) &(final_dest_addr)) != PRGC_NIL))
                        {
                        /* Printing out information to ODB.                              */
                        if (wlan_trace_active == OPC_TRUE)
                                {
                                sprintf    (msg_string,    "All    fragments    of    data    packet    "
OPC_PACKET_ID_FMT " is received by the AP", pkt_id);
                                op_prg_odb_print_major (msg_string, "and enqueued for transmission
within the BSS.", OPC_NIL);
                                }
                        /* If the destination address is broadcast address then we       */
                        /* need to send a copy also to the higher layer.                 */
                        if (final_dest_addr == MAC_BROADCAST_ADDR)
                                {
                                copy_pkptr = op_pk_copy (seg_pkptr);
                                send_to_higher = OPC_TRUE;
                                }
                        else
                                {
                                copy_pkptr = seg_pkptr;
                                send_to_higher = OPC_FALSE;
                                }
                        /* Enqueuing packet for transmission within a subnet. First      */
                        /* register the outgoing traffic statistics for   the AC of      */
                        /* the packet, if necessary and check whether we have            */
                        /* sufficient buffer space to store the packet.                  */
if (!(wlan_ac_flags->stats_registered & WLANC_AC_BITMAP_ARRAY [tx_ac]))
        wlan_hcf_ac_statistics_register (tx_ac, OPC_TRUE);
                        /* Check the availability of the buffer space.                   */
                        pkt_size = op_pk_total_size_get (copy_pkptr);
                        if (total_hlpk_size + pkt_size > hld_max_size)
                                {
                                /* Buffer is too full to accept the packet.              */
                                wlan_hcf_hl_packet_drop (copy_pkptr, pkt_size, tx_ac);
                                }
                        else
                                {
                                /* Enqueue the packet.                                   */
wlan_hcf_hlpk_enqueue   (copy_pkptr,   tx_ac,   final_dest_addr,   src_addr,   tid,   protocol_type,   pkt_size,
PRGC_NIL);
                                }
                        }
                else
                        send_to_higher = OPC_TRUE;
                /* Send the packet to the higher layer if not destined within            */
                /* own BSS or if it has broadcast address as destination                 */
                /* address.                                                                      */
                if (send_to_higher == OPC_TRUE)
                        {
                        /* Update the local/global throughput and end-to-end delay       */
                        /* statistics based on the packet that will be forwarded to      */
                        /* the higher layer.                                                     */
```

```
            wlan_hcf_accepted_frame_stats_update (seg_pkptr, tx_ac);
            /* Set the contents of the LLC-destined ICI.                    */
            op_ici_attr_set_int64 (llc_iciptr, "src_addr", src_addr);
            op_ici_attr_set_int64 (llc_iciptr, "dest_addr", final_dest_addr);
            op_ici_attr_set (llc_iciptr, "protocol_type", protocol_type);
            /* Install the ICI.                                             */
            op_ici_install (llc_iciptr);
            /* Printing out information to ODB.                             */
            if (wlan_trace_active == OPC_TRUE)
                {
                sprintf (msg_string, "All fragments of Data packet "
OPC_PACKET_ID_FMT " is received and sent to the higher layer.", pkt_id);
                op_prg_odb_print_major (msg_string, OPC_NIL);
                }
/****************Modified by Palak on 12th march 2009**************/
            /* Sending data to higher layer.                                */

            if (protocol_type!=OMSC_PROTOCOL_TYPE_IP)
            {
                wlan_rcvd_pkt_higher_layer_forward (seg_pkptr, wlan_flags-
>bridge_flag, mac_client_reassembly_buffer, outstrm_to_sink);
            }
    else
            {
                wlan_rcvd_pkt_higher_layer_forward (seg_pkptr, wlan_flags-
>bridge_flag, mac_client_reassembly_buffer, outstrm_to_mac_if);
            }
    /******************************Modification Ends**************/
            }
        }
    else
        {
        /* If the station is a gateway and not an access point then do     */
        /* not send     data to higher layer for address resolution. This   */
        /* is for not allowing data to go out of the ad-hoc BSS.            */
        /* Except, in the case of broadcast packets and packets             */
        /* addressed to this station. On the other hand, if we are in a     */
        /* bridge/switch node and not AP enabled, then drop the packet.     */
        if ((wlan_flags->gateway_flag == OPC_TRUE  && dest_addr != my_address &&
dest_addr >= 0) ||
            wlan_flags->bridge_flag == OPC_TRUE)
            {
            /* Printing out information to ODB.                             */
            if (wlan_trace_active == OPC_TRUE)


