

4-2018

Traffic Characterization of an Internet of Things(IOT) Network Architecture

Maitha Saif Salem Mohammed Alderei

Follow this and additional works at: https://scholarworks.uaeu.ac.ae/electric_theses



Part of the [Engineering Commons](#)

Recommended Citation

Mohammed Alderei, Maitha Saif Salem, "Traffic Characterization of an Internet of Things(IOT) Network Architecture" (2018). *Electrical Engineering Theses*. 11.
https://scholarworks.uaeu.ac.ae/electric_theses/11

This Thesis is brought to you for free and open access by the Electrical Engineering at Scholarworks@UAEU. It has been accepted for inclusion in Electrical Engineering Theses by an authorized administrator of Scholarworks@UAEU. For more information, please contact fadl.musa@uaeu.ac.ae.

UAEU



جامعة الإمارات العربية المتحدة
United Arab Emirates University

United Arab Emirates University

College of Engineering

Department of Electrical Engineering

TRAFFIC CHARACTERIZATION OF AN INTERNET OF THINGS
(IOT) NETWORK ARCHITECTURE

Maitha Saif Salem Mohammed Alderei

This thesis is submitted in partial fulfilment of the requirements for the degree of
Master of Science in Electrical Engineering

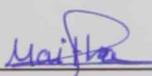
Under the Supervision of Dr. Atef Amin Abdrabou

April 2018

Declaration of Original Work

I, Maitha Saif Salem Mohammed Alderei, the undersigned, a graduate student at the United Arab Emirates University (UAEU), and the author of this thesis entitled "*Traffic Characterization of an Internet of Things (IoT) Network Architecture*", hereby, solemnly declare that this thesis is my own original research work that has been done and prepared by me under the supervision of Dr. Atef Amin Abdrabou, in the College of Engineering at UAEU. This work has not previously been presented or published, or formed the basis for the award of any academic degree, diploma or a similar title at this or any other university. Any materials borrowed from other sources (whether published or unpublished) and relied upon or included in my thesis have been properly cited and acknowledged in accordance with appropriate academic conventions. I further declare that there is no potential conflict of interest with respect to the research, data collection, authorship, presentation and/or publication of this thesis.

Student's Signature: _____



Date: _____

16/5/2018

Approval of the Master Thesis

This Master Thesis is approved by the following Examining Committee Members:

- 1) Advisor (Committee Chair): Dr. Atef Amin Abdrabou

Title: Associate Professor

Department of Electrical Engineering

College of Engineering

Signature 

Date 8/5/2018

- 2) Member: Dr. Qurban Ali Memon

Title: Associate Professor

Department of Electrical Engineering

College of Engineering

Signature 

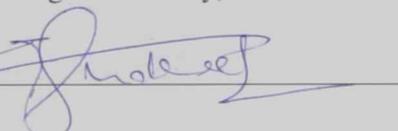
Date 08-05-2018

- 3) Member (External Examiner): Dr. Liang Cheng

Title: Associate Professor

Department of Computer Science and Engineering

Institution: Lehigh University, USA

Signature 

Date 08-05-2018

for

DR. M. S. LAGHARI

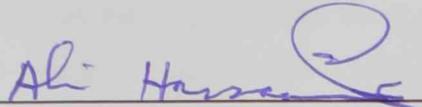
EE Graduate Program Coordinator

This Master Thesis is accepted by:

Dean of the College of Engineering: Professor Sabah Alkass

Signature  Date 15/5/2018

fa Dean of the College of Graduate Studies: Professor Nagi T. Wakim

Signature  Date 16/5/2018

Copyright © 2018 Maitha Saif Salem Mohammed Alderei
All Rights Reserved

Abstract

Internet of things (IoT) is an evolving paradigm that is currently getting more attention and rapidly gaining importance. The basic idea of IoT is to connect everyone and everything to the Internet for information exchange. It is essential to develop a clear understanding of characteristics of IoT traffic sources as well as to find a traffic model that efficiently characterizes the statistical behavior of IoT traffic. Since many IoT devices generate relatively small sized data, we are particularly interested in an IoT network architecture where data from a number of different IoT devices are aggregated at an IoT gateway. We focus on characterizing the IoT aggregated traffic pattern for three common IoT applications with real-time and non-real-time quality of service (QoS) requirements. These applications include healthcare, smart cities, and video surveillance. Our study is based on generating a real IoT traffic trace in a lab by using various sensors and devices in the aforementioned applications. The generated traffic trace is transmitted wirelessly over the air using Wi-Fi technology to an IoT gateway. The input network traffic to this gateway is characterized. In the experiments, the amount of input traffic to the gateway is varied and different traffic patterns for each of the selected applications are examined. Statistical tests and parameters are used to determine the best matching packet inter-arrival time distribution for different traffic penetrations. Moreover, we also examine packet size distributions. Based on our empirical data, the experimental results indicate that IoT packet inter-arrival time follows a Pareto distribution. However, it can be better modeled as a Weibull distribution in some traffic patterns. Our experimental results also reveal that the packet size distribution of different penetrations of the studied IoT applications is not in a good match with the commonly used Geometric distribution. Furthermore, we investigate the impact of traffic characterization on the performance of the considered IoT network architecture for a certain availability of network resources using computer simulations.

Keywords: IoT, QoS, Wi-Fi, packet inter-arrival time distribution, packet size distribution, IoT gateway, traffic model.

Title and Abstract (in Arabic)

توصيف حركة المرور لبنية شبكة إنترنت الأشياء

الملخص

يعتبر إنترنت الأشياء نموذج متطور، يحظى في الوقت الحاضر على الكثير من الاهتمام ويحصد أهمية متزايدة. الفكرة الأساسية لإنترنت الأشياء هي توصيل كل شخص وكل شيء على شبكة الإنترنت بهدف تبادل المعلومات. من الضروري فهم خصائص مصادر حركة المرور لهذه الشبكة بشكل واضح بالإضافة إلى إيجاد نموذج يصف بكفاءة وفعالية السلوك الإحصائي لحركة المرور. نظراً لأن العديد من الأجهزة التي تستخدم في إنترنت الأشياء تنتج بيانات ذات حجم صغير نسبياً، فإننا مهتمون في هذه الأطروحة ببنية شبكة إنترنت الأشياء حيث يتم تجميع البيانات من عدد من الأجهزة المختلفة في بوابة إنترنت الأشياء. ونركز على وصف نمط حركة المرور المجمع لثلاثة تطبيقات شائعة لإنترنت الأشياء مع متطلبات جودة الخدمة في الزمن الحقيقي وغير الحقيقي. وتشمل هذه التطبيقات الرعاية الصحية والمدن الذكية والمراقبة بالفيديو. تستند دراستنا على إنشاء تتبع حقيقي لحركة مرور إنترنت الأشياء في المختبر باستخدام أجهزة استشعار وأجهزة مختلفة مستخدمة بالفعل في التطبيقات المذكورة أعلاه. يتم نقل حركة المرور لاسلكياً عبر الأثير باستخدام تقنية الواي فاي إلى بوابة إنترنت الأشياء. ثم يتم توصيف مدخلات حركة المرور إلى هذه البوابة. في التجارب المجراة، يتم تغيير مقدار حركة المرور المدخلة إلى البوابة بالإضافة إلى دراسة أنماط مختلفة من حركة المرور لكل تطبيق من التطبيقات المستخدمة. اختبارات ومعايير إحصائية استخدمت لتحديد أفضل توزيع لوقت الوصول بين الحزم لأنماط حركة المرور المختلفة. علاوة على ذلك، نقوم أيضاً بدراسة توزيع حجم الحزمة. استناداً إلى بياناتنا التجريبية، تشير النتائج إلى أن وقت الوصول بين حزم إنترنت الأشياء يتبع توزيع باريتو. مع ذلك، بعض أنماط الحركة يتم توصيفها بشكل أفضل كتوزيع وايبل. وتكشف نتائجنا التجريبية أيضاً أن توزيع حجم الحزمة لمختلف أنماط تطبيقات إنترنت الأشياء المدروسة لا يتطابق بشكل جيد مع التوزيع الهندسي. علاوة على ذلك، نقوم بالتحري عن تأثير توصيف حركة المرور على أداء بنية شبكة إنترنت الأشياء المدروسة مع توافر موارد معينة للشبكة باستخدام المحاكاة الحاسوبية.