                {
                strcpy (msg_string, "Gateway is not an access point so all received
fragments are discarded.");
                op_prg_odb_print_major (msg_string, OPC_NIL);
                }
            op_pk_destroy (seg_pkptr);
            }
        else
```

```
            {
            /* Update the local/global throughput and end-to-end delay      */
            /* statistics based on the packet that will be forwarded to      */
            /* the higher layer.                                             */
            wlan_hcf_accepted_frame_stats_update (seg_pkptr, tx_ac);
            /* Send the packet to the higher layer unless it is a            */
            /* spanning tree BPDU. No need to check whether the              */
            /* surrounding node is a bridge/switch since WLAN ports          */
            /* can't be used for bridge-to-bridge connections.               */
            if (dest_addr == BRIDGE_BROADCAST_ADDR || dest_addr == PVST_BPE_MCAST_ADDR)
                op_pk_destroy (seg_pkptr);
            else
                {
                /* Printing out information to ODB.                      */
                if (wlan_trace_active == OPC_TRUE)
                    {
                    sprintf (msg_string, "All fragments of Data packet " OPC_PACKET_ID_FMT " is received and sent to the higher layer.", pkt_id);
                    op_prg_odb_print_major (msg_string, OPC_NIL);
                    }
            /******Modified by Palak on 12th march 2009***************/
            /* Sending data to higher layer.                         */
            if (protocol_type!=OMSC_PROTOCOL_TYPE_IP)
            {
                wlan_rcvd_pkt_higher_layer_forward (seg_pkptr, wlan_flags->bridge_flag, mac_client_reassembly_buffer, outstrm_to_sink);
            }
            else
            {
                wlan_rcvd_pkt_higher_layer_forward (seg_pkptr, wlan_flags->bridge_flag, mac_client_reassembly_buffer, outstrm_to_mac_if);
            }
            /***************Modification Ends***************/
                }
            }
        }
    FOUT;
    }
```

D.2 wlan_mac_hcf_TRANSMIT_Exit_Executirives_GOOSE

```
/* Lock the mutex that serializes accessing the roaming related          */
/* information of this MAC.                                              */
op_prg_mt_mutex_lock (roam_state_ptr->roam_info_mutex, 0);
/* Check the interrupt type.                                             */
if (op_intrpt_type () == OPC_INTRPT_STAT)
    {
    /* If the packet is received while the the station is transmitting */
    /* then mark the received packet as bad.                           */
    intrpt_code = (WlanT_Mac_Intrpt_Code) op_intrpt_stat ();
```

```
    if (intrpt_code < TRANSMITTER_BUSY_INSTAT && op_stat_local_read (intrpt_code) >
rx_power_threshold &&
        wlan_flags->rcvd_bad_packet == OPC_FALSE &&
        (wlan_flags->bad_packet_dropped == OPC_FALSE || wlan_flags->receiver_busy ==
OPC_FALSE) &&
        rx_state_info_ptr->busy_due_to_jammer == OPC_FALSE)
        {
        wlan_flags->rcvd_bad_packet = OPC_TRUE;

        /* If we are transmitting a CTS-to-self, then mark it as bad,      */

        if (last_tx_frtype_arr [cur_tx_ac] == WlanC_Cts && expected_frame_type ==
WlanC_Cts)
            wlan_flags->rcvd_bad_cts = OPC_TRUE;
        }
    /* If we completed the transmission then reset the transmitter flag.*/
    else if (intrpt_code == TRANSMITTER_BUSY_INSTAT)
        {
        wlan_flags->transmitter_busy = OPC_FALSE;