مفاهيم البحث الرئيسية: إنترنت الأشياء، جودة الخدمة، واي فاي، توزيع وقت الوصول بين الحزم، توزيع حجم الحزمة، بوابة إنترنت الأشياء، نموذج حركة المرور.

Acknowledgements

I would like to express my deepest gratitude and appreciation to my thesis advisor Dr. Atef Abdrabou for his guidance, continuous encouragement and support throughout the thesis duration.

I would like to thank my committee for their guidance, support, and assistance throughout my preparation of this thesis. I would like to thank the chair and all members of the Department of Electrical Engineering at the United Arab Emirates University for assisting me all over my studies and research. My special thanks are extended to the Library Research Desk for providing me with the relevant reference material.

Special thanks go to my parents, brothers, and my only sister who helped to reach my goal. I am sure they suspected it was endless. In addition, special thanks are extended to my colleagues for their assistance and friendship.

Dedication

To my beloved parents and family

Table of Contents

Title	i
Declaration of Original Work.....	ii
Copyright.....	iii
Approval of the Master Thesis	iv
Abstract	vi
Title and Abstract (in Arabic).....	vii
Acknowledgements.....	viii
Dedication	ix
Table of Contents.....	x
List of Tables	xii
List of Figures.....	xiii
List of Abbreviations	xvi
Chapter 1: Introduction	1
1.1 Overview	1
1.2 IoT Challenges	3
1.2.1 Traffic Characterization	3
1.2.2 Quality of Service	4
1.2.3 Security and Privacy Challenges	4
1.2.4 Big Data Analytics	5
1.3 IoT Applications.....	6
1.3.1 Healthcare.....	6
1.3.2 Smart City.....	6
1.4 Thesis Research.....	7
1.5 Thesis Organization.....	7
Chapter 2: Background and Related Works.....	8
2.1 IoT Applications.....	8
2.1.1 Smart Cities	9
2.1.2 Healthcare.....	10
2.1.3 Security and Surveillance	13
2.1.4 Smart Business and Product Management	14
2.2 IoT Architecture	15
2.2.1 Three-layer Architecture	15
2.2.2 Five-layer Architecture	17
2.3 Traffic Characterization.....	20
2.3.1 Probability Distribution.....	21

2.4 Related Works	24
Chapter 3: System Model	27
3.1 Proposed Study	27
3.1.1 Perception Layer	28
3.1.2 Network Layer	30
3.2 Communication Layers	33
3.2.1 Physical Layer	33
3.2.2 Data Link Layer	33
3.2.3 Transport Layer	36
Chapter 4: Results and Discussion	38
4.1 Experimental Setup	38
4.1.1 Healthcare Traffic	40
4.1.2 Smart Cities Traffic	47
4.1.3 Video Surveillance Traffic	52
4.2 Experimental Results	54
4.2.1 IoT Packet Inter-arrival Time Distribution	54
4.2.2 IoT Packet Size Distribution	100
4.3 Impact of Traffic Characterization on Resource Allocation	108
4.3.1 Traffic Pattern 1: Equal Percentage of the Three Applications	109
4.3.2 Traffic Pattern 2: Healthcare Application only	111
Chapter 5: Conclusion and Future Directions	113
References	116

List of Tables

Table 2.1: Applications Areas of IoT	8
Table 3.1: Communication Protocols for IoT-based Smart Cities	34
Table 3.2: IEEE 802.11n PHY Standards	35
Table 4.1: Gases Sensors Format	48
Table 4.2: Smart Cities Sensors Format.....	50
Table 4.3: Distributions' Parameters for Pattern 1 & 6 Nodes	57
Table 4.4: Distributions' Parameters for Pattern 1 & 9 Nodes	58
Table 4.5: Distributions' Parameters for Pattern 1 & 12 Nodes.....	59
Table 4.6: Distributions' Parameters for Pattern 1 & 15 Nodes.....	60
Table 4.7: Distributions' Parameters for Pattern 2 & 6 Nodes	64
Table 4.8: Distributions' Parameters for Pattern 2 & 9 Nodes	64
Table 4.9: Distributions' Parameters for Pattern 2 & 12 Nodes.....	65
Table 4.10: Distributions' Parameters for Pattern 2 & 15 Nodes.....	66
Table 4.11: Distributions' Parameters for Pattern 3 & 6 Nodes.....	70
Table 4.12: Distributions' Parameters for Pattern 3 & 9 Nodes.....	71
Table 4.13: Distributions' Parameters for Pattern 3 & 12 Nodes.....	72
Table 4.14: Distributions' Parameters for Pattern 3 & 15 Nodes.....	73
Table 4.15: Distributions' Parameters for Pattern 4 & 6 Nodes.....	76
Table 4.16: Distributions' Parameters for Pattern 4 & 9 Nodes.....	77
Table 4.17: Distributions' Parameters for Pattern 4 & 12 Nodes.....	78
Table 4.18: Distributions' Parameters for Pattern 4 & 15 Nodes.....	79
Table 4.19: Distributions' Parameters for Pattern 5 & 6 Nodes.....	82
Table 4.20: Distributions' Parameters for Pattern 5 & 9 Nodes.....	83
Table 4.21: Distributions' Parameters for Pattern 5 & 12 Nodes.....	84
Table 4.22: Distributions' Parameters for Pattern 5 & 15 Nodes.....	85
Table 4.23: Distributions' Parameters for Pattern 6 & 6 Nodes.....	88
Table 4.24: Distributions' Parameters for Pattern 6 & 9 Nodes.....	89
Table 4.25: Distributions' Parameters for Pattern 6 & 12 Nodes.....	90
Table 4.26: Distributions' Parameters for Pattern 6 & 15 Nodes.....	91
Table 4.27: Distributions' Parameters for Pattern 7 & 6 Nodes.....	94
Table 4.28: Distributions' Parameters for Pattern 7 & 9 Nodes.....	95
Table 4.29: Distributions' Parameters for Pattern 7 & 12 Nodes.....	96
Table 4.30: Distributions' Parameters for Pattern 7 & 15 Nodes.....	97

List of Figures

Figure 1.1: Projected Market Share of Dominant IoT Applications by 2020	2
Figure 2.1: IoT Healthcare Services and Applications	10
Figure 2.2: Three-layer Architecture of IoT.....	16
Figure 2.3: Five-layer Architecture of IoT.....	18
Figure 3.1: Single-Hop Star Topology.....	31
Figure 3.2: Proposed System Model.....	32
Figure 4.1: Experimental Setup Diagram.....	38
Figure 4.2: Wasmote ASCII Frame Structure	40
Figure 4.3: ECG Sensor Placement	42
Figure 4.4: Media Bridge Mode	43
Figure 4.5: LAN for ECG Measuring System.....	43
Figure 4.6: ECG Waveform	44
Figure 4.7: EMG Sensor Placement	45
Figure 4.8: EMG Waveform	46
Figure 4.9: Wasmote Gases Board	48
Figure 4.10: LAN for Smart Cities Sensors	50
Figure 4.11: Light Sensor Circuit Diagram.....	51
Figure 4.12: Light Sensor Connection	51
Figure 4.13: WLAN for Video Streaming	52
Figure 4.14: Streaming Process.....	53
Figure 4.15: CDF of Inter-arrival Time for Pattern 1 & 6 Nodes	57
Figure 4.16: CDF of Inter-arrival Time for Pattern 1 & 9 Nodes	58
Figure 4.17: CDF of Inter-arrival Time for Pattern 1 & 12 Nodes	59
Figure 4.18: CDF of Inter-arrival Time for Pattern 1 & 15 Nodes	60
Figure 4.19: Distribution Fitting Results for Pattern 1 & 6 Nodes.....	61
Figure 4.20: Distribution Fitting Results for Pattern 1 & 9 Nodes.....	61
Figure 4.21: Distribution Fitting Results for Pattern 1 & 12 Nodes.....	62
Figure 4.22: Distribution Fitting Results for Pattern 1 & 15 Nodes.....	62
Figure 4.23: CDF of Inter-arrival Time for Pattern 2 & 6 Nodes	63
Figure 4.24: CDF of Inter-arrival Time for Pattern 2 & 9 Nodes	64
Figure 4.25: CDF of Inter-arrival Time for Pattern 2 & 12 Nodes	65
Figure 4.26: CDF of Inter-arrival Time for Pattern 2 & 15 Nodes	66
Figure 4.27: Distribution Fitting Results for Pattern 2 & 6 Nodes.....	67
Figure 4.28: Distribution Fitting Results for Pattern 2 & 9 Nodes.....	68
Figure 4.29: Distribution Fitting Results for Pattern 2 & 12 Nodes.....	68
Figure 4.30: Distribution Fitting Results for Pattern 2 & 15 Nodes.....	69
Figure 4.31: CDF of Inter-arrival Time for Pattern 3 & 6 Nodes	70
Figure 4.32: CDF of Inter-arrival Time for Pattern 3 & 9 Nodes	71
Figure 4.33: CDF of Inter-arrival Time for Pattern 3 & 12 Nodes	72
Figure 4.34: CDF of Inter-arrival Time for Pattern 3 & 15 Nodes	73

Figure 4.35: Distribution Fitting Results for Pattern 3 & 6 Nodes.....	74
Figure 4.36: Distribution Fitting Results for Pattern 3 & 9 Nodes.....	74
Figure 4.37: Distribution Fitting Results for Pattern 3 & 12 Nodes.....	75
Figure 4.38: Distribution Fitting Results for Pattern 3 & 15 Nodes.....	75
Figure 4.39: CDF of Inter-arrival Time for Pattern 4 & 6 Nodes	76
Figure 4.40: CDF of Inter-arrival Time for Pattern 4 & 9 Nodes	77
Figure 4.41: CDF of Inter-arrival Time for Pattern 4 & 12 Nodes	78
Figure 4.42: CDF of Inter-arrival Time for Pattern 4 & 15 Nodes	79
Figure 4.43: Distribution Fitting Results for Pattern 4 & 6 Nodes.....	80
Figure 4.44: Distribution Fitting Results for Pattern 4 & 9 Nodes.....	80
Figure 4.45: Distribution Fitting Results for Pattern 4 & 12 Nodes.....	81
Figure 4.46: Distribution Fitting Results for Pattern 4 & 15 Nodes.....	81
Figure 4.47: CDF of Inter-arrival Time for Pattern 5 & 6 Nodes	82
Figure 4.48: CDF of Inter-arrival Time for Pattern 5 & 9 Nodes	83
Figure 4.49: CDF of Inter-arrival Time for Pattern 5 & 12 Nodes	84
Figure 4.50: CDF of Inter-arrival Time for Pattern 5 & 15 Nodes	85
Figure 4.51: Distribution Fitting Results for Pattern 5 & 6 Nodes.....	86
Figure 4.52: Distribution Fitting Results for Pattern 5 & 9 Nodes.....	86
Figure 4.53: Distribution Fitting Results for Pattern 5 & 12 Nodes.....	87
Figure 4.54: Distribution Fitting Results for Pattern 5 & 15 Nodes.....	87
Figure 4.55: CDF of Inter-arrival Time for Pattern 6 & 6 Nodes	88
Figure 4.56: CDF of Inter-arrival Time for Pattern 6 & 9 Nodes	89
Figure 4.57: CDF of Inter-arrival Time for Pattern 6 & 12 Nodes	90
Figure 4.58: CDF of Inter-arrival Time for Pattern 6 & 15 Nodes	91
Figure 4.59: Distribution Fitting Results for Pattern 6 & 6 Nodes.....	92
Figure 4.60: Distribution Fitting Results for Pattern 6 & 9 Nodes.....	92
Figure 4.61: Distribution Fitting Results for Pattern 6 & 12 Nodes.....	93
Figure 4.62: Distribution Fitting Results for Pattern 6 & 15 Nodes.....	93
Figure 4.63: CDF of Inter-arrival Time for Pattern 7 & 6 Nodes	94
Figure 4.64: CDF of Inter-arrival Time for Pattern 7 & 9 Nodes	95
Figure 4.65: CDF of Inter-arrival Time for Pattern 7 & 12 Nodes	96
Figure 4.66: CDF of Inter-arrival Time for Pattern 7 & 15 Nodes	97
Figure 4.67: Distribution Fitting Results for Pattern 7 & 6 Nodes.....	98
Figure 4.68: Distribution Fitting Results for Pattern 7 & 9 Nodes.....	98
Figure 4.69: Distribution Fitting Results for Pattern 7 & 12 Nodes.....	99
Figure 4.70: Distribution Fitting Results for Pattern 7 & 15 Nodes.....	99
Figure 4.71: CDF of Packet Size for Pattern 1	101
Figure 4.72: Comparison with Geometric Distribution for Pattern 1	102
Figure 4.73: CDF of Packet Size for Pattern 2.....	103
Figure 4.74: Comparison with Geometric Distribution for Pattern 2	103
Figure 4.75: CDF of Packet Size for Pattern 3.....	104
Figure 4.76: Comparison with Geometric Distribution for Pattern 3	104
Figure 4.77: CDF of Packet Size for Pattern 4.....	105

Figure 4.78: Comparison with Geometric Distribution for Pattern 4	105
Figure 4.79: CDF of Packet Size for Pattern 5	106
Figure 4.80: Comparison with Geometric Distribution for Pattern 5	106
Figure 4.81: CDF of Packet Size for Pattern 6	107
Figure 4.82: Comparison with Geometric Distribution for Pattern 6	107
Figure 4.83: Average Packet Delay Performance Comparison for Pattern 1	110
Figure 4.84: Delay Jitter Performance Comparison for Pattern 1	110
Figure 4.85: Average Packet Delay Performance Comparison for Pattern 2	112
Figure 4.86: Delay Jitter Performance Comparison for Pattern 2	112

List of Abbreviations

3G	Third Generation
4G	Fourth Generation
AAL	Ambient Assisted Living
ADC	Analog-to-Digital Converter
AP	Access Point
ASCII	American Standard Code for Information Interchange
CDF	Cumulative Distribution Function
ECG	Electrocardiogram
EMG	Electromyography
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communication
HRV	Heart Rate Variability
ICMP	Internet Control Message Protocol
IDC	International Data Corporation
IDE	Integrated Development Environment
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
ITS	Intelligent Transportation System
LAN	Local Area Network

LTE	Long-Term Evolution
M2M	Machine-to-Machine
MAC	Medium Access Control
MIMO	Multiple-Input Multiple-Output
MPEG TS	Moving Picture Expert Group Transport Stream
MTC	Machine-Type Communication
NS2	Network Simulator 2
OFDM	Orthogonal Frequency-Division Multiplexing
PC	Personal Computer
PCAP	Packet Capture
PDF	Probability Density Function
PHY	Physical
PMF	Probability Mass Function
PPM	Parts per Million
QoS	Quality of Service
RFID	Radio Frequency Identification
SRA	Strategic Research Agenda
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VLC	VideoLAN Client
Wi-Fi	Wireless Fidelity

WLAN Wireless Local Area Network

WSN Wireless Sensor Network

Chapter 1: Introduction

This chapter provides a general introduction to Internet of Things (IoT) and statistically shows future trends in this area. Current open issues associated with this innovation and its applications are also presented in this chapter. Finally, it briefly describes the research along with the thesis structure.