        /* Also update the receiver idle time, since with the end of       */
        /* our transmission, the medium may become idle again. If the */
        /* transmission requires 11g signal extension, model the 6-usec             */
        /* no-transmission duration of signal extension by adjusting     */
        /* the receiver idle time accordingly.                                        */
        if (wlan_flags->wait_signal_ext == OPC_FALSE)
            rcv_idle_time = op_sim_time ();
        else
            {
    rcv_idle_time = op_sim_time () + WLANC_11g_SIGNAL_EXTENSION;
    wlan_flags->wait_signal_ext = OPC_FALSE;
            }
        /* "Response frame to send" will be set to QoS_Data if the                */
        /* current transmission is broadcast and we were planning to    */
        /* continue with another transmission within the current TXOP.            */
        /* When the transmission completes, if the receiver is busy,      */
        /* then this STA detects the collision involving its                          */
        /* transmission and terminates its TXOP prematurely.             */
        if (wlan_flags->receiver_busy == OPC_TRUE && fresp_to_send == WlanC_QoS_Data)
            fresp_to_send = WlanC_None;
        /* If we transmitted a CTS-to-self that is marked bad because  */
        /* of a colliding reception, then reset the corresponding flag,    */
        /* if our receiver is currently not      busy. That means, the                  */
        /* reception has started and ended while we were transmitting  */
        /* our CTS-to-self, and       therefore we can't detect that                  */
        /* collision. Hence, we have to assume that our CTS-to-self                 */
        /* transmission was            successful and to continue the frame                         */
        /* sequence with the transmission of the data frame.                      */
        if (wlan_flags->rcvd_bad_cts == OPC_TRUE && wlan_flags->receiver_busy ==
OPC_FALSE)
            wlan_flags->rcvd_bad_cts = OPC_FALSE;
        }
    }
/******************Modified by Palak on 12th March 2009 ************/
```

```
else if ((op_intrpt_type () == OPC_INTRPT_STRM) && (op_intrpt_strm () != instrm_from_mac_if))
/*&& (op_intrpt_strm () != instrm_from_source))*/
        {
        /* While transmitting, we received a packet from physical layer.          */
        /* Mark the packet as bad.                                                */
        wlan_flags->rcvd_bad_packet = OPC_TRUE;
        /* If we are transmitting a CTS-to-self, then mark it as bad too.         */
        if (last_tx_frtype_arr [cur_tx_ac] == WlanC_Cts && expected_frame_type == WlanC_Cts)
                wlan_flags->rcvd_bad_cts = OPC_TRUE;
        }
/* Call the interrupt processing routine for each interrupt.                      */
wlan_hcf_interrupts_process ();
```

D.3 wlan_mac_interface_Function Block_GOOSE_final

```
static void
wlan_mac_higher_layer_intf_sv_init ()
        {
        int                     type_of_service;
        int                     integer_mac_address = -1;
        /** Initializes all state variables used in this  **/
        /** process model.                                 **/
        IN (wlan_mac_higher_layer_intf_sv_init ());
        /* Object identifier for the surrounding module and node.       */
        my_objid = op_id_self ();
        my_node_objid = op_topo_parent (my_objid);
        /* Stream indices to and from the WLAN MAC process.             */
        /* these will be set in the "exit execs" of "init".     */
        outstrm_to_mac  = OPC_INT_UNDEF;
        instrm_from_mac = OPC_INT_UNDEF;
        /* Determine the destination to which packet should    */
        /* be sent,and the prioritization to be provided to     */
        /* the transmitted packet.                              */
        op_ima_obj_attr_get (my_objid, "Destination Address", &integer_mac_address);
        destination_address = integer_mac_address;
        op_ima_obj_attr_get (my_objid, "Type of Service",     &type_of_service);
        /* Some interface control information is needed to      */
        /* indicate to the MAC of the destination to which      */
        /* a given packet needs to be sent. Create it.          */
        wlan_mac_req_iciptr = op_ici_create ("wlan_mac_request");
        op_ici_attr_set (wlan_mac_req_iciptr, "type_of_service", type_of_service);
        op_ici_attr_set (wlan_mac_req_iciptr, "protocol_type",   -1);

        FOUT;
        }
static void
wlan_mac_higher_layer_register_as_arp ()
        {
        char                            proc_model_name [128];
        OmsT_Pr_Handle                  own_process_record_handle;
```