1.1 Overview

The Internet is an evolving entity that continues to grow in importance. The phrase “Internet of Things” was coined by Kevin Ashton in 1999 [1]. Recently, IoT has been eliciting increasing attention and rapidly gaining importance because of numerous technology advancements. Such advancements provide connectivity to anyone at any time and place to anything, thereby allowing the translation of the physical world into a digital cyber world with meaningful information.

The basic concept behind IoT is to allow the cooperation between the Internet and “things”. In IoT, the term “Things” refers to objects that are equipped with identification, sensing, actuation, storage, or processing capabilities. These smart objects can communicate and interact with one another over the Internet to accomplish certain goals, such as reducing costs and increasing optimization in any domain [2] [3].

IoT will drive the future of technology as various innovative and creative products will be designed. The US National Intelligence Council reported that Internet nodes are expected to be found in everyday items, including food packages, furniture, and paper documents, by 2025 [3].

Approximately 15 billion interconnected devices were estimated in 2015. This number is expected to grow rapidly to 24 billion by 2020 according to GSMA [4]. This increase will result in revenue opportunities of \$1.3 trillion for mobile network operators alone, which will span to vertical segments, including health, automotive, utilities, and consumer electronics. The International Data Corporation (IDC) forecasted that the worldwide IoT market will be worth \$1.7 trillion in 2020, i.e., up from \$655.8 billion in 2014, with a compound annual growth rate of 16.9 percent [5]. In the same year, devices alone are predicted to represent 31.8 percent of the total worldwide IoT market. This increased percentage in revenue is expected due to the building of IoT platforms, application software, and service-related offerings [5]. Figure 1.1 displays the projected market share of dominant IoT applications by 2020 [6].

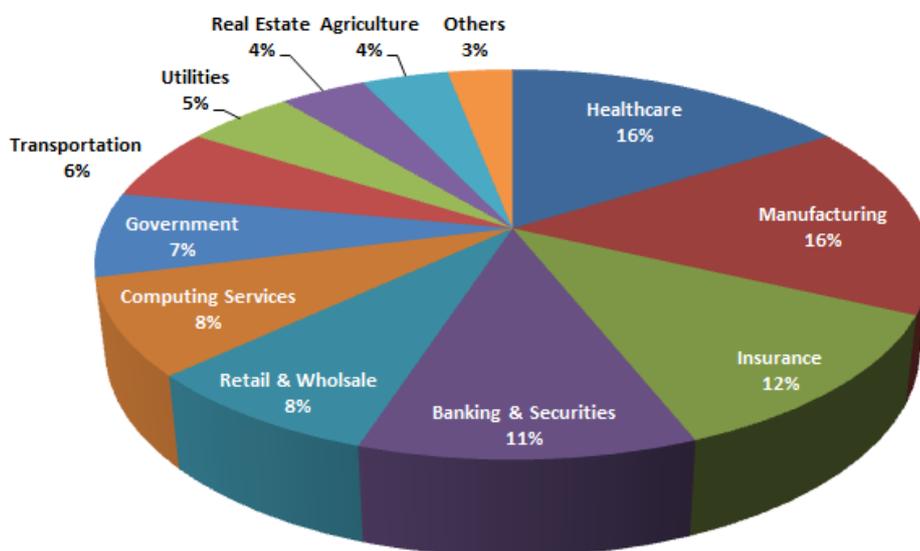


Figure 1.1: Projected Market Share of Dominant IoT Applications by 2020 [6]

1.2 IoT Challenges

Several challenges and open issues should be addressed and overcome for IoT to achieve its vision. These challenges include contextual, technical and applications ones, e.g., traffic characterization, privacy and security, quality of service (QoS), standards, interoperability, big data, and communication protocols.

1.2.1 Traffic Characterization

Traffic characterization represents a critical research issue that concerns networking aspects. This issue is attributed to several reasons. First, the characteristics of IoT traffic remain unknown [3]. Second, traffic patterns generated by an IoT network are expected to differ significantly from Internet traffic.

In a wireless sensor network (WSN), traffic characteristics are not considered a problem given that characteristics are application dependent and the focus is on the traffic flows inside a network. However, the situation is different in IoT because sensor nodes become parts of the overall Internet and are deployed for heterogeneous purposes. A huge amount of data will traverse the Internet, which will result in different traffic characteristics. Furthermore, large-scale and distributed radio frequency identification (RFID) systems have been recently deployed and their related traffic flows have not yet been studied [3].

Investigating the characteristics of IoT traffic is essential because these characteristics are highly involved in designing and planning network infrastructure and protocols [3].

1.2.2 Quality of Service

Heterogeneous networks provide more than one distinct applications or services (multi-services). This feature implies multiple traffic types within the network and the capability of a single network to support all applications without compromising QoS.

Applications generate either throughput- and delay-tolerant elastic traffic or bandwidth/delay sensitive inelastic (real-time) traffic, which can be further characterized according to data-related applications (e.g., high-resolution versus low-resolution videos) with different QoS requirements. Therefore, in addition to traffic modeling, a set of traffic requirements is necessary to provide appropriate solutions for supporting QoS.

QoS guarantees are not easily provided in wireless networks. Furthermore, dynamic scheduling and resource allocation algorithms based on particle swarm optimization are currently being developed [1].

1.2.3 Security and Privacy Challenges

Security is a serious and major concern in any network. An IoT system can be attacked by disabling network availability, pushing erroneous data into the network, or accessing personal information. A study conducted by HP indicates that 70 percent of common IoT devices are at risk of being attacked as a result of various vulnerabilities, such as insufficient authorization, inadequate software protection, and weak encrypted communication protocols.

RFID, WSN, and cloud may be parts of an IoT system that are vulnerable to such attacks. RFID appears to be the most vulnerable because it allows tracking individuals or objects but no high-level intelligence function is enabled in these devices [3].

Apart from security, privacy remains a problem that must be addressed, particularly in activities where privacy protection is required (e.g. transportation, personal activities, business processes, and information protection). Therefore, offering a design with authorization roles and policies is important to ensure that only authorized parties have access to sensitive data [7].

1.2.4 Big Data Analytics

A massive amount of information will be produced from various IoT applications. These data may include information from surrounding environments and user private data (e.g., health information), and thus, they will have non-uniform schemas and structures. To accurately analyze these diverse data formats, intelligent techniques and algorithms are required.

Deep learning algorithms can be adopted to efficiently analyze a huge amount of information generated by locally connected devices. User privacy should be respected in data analysis. Infrastructure for collecting, storing, and analyzing big data should be developed so that data anonymity should be provided for sensitive data [8] [5].

1.3 IoT Applications

IoT has considerable potential to influence and improve every aspect of everyday reality. As the Internet evolves and extends toward things, the concept of IoT has been demonstrated and involved in a variety of domains ranging from transportation and logistics, smart environment (e.g., home, office, and plant), healthcare to personal and social domains [9]. At present, only a few intelligent applications are deployed. Some important examples are briefly discussed in the following subsections.

1.3.1 Healthcare

The majority of IoT applications are implemented in the healthcare domain. Introducing smart things that are fitted with medical sensing will allow for remote monitoring and collection of various medical parameters. These collected data will be available over the Internet to doctors, family members, and other interested parties to improve the treatment and responsiveness of patients. In addition, IoT devices can be used to track objects and people (e.g., staff and patients) and to identify patients with a smart authentication system [10].

1.3.2 Smart City

A smart city refers to integrating digital technologies that include IoT into the overall key functionality of a city. IoT can be applied to energy management, traffic, healthcare, public transport, water supply, and waste management, to culture, public service, and governance. The goals are to increase resource effectiveness and sustainability, enhance livability, and improve public services.

1.4 Thesis Research

In the literature, many applications can be deployed in IoT networks. These applications will produce a huge amount of data. Therefore, an accurate traffic model is required in order to better design the network and the applications. In this thesis, we model the traffic generated by three common IoT applications, namely healthcare, smart cities, and video surveillance. The research is conducted based on realistic traffic traces with real- and non-real-time constraints. The data are wirelessly obtained from actual sensors and devices using Wireless Fidelity (Wi-Fi) technology. Using statistical approaches, we determine the best distribution to model packet inter-arrival time and provide some insights about packet size distribution. Also, we evaluate the impact of traffic models on the network performance using computer simulations. We show how the packet delay and delay jitter are significantly affected by the selection of the traffic model used especially when Poisson traffic is assumed.

1.5 Thesis Organization

The thesis is divided into five chapters. The first chapter provides an overview of IoT. Chapter 2 presents a relevant background review and discusses previous works done on the topic. The third chapter describes the system model. Chapter 4 introduces the results and discusses the major findings of the performed experiments. The last chapter concludes the study and states future directions of the research.

Chapter 2: Background and Related Works

This chapter discusses topics related to the thesis objectives. It starts with highlighting several IoT applications. The next section describes available IoT architectures. Finally, IoT traffic modeling is discussed along with the related works.

2.1 IoT Applications

IoT will play a vital role in numerous domains and its applications can be adopted to significantly enrich the quality of every aspect of daily life. IoT applications can be broadly classified into five areas [10], as described in Table 2.1.

Table 2.1: Applications Areas of IoT

Domain	Description	Applications
Smart Buildings	Related to a smart home by covering the provision of sensing and controlling the activities occurring at a user's house	Smart door, living room, cooling, washroom, and kitchen
Societal Issues	Related to a smart society by covering the effects of IoT and its solutions on society	Smart city, transportation, parking, healthcare, marketing, and similar social services
Environmental Monitoring	Related to a smart environment by covering the protection, monitoring, and development of natural resources	Smart water, ecosystem, disaster alert, and wildlife monitoring
Industry Applications	Focuses on technological aspects and related issues	Smart industry, security, and shopping
Emergency and Critical Situations	Deals with critical and global issues associated with the existence and persistence of human life	Handling natural calamities, water and radiation levels, toxic gas generation, ozone layer depletion, and enemy intrusion on borders

In 2010, the IoT Strategic Research Agenda (SRA) identified six or more application domains of IoT: smart energy, smart health, smart buildings, smart transport, smart living, and smart cities [11].

In 2012, a published ranking report identified 50 applications that can transform the real world into a smart world. These applications are classified into categories: smart cities, environment, water, metering, security, emergency response, retail, logistics, industrial control, agriculture, animal farming, home automation, education, and e-health [10]. Some IoT applications are briefly explained in the next sections.

2.1.1 Smart Cities

First, “smart cities” is used to define the emerging cyber-physical ecosystem that results from the deployment of advanced communication infrastructure and novel services over city-wide scenarios. The potential offered by IoT allows the optimization of the usage of physical city infrastructure and the quality of life of citizens by adding smartness to various city applications. These applications include monitoring the availability of parking spaces in a certain area, vibrations and material conditions of buildings and bridges, sensitive locations of cities, vehicles and pedestrian levels, intelligent and weather adaptive lighting of street lights, level of waste containers, smart roads and highways with warning messages and diversions according to climate conditions or unpredictable events (e.g., accidents or traffic jams). This type of IoT applications uses RFID, WSN, and sensors as IoT elements. The bandwidth of such applications ranges from small to large. Awarehome, Smart Santander, and City Sense are examples of smart cities that have developed IoT applications [2] [11].

2.1.2 Healthcare

Healthcare is one of the most rapidly expanding applications of IoT technology. IoT has the potential to give rise to many applications and services in the medical sector. Applications are further divided into two groups, namely, single- and clustered-condition applications (Figure 2.1). A single-condition application refers to a specific disease or infirmity, whereas a clustered-condition application deals with a number of diseases or conditions taken together as a whole. The previous classification is framed based on currently available healthcare solutions via IoT [12] [13].

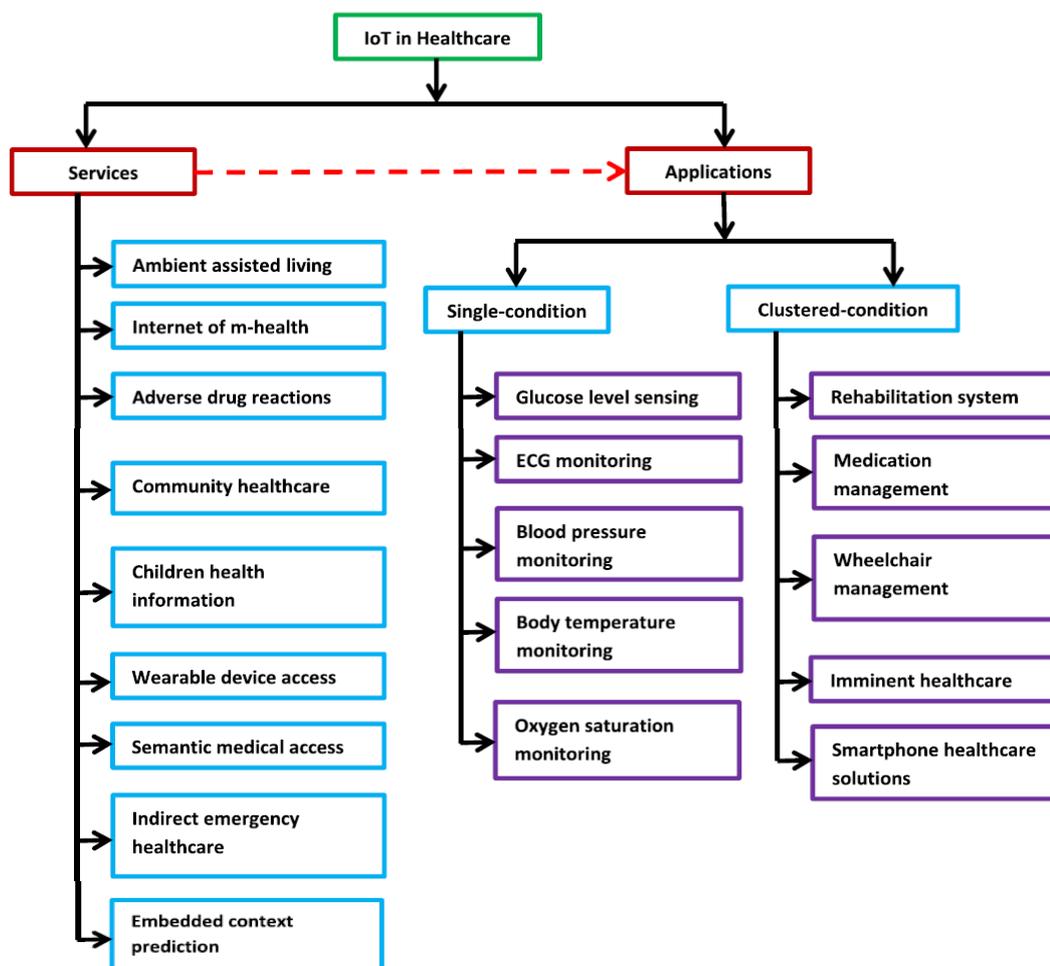


Figure 2.1: IoT Healthcare Services and Applications [13]

2.1.2.1 IoT-enabled Healthcare Services

IoT is expected to enable a variety of healthcare services in which each service provides a set of healthcare solutions. In the context of healthcare, no standard definition of IoT service is available. In [13], a service is by some means generic in nature and has the potential to be a building block for a set of solutions or applications. Examples of such services are briefly discussed in the following subsections [13].