```
Prohandle                               own_prohandle;
/** Register this process in the model-wide process registry.     **/
FIN (wlan_mac_higher_layer_register_as_arp ());
/* Obtain the process model name and process handle.              */
op_ima_obj_attr_get (my_objid, "process model", proc_model_name);
own_prohandle = op_pro_self ();
/* Register this process in the model-wide process registry        */
own_process_record_handle = (OmsT_Pr_Handle) oms_pr_process_register (
                    my_node_objid, my_objid, own_prohandle, proc_model_name);
/***************Modified by Palak on 17th March********************/
/* Register this protocol attribute and the element address        */
/* of this process into the model-wide registry.                   */
oms_pr_attr_set (own_process_record_handle,
          "protocol",               OMSC_PR_STRING,               "arp1",
          "location",               OMSC_PR_STRING,               "mac_if",
          OPC_NIL);
FOUT;
```

Appendix E Radio Noise in Substations

Major radio noises available in a power substation environment can be divided in two different types: 1) Electro-Magnetic Interferences (EMI) from gap or insulation breakdown due to switching operation of SF6 circuit breaker or disconnector, lightning discharge, corona discharge, etc.; 2) Interferences from other radio devices (i.e. RFI) installed within substation or in vicinity of a substation. There are other background noises, e.g. temperature at the receiver antenna, atmospheric weather condition, etc.

E.1 Existing Noise Model in OPNET

E.1.1 Interference Noise

The interference noise stage is the ninth stage of the radio transceiver pipeline, and is specified by the "inoise model" attribute of the radio receiver. It is executed for a packet under two circumstances: the packet is valid and arrives at its destination channel while another packet is already being received, or the packet is valid and already being received when another packet (valid or invalid) arrives. The first circumstance can occur at most once for each packet, and the second can occur any number of times depending upon the transmission activities of other transmitters in the model.

E.1.2 Background Noise

The background noise stage is the tenth stage of the radio transceiver pipeline, and is specified by the "bkgnoise model" attribute of the radio receiver. It is executed immediately after return of the received power stage, with no simulation time elapsing in between. This stage considers ambient temperature, background noise level, etc. The purpose of this stage is to represent the effect of all noise sources except for other concurrently arriving transmissions (because these are accounted for by the interference noise stage). The expected result is the sum of the power (in watts) of other noise sources, measured at the receiver's location and in the receiver channel's band.

E.2 Implementation of Substation Noise Model in OPNET

The implementation of substation noise model in the pipeline stages of OPNET tool, especially background noise pipeline stage. It can be observed from the code below that the noise models for normal distribution and generalized extreme value distribution are implemented as a background noise.

```
/* dra_bkgnoise.ps.c */
/* Default background noise model for radio link Transceiver Pipeline */
#include "opnet.h"

//added by Palak
#include "math.h"
/***** constants *****/
#define BOLTZMANN                       1.379E-23
#define BKG_TEMP                        290.0
#define AMB_NOISE_LEVEL                 1.0E-26

/***** procedure *****/
#if defined (__cplusplus)
extern "C"
#endif
void

dra_bkgnoise_mt (OP_SIM_CONTEXT_ARG_OPT_COMMA Packet * pkptr)
        {
        double          rx_noisefig, rx_temp, rx_bw;
        double          bkg_temp, bkg_noise, amb_noise;

//added by Palak
//For NOrmal Distribution
        // double       r=0,Mean,Variance;
        //      Distribution* dist_ptr;

//For Generlized Extreme Value Distribution
         double         substation_noise=0,u,k,mu,sigma,R;

        //addition ends

        /** Compute noise sources other than transmission interference. **/
        FIN_MT (dra_bkgnoise (pkptr));

        /* Get receiver noise figure. */
        rx_noisefig = op_td_get_dbl (pkptr, OPC_TDA_RA_RX_NOISEFIG);

        /* Calculate effective receiver temperature. */
        rx_temp = (rx_noisefig - 1.0) * 290.0;

        /* Set the effective background temperature. */
```

```
bkg_temp = BKG_TEMP;