2.1.2.1.1 Ambient Assisted Living (AAL)

AAL is known as an IoT platform powered by artificial intelligence that focuses on the healthcare of aging and incapacitated individuals. This service aims to conveniently and safely extend the independent life of the elderly in their place of living. In addition, AAL provides solutions to ensure autonomy and offer human servant-like assistance in case of any problem.

2.1.2.1.2 Indirect Emergency Healthcare

Indirect emergency healthcare is a service that offers a bundle of solutions, including information availability, alert notification, post-accident action, and record keeping, in case of emergency situations where healthcare issues are heavily involved, such as adverse weather conditions, transport (aircraft, ship, train, and vehicle) accidents, earthen site collapse, and fire.

2.1.2.2 IoT-based Healthcare Applications

In general, services are used to develop applications that are directly used by users and patients. Therefore, services are developer-centric, whereas applications are user-centric. Various IoT-based healthcare applications are discussed in the next subsections [13].

2.1.2.2.1 Glucose Level Sensing

Diabetes is a group of metabolic diseases that are characterized by high blood glucose levels over a long period. The monitoring of blood glucose shows individual patterns of blood glucose changes and helps in planning the meals, activities, and medication times of diabetics.

2.1.2.2.2 Electrocardiogram Monitoring

Electrocardiogram (ECG) is the register of the electrical activity of the heart via electrocardiography. It is used in simple heart rate measurement, basic rhythm determination, and the diagnosis of multifaceted arrhythmias, myocardial ischemia, and prolonged QT intervals. IoT-based ECG monitoring allows doctors to have patient's full medical information to immediately detect any critical event and take the corresponding appropriate action.

2.1.3 Security and Surveillance

Security and surveillance have become essential in enterprise buildings, shopping malls, factory floors, car parks, and other public places. IoT technologies can be used to improve the performance of current solutions by providing less expensive and less invasive alternatives to the widespread deployment of cameras while preserving user privacy. Examples of these technologies are as follows [11]:

1. Perimeter access control is used to detect and control the access of unauthorized people to restricted areas.
2. Liquid presence detection is used to detect liquid in data centers, warehouses, and sensitive building grounds to prevent breakdown and corrosion.
3. Radiation level and explosive detection is used to measure the radiation level in the surroundings of nuclear power stations to generate leakage alerts.
4. Hazardous gas detection is used to detect gas level and leakage in industrial environments, the surroundings of chemical factories, and interior mines.

The advantages in this market are in terms of enhanced functionality, increased user acceptance through the reduction of camera use, reduced operational costs, and increased flexibility in a changing environment [2].

2.1.4 Smart Business and Product Management

RFID technologies have already been adopted in many sectors for inventory management across the supply and delivery chain because of their capability to identify and provide support in tracking goods. RFIDs are typically used to monitor and manage product movement along the supply chain. Tags are directly attached to the items or to the containers that carry them while readers are placed throughout the facility for monitoring. IoT technologies can enhance flexibility in terms of reader positions and simultaneously enable seamless interoperability among RFID-based applications used by different actors dealing with a product throughout various phases of its life cycle.

In retail applications, IoT technologies can monitor real-time product availability and maintain accurate stock inventory. They can also play a role in after-market support, whereby users can automatically retrieve all data about the products they bought. In addition, identification technologies can help in limiting theft and counterfeiting by providing each product with a unique identifier, including a full description of the item. Furthermore, bio-sensor technologies in combination with RFID technology can control the production procedures, final quality, and possible shelf life deterioration of a product, such as in the food industry. For example, RFID devices can be used to identify and track a product, whereas bio-sensors can monitor parameters, such as temperature and bacterial composition, to guarantee the required quality of the final product [2].

Among various IoT applications, healthcare, smart cities, and video surveillance are selected to be deployed in the proposed system model.

2.2 IoT Architecture

Several IoT architectures have been proposed by different researchers. However, no single consensus on a unique architecture for IoT has been agreed upon universally.

A number of essential factors should be addressed when defining a new standard architecture for IoT, such as sustainability, scalability, interoperability, data storage reliability, and QoS. The main procedure of IoT is to connect between everything and everyone to enable information exchange, and thus, increase network traffic and storage capacity. Interoperability is considered a design issue due to the lack of an international standard for manufacturing devices. Moreover, a network may consist of billions of heterogeneous devices, which makes scalability another critical issue. The improvement of IoT relies on the advancement of the technology adopted in different useful applications and business models [14].

2.2.1 Three-layer Architecture

The well-known and most basic architecture consists of three layers: perception, network, and application. A set of functions, devices, and technologies are associated with each layer, as shown in Figure 2.2.

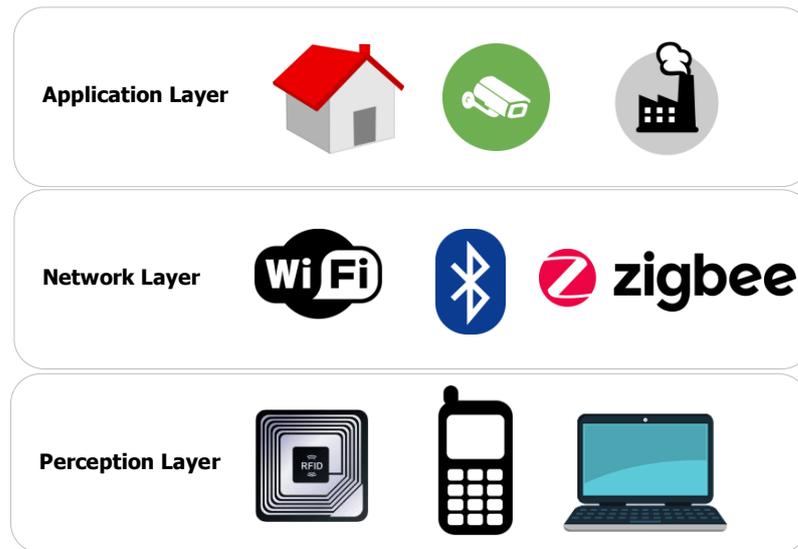


Figure 2.2: Three-layer Architecture of IoT

2.2.1.1 Perception Layer

As the bottom layer in the architecture, the perception layer is also known as the sensor or device layer. The main functions of this layer are to connect things to the network and then measure, collect, and process the information (e.g., humidity and temperature) associated with these things via deployed smart devices. Then, the processed information is transmitted to the upper layer via layer interfaces. The perception layer consists of RFID tags, sensors, cameras, 2D code tags, code readers, and Global Positioning System (GPS) units [15] [16] [17].

2.2.1.2 Network Layer

The network or transmission layer is implemented as the middle layer and considered the core of IoT architecture because different devices (e.g., hub, switch, gateway, and cloud computing platform) and different communication technologies (e.g., Bluetooth, Wi-Fi, and Long-Term Evolution (LTE)) are integrated into this layer.

The network layer is responsible for receiving the processed information obtained by the perception layer and determining the routes for transmitting data to the application layer [15].

2.2.1.3 Application Layer

On top of the stack is the application layer, which is responsible for the global management of the applications implemented by IoT. This layer receives the data transmitted from the network layer and uses them to deliver the required services or operations to the user. A set of applications exists in this layer, each having different requirements, such as smart grid, transportation, cities, homes, and healthcare [15].

2.2.2 Five-layer Architecture

The three-layer architecture has become insufficient due to the rapid development of IoT. Therefore, a five-layer architecture, which has additional middleware and business layers, has been proposed as illustrated in Figure 2.3.



Figure 2.3: Five-layer Architecture of IoT

2.2.2.1 Perception Layer

The role of the perception layer is still the same as that in the three-layer architecture, which is acquiring and processing data from the environment. Therefore, this layer consists of sensors and actuators that perform different functionalities, such as querying location, temperature, weight, motion, vibration, acceleration, wind speed, and amount of dust in the air [14].

2.2.2.2 Network Layer

The purpose of this layer is to securely transfer and maintain sensitive and confidential information from sensor devices. The movement is from the perception layer to the central information processing system (middleware layer).

The selection of the transmission medium (whether wired or wireless), along with the technology used, (e.g., third generation (3G), fourth generation (4G), Universal Mobile Telecommunications System (UMTS), Wi-Fi, Bluetooth, infrared, and ZigBee), is based on the type of sensor devices. Many protocols are found in this layer, such as Internet Protocol (IP) version 6, which is necessary to address the massive number of things [18].

2.2.2.3 Middleware Layer

The devices in an IoT system generate different types of service. Each device connects and communicates only with the devices that produce the same type of service. The middleware or processing layer has two essential functions: service management and storage of the lower-layer information in the database. Moreover, this layer can perform information processing and ubiquitous computation, and then automatically make a decision based on the computational results [14].

2.2.2.4 Application Layer

The application layer in the five-layer architecture is responsible for providing inclusive management of the application based on the processed information in the middleware layer. Numerous applications are implemented by IoT, such as smart home, healthcare, smart car, smart city, and intelligent transportation [14].

2.2.2.5 Business Layer

This layer, also known as the management layer, manages the overall IoT applications and services. The business layer is responsible for creating business models, flowcharts, executive reports, and graphs based on the data received from the application layer. Moreover, this layer helps determine future actions, business strategies, and roadmaps based on good result analysis [19].

The system model follows the three-layer architecture. However, with respect to the study's level, both architectures can be adopted.

2.3 Traffic Characterization

Traffic profiles can change unpredictably as packets travel along their routes; thus, traffic modeling aims to find stochastic processes that can represent the behavior of any network traffic. Traffic models need to accurately characterize actual traffic for the proper management and planning of the network to provide the desired QoS. Otherwise, overestimation or underestimation may affect the performance of the network and applications [20] [21] [22]. These models can be either source traffic models (e.g., video, data, or voice) or aggregated traffic models (e.g., backbone networks and the Internet).

Furthermore, one model cannot efficiently capture the traffic characteristics of all networks types under every situation. Thus, the selection of a traffic model depends on network type and the characteristics of the traffic on the network. More than one model can be used to characterize the same traffic. An ideal traffic model has to closely mimic reality and should be simple to use at the same time. A trade-off commonly occurs between simplicity and accuracy [20] [23] [24].

Network traffic can be modeled and expressed as a function of two random processes, namely, packet length and packet inter-arrival time, as presented in (1). Other parameters can be found in network traffic models (e.g., routes and distribution of destinations), but these parameters are less important [25] [26].

$$Z(t) = F(X(t), Y(t)) \quad (1)$$

where

$Z(t)$: Network traffic

$X(t)$: Packet length process

$Y(t)$: Packet inter-arrival time process

2.3.1 Probability Distribution

A probability distribution is a statistical function that describes the probability that a random variable is within a given range. This function is expressed through probability density function (PDF) and cumulative distribution function (CDF).

Old traffic models are based on simple probability distributions with the assumption that these models are correct in large aggregations, e.g., Poisson traffic distributions with exponential inter-arrival times. However, these models are not satisfactory because they do not exhibit bursts as real network traffic [26].

The following subsections describe some distributions that are commonly used to model packet length and packet inter-arrival time. These distributions are Exponential, Pareto, Weibull and Geometric.

2.3.1.1 Exponential Distribution

Exponential distribution is one of light-tailed distributions that are suitable for modeling network traffic with short-range dependence. This distribution is mathematically expressed through the PDF in (2) and the CDF in (3) [25].

$$P(x) = \frac{1}{\mu} e^{-x/\mu} \quad (2)$$

$$F(x) = 1 - e^{-\frac{x}{\mu}} \quad (3)$$

where $1/\mu$ is the only parameter for the distribution. It is called the rate and typically denoted as λ .

In machine-to-machine (M2M) traffic, the packet inter-arrival time of M2M devices (e.g., smart electrical meters, home security systems, sensor devices for the elderly, smart parking sensors, traffic sensors, and movie rental machines) is often modeled using Exponential distribution as in [27] and [28].

2.3.1.2 Pareto Distribution

Pareto distribution is one of the simplest heavy-tailed distributions and is the power law over its entire range. The PDF of this distribution is shown in (4). Furthermore, the CDF of Pareto distribution is given by (5) [25].

$$P(x) = \alpha k^\alpha x^{-\alpha-1} \quad (4)$$

$$F(x) = 1 - \left(\frac{k}{x}\right)^\alpha \quad (5)$$

where α is known as the shape parameter ($\alpha > 0$), and k is the local parameter ($k > 0$ and $x \geq k$).

2.3.1.3 Weibull Distribution

Weibull distribution is a heavy-tailed distribution. Its PDF is given by (6). In addition, its CDF is expressed using (7) [25].

$$P(x) = \frac{\alpha}{k} \left(\frac{x}{k}\right)^{\alpha-1} e^{-\left(\frac{x}{k}\right)^\alpha}, \quad x \geq 0 \quad (6)$$

$$F(x) = 1 - e^{-\left(\frac{x}{k}\right)^\alpha}, \quad x \geq 0 \quad (7)$$

where α is the shape parameter ($\alpha > 0$), and k is the local parameter ($k > 0$).

Heavy-tailed distributions, including Pareto and Weibull, are suitable for describing traffic with long-range dependence. Moreover, these two distributions have become the main distributions for describing stochastic processes in networks (time between packets and packet sizes) [25]. In [29], Pareto distribution is used to model the packet size in the system design for narrowband IoT system based on LTE. Furthermore, Weibull distribution can model the inter-arrival time at the packet level in Internet traffic [30].

2.3.1.4 Geometric Distribution

Geometric distribution is a discrete probability distribution. Its probability mass function (PMF) and CDF are mathematically expressed in (8) and (9), respectively.

$$P(x) = (1 - p)^x p, \quad x = 0, 1, 2, \dots ; \quad (8)$$

$$F(x) = 1 - (1 - p)^{x+1}, \quad x = 0, 1, 2, \dots ; \quad (9)$$

where p is the probability of success, and x is the number of failures before the first success.

The probability of success p is the only parameter for this distribution. It has a value between 0 and 1. In addition, the mean of a Geometric random variable X is

$$\mu = E(X) = \frac{1 - p}{p} \quad (10)$$

Moreover, Geometric distribution is a special case of the negative binomial distribution where the number of successes is equal to 1. In [27], this discrete distribution is used to model the packet size of data generated by group of sensors and aggregated at a M2M aggregator.

2.4 Related Works

The research on IoT traffic characterization (also referred as M2M traffic) is still in its infancy stages [31]. The work in [32] is considered among the first large-scale studies conducted to investigate whether there are new design and management challenges for cellular networks associated with M2M traffic. M2M traffic is compared with the traditional smartphone traffic using a set of different metrics, e.g., temporal variations, mobility, and network performance. This study recommends network operators to take into account the aforementioned parameters when managing networks [32].