/* Get receiver channel bandwidth (in Hz). */
rx_bw = op_td_get_dbl (pkptr, OPC_TDA_RA_RX_BW);


/*This code is added by Palak March 2011 */
// r = op_dist_uniform (1e-12);

// Normal Distribution
/* Mean=2e-13;
Variance=2.33e-27;

dist_ptr = op_dist_load ("normal", Mean, Variance);

substation_noise= op_dist_outcome(dist_ptr);
op_dist_unload (dist_ptr); */

// printf("r=%lf",r);

// Generlized Extreme Value Distribution
k=-0.0453376;
mu= 1.96053e-13; // can be varied in order to change the SNFR
sigma= 4.14563e-14;

u=op_dist_uniform (1);
R=(exp(-k*log(-log(u)))-1)/k;
substation_noise=mu+sigma*R;

/* Calculate in-band noise from both background and thermal sources. */
bkg_noise = (rx_temp + bkg_temp) * rx_bw * BOLTZMANN + substation_noise;

/* Calculate in-band ambient noise. */
amb_noise = rx_bw * AMB_NOISE_LEVEL;

/* Put the sum of both noise sources in the packet transmission data attr.*/
op_td_set_dbl (pkptr, OPC_TDA_RA_BKGNOISE, (amb_noise + bkg_noise));
FOUT
}
```

Curriculum Vitae

Name: Palak Parikh

EDUCATION

- PhD in Electrical and Computer Engineering, 2007 –2011
  University of Western Ontario, London, ON
- Master in Power System Engineering, 2003- 2005
  Sardar Patel University, Gujarat, India
- Bachelor in Electrical Engineering, 1999- 2003
  Sardar Patel University, Gujarat, India

EXPERIENCE

Industrial:

- **Application Engineer (Protection & Control), GE Digital Energy** 2011-Cont.
  Involved in product research and development for distribution automation & industrial product lines. Also, supported for developing product manual, white paper, test plans, etc.

Research:

- **Research Assistantship**, University of Western Ontario 2007- 2011
  worked on research project partially funded by Hydro-One and Ontario Center of Excellence (OCE).

Teaching:

- **Teaching Assistantship**, University of Western Ontario 2007 - 2011
  Conducting undergraduate laboratories, grading reports and exams.
- **Lecturer**, A. D. Patel Institute of Technology, Gujarat, India. 2005- 2007
  Supervised four undergraduate projects, mentored 38 students as a Faculty Advisor, organized several Industrial visits, and initiated Personality Development Training Program in the department for the undergraduates.

RESEARCH AND TECHNICAL SKILLS

- Applications for Distribution automation & protection (esp. sensors, and FDIR); as well as, Arc Flash industrial protection systems.
- Noise/interference measurements at 27.6 kV and 13.8 kV distribution substations in the high frequency bands of WLAN (2.4-2.5GHz, and 5.8 GHz) and WIMAX (1.7 - 1.8 GHz); Modeling and analysis of measured noise in MATLAB
- Development of IEEE 802.11 (wireless LAN) based Protection & Control relay/IED and merging unit using embedded industrial computers in a laboratory environment
- Development of IEEE 802.11 based wireless automation device models in OPNET
- Helped in writing research project proposal to obtain industrial funding at University of Western Ontario
- Writing, presenting, and reviewing papers for journals/conference
- **Hardware Tools:** Real Time Digital Simulator (RTDS); Embedded industrial systems; RuggedCom Industrial Wireless Router and Ethernet switches; Agilent E4402B Spectrum Analyzer; CACE Pilot Network Analyzer, Microprocessor 8085, Microcontroller 8051.
- **Simulation Tools:** MATLAB/SIMULINK, PSCAD, RSCAD, OPNET, P-SPICE.

PUBLICATIONS

1. "A Comprehensive Investigation of Wireless LAN for IEC 61850 Based Smart Distribution Substation Applications," [Selected for Publication], IEEE Transaction on Industrial Informatics, 2012.

2. "Modeling and performance evaluation of WLAN technologies for IEC 61850 based smart distribution substations," [under internal review], IET Journal, 2012.

3. "Configuration and Performance Testing of IEC 61850 GOOSE," in proc. The International Conference on Advanced Power System Automation and Protection, Aug. 2011.

4. "Opportunities and Challenges of Wireless Communication Technologies for Smart Grid Applications," *in Proc. IEEE PES General Meeting,* Minneapolis, USA, July 2010.

5. "Evaluation of Communication Technologies for IEC 61850 based Distribution Automation System with Distributed Energy Resources," *in Proc. IEEE PES General Meeting,* Calgary, July 2009.

6. “Implementation issues with IEC 61850 based substation automation systems,” *in Proc. National Power System Conference-08,* India, Dec. 2008.

PROFESSIONAL TRAINING / WORKSHOPS

- GE Digital Energy Interactive CD course on Power System Protection at University of Western Ontario, Canada [Dec. 2009].
- ABB workshop on IEC 61850, Burlington. [May, 2009]
- Tutorial on “Distribution Automation for Smart Grid”, by S. S. (Mani) Venkata, [Dec. 2008].
- GE Seminar on “Reduce your Substation Communication Cost”, Niagara Falls [Sept. 2008].
- Seminar on “Diagnostic Testing & Condition Monitoring of Power Plant Equipment” at Nasik, India [Jan., 2007].
- Workshop on “Application of Power electronics devices in Power system” at Energy Research and Development Association (ERDA), Vadodara, India [June 2006].
- Workshop on “Computational Electromagnetic” at IIT Bombay, Powai, India [Nov. 2005].
- Training at L & T Switchgear training center, Pune, India [April, 2004].
- Training at Thermal Power Station at Wanakbori, Gujarat, India [June, 2002].

RESEARCH PROJECTS UNDERTAKEN

- PhD Thesis [Tentative]: “Performance Evaluation of Wireless LAN for IEC 61850 Based Smart Distribution Substations”.
- Master’s Thesis [June, 2005]: “Power Quality Improvement with the help of Active Power Filter”. Using MATLAB/SIMULINK, Active Power Filter (APF) and its controller have been simulated to comply with Power Quality standard (IEC 61400-21). It has been showed that using APF, 28.64% total harmonic distortion (THD) of non-linear load can be reduced to 1.42%. Furthermore, APF has improved power factor to unity for highly inductive loads.
- Modeling and control of grid-connected PMSG based Wind Energy Conversion System (WECS) using PSCAD/EMTDC and MATLAB.
- Performance evaluation of IEC 61850 based Process bus of Substation Automation System.
- Report on review of Distribution Automation System (DAS)
- Power System and its Component Analysis with help of MATLAB Programming

MAJOR CREDITED COURSES

- Computer based Power System Protection, Advance Digital Signal Processing, Power Electronics Converter System, Performance Evaluation and Modeling of Computer Networking, Communication System and Data Networking, Wireless Communication,

  Power System Switchgears, Microprocessor Application to Power Systems, Power System Practice and Design, Power System Operation and Control, Power System Reliability & Evaluation.

UNDERGRADUTE PROJECTS SUPERVISED

- Single Sided Linear Induction Motor (SLIM): Experimental lab model of SLIM has been developed successfully for the Electrical Machines lab.
- Area Measuring Robot using IC89S52: Developed working model of Robot Arm for autonomous operation.
- Microcontroller Based Automation System Using DTMF (Dual Tone Multi Frequency)

POSITION OF RESPONSIBILITY

- **International Journal Reviewer:**
  - IEEE Transaction on Smart Grid
  - IEEE Transaction on Industrial Electronics
  - Journal of Computer Systems, Networks, and Communications
- Convener of Poster Presentation Competition organizes by IEEE students chapter at ADIT college, India.
- Member of organizing committee for Paper Presentation Competition on the occasion of National Science Day Celebration 2006 at ADIT college, India [Feb. 2006].
- Active member of the department for Personality Development Training & Placement Activities.
- Solely organized industrial visits to ABB, Atlanta Transfomers Ltd., Wanakbori thermal power plant, Kadana Hydro power plant, etc. for undergraduates.

COMPUTER SKILLS

- Operating Systems: QNX Real-Time Operating System; Microsoft Windows.
- Languages: FORTRAN, C/C++, Assembly language for Microprocessor 8085, and microcontroller 8051.