The work in [31] characterizes IoT traffic for smart-campus environment. Traffic traces are collected from various IoT devices such as cameras, appliances, and health monitors. Then their data rates, burstiness, activity cycles, and signaling patterns are statistically characterized. Moreover, conventional approaches including the standard Poisson process are inadequate to model IoT traffic [33]. According to [34], the characteristics of aggregated periodic IoT data using Poisson process can introduce large errors depending on the performance metric of interest.

The Third Generation Partnership Project (3GPP) association suggests modeling the aggregated traffic generated by a large number of machine-type communication (MTC) devices, e.g. thousands of them connected via an LTE network, by either uniform distribution or Beta distribution [35]. The uniform distribution is meant to model the nominal non-synchronized case, while Beta distribution represents the extreme case when a huge number of devices try to access the network at the same time [35]. Furthermore, the authors in [36] propose a Coupled Markov Modulated Poisson Process model for capturing the behavior of source traffic generated by a single or a huge number of MTC devices. However, the models in [35] and [36] are different from our studied architecture where the traffic is first aggregated at gateways through different wireless technologies.

In [37], the authors propose a model for periodic uplink reporting for cellular IoT applications (e.g., smart utility metering reports of gas/water/electric consumptions, smart agriculture, and smart environment monitoring). In this model, each device is assigned a reporting period with Pareto distributed packet length [37]. Again, this model assumes direct communications between IoT devices and a cellular network and focuses only on smart city kind of applications.

The authors in [38] address one of IoT components used for medical and tracking applications. The distribution of ON and OFF periods in this network follows a generalized Pareto distribution [38]. The Weibull distribution is known to better model the inter-arrival times of Transmission Control Protocol (TCP) connection in Internet traffic [39].

To the best of our knowledge, no other work in the literature addresses the characterization of aggregated traffic of IoT gateways for three major applications, which are healthcare, smart city, and video surveillance with different scales of each application. Moreover, our work is based on real traffic data captured from realistic experimental setups that mimic the real-life scenarios.

Chapter 3: System Model

This chapter provides a detailed description of the proposed system model and explains the topology, components, and communication technologies involved in the suggested model. In addition, this chapter states the main assumptions considered while designing the system model.

The purpose of the proposed study is to model aggregated IoT traffic via packet inter-arrival time and packet size for widely used applications, such as healthcare, smart city, and video surveillance. Moreover, the study examines the impact of varying network load (i.e., number of sensor nodes) with different penetration ratios of the aforementioned applications (e.g., when the network is only used for sending healthcare, smart city, or video surveillance data) on the distribution of inter-arrival time and the impact of traffic models on network performance.

3.1 Proposed Study

The three-tier topology is followed in the system model. The model divides IoT into three layers: the perception, the network, and the application. In addition, the model targets the flow of data coming from the devices located in the perception layer and aggregated by an IoT gateway in the network layer. The study addresses aggregate traffic characterization at the gateway. The application layer is out of the scope of this research.

3.1.1 Perception Layer

The system model involves generating packet traffic based on a real IoT system. This step can be accomplished by deploying different types of devices and sensors that represent various IoT applications in the perception layer. Healthcare, smart city and video surveillance are examples of applications that can be implemented in this system. Furthermore, such applications can provide a mixture of traffic that is acquired in real-time and non-real time.

3.1.1.1 Healthcare Application

Healthcare is considered one of the most rapidly expanding IoT applications [40]. Therefore, a set of wearable sensors that are directly attached to the human body can be included in this model. These sensors can monitor patient's vital signs, e.g., ECG, electromyography (EMG), body temperature, and blood pressure.

To obtain accurate results from the sensors, the number of samples per second should be selected properly. In general, the highest frequency components of an EMG signal are approximately 400–500 Hz; thus, the sampling rate should be higher than twice the Nyquist rate (800–1000 Hz) to avoid aliasing and other distortions [41]. In case of ECG, the European Society of Cardiology and the North American Society of Pacing and Electrophysiology recommend using a sampling frequency between 250 Hz and 500 Hz or higher to measure heart rate variability (HRV) without any interpolation [42].

ECG and EMG are classified as life-critical medical data, and thus, ensuring that cardiac technicians, physicians, or cardiologists can view the acquired data immediately and interpret the received readings correctly is essential.

One way to avoid the late arrival of readings and discontinuity in the ECG or EMG graph is to send multiple measurements simultaneously, e.g., acquiring sufficient number of samples and then combining them into one packet. In this case, it is important that the used transmission protocols are capable of solving the problem of packet losses. A set of reliable User Datagram Protocol (UDP)-based transport protocols for IoT is discussed in [43].

3.1.1.2 Smart City Application

Many services can be offered by an IoT-based smart city, such as waste management, air quality monitoring, noise measurement, traffic congestion, health monitoring for buildings, and smart parking.

Our system model addresses common smart city applications, including weather conditions, such as temperature, relative humidity, atmospheric pressure, and light intensity. In addition, air quality monitoring is expected to be a typical application of smart cities given its close relation to the health and welfare of citizens. This monitoring can be achieved by using sensors that are responsible for measuring the concentration of non-contaminant and contaminant gases, such as carbon dioxide (CO₂), nitrogen dioxide (NO₂), carbon monoxide (CO), ozone (O₃), toluene (C₆H₅CH₃), hydrogen sulfide (H₂S), ethanol (CH₃CH₂OH), ammonia (NH₃), and hydrogen (H₂). An ultrasonic sensor is commonly found in smart cities. For example, such sensor is used in waste management service to control the waste level in dumpsters, and thus, ensure an effective waste collection mechanism.

3.1.1.3 Video Surveillance Application

Smart cameras are equipped with sensing, processing, and communication capabilities to provide real-time video acquisition and processing [44]. They are expected to play a vital role in several IoT applications. In a smart city, cameras can be used for traffic monitoring and for security purposes. The use of smart cameras in the healthcare domain allows for remote tracking of patient movements and behavior.

Furthermore, surveillance is considered an application that extensively uses such devices. In this application, cameras can track targets, identify suspicious activities, and monitor unauthorized access [1].

End-to-end delay is an important factor in video surveillance application. Usually, the tolerable delay is one second [45]. Therefore, the transmission protocol has to deliver the data without exceeding delay limits. Otherwise, the received packets are unusable and cannot be used further in decoding video frames.

3.1.2 Network Layer

Our system model follows the general consensus that traffic generated in IoT networks tends to be more uplink than downlink [46]. In this layer, a gateway can be deployed to collect the data coming from different IoT devices in the lower layer (perception layer) for further analysis. The gateway is directly connected to each sensor node over an IP network with a single-hop star topology, as illustrated in Figure 3.1. This design offers fast monitoring and response that are particularly required by healthcare devices, which may send critical information.

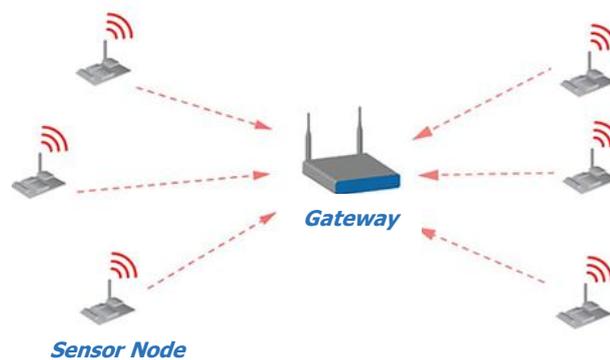


Figure 3.1: Single-Hop Star Topology

The size of the packets can either be variable or constant depending on the type of the device, the condition being monitored, and the type of collected data. Figure 3.2 shows an illustration of the proposed system model to study the characteristics of IoT traffic aggregated at the gateway and their impact on network performance. The captured data are transmitted over the air from the perception layer and aggregated by IoT gateways. The system can be implemented to emulate several real indoor and outdoor scenarios.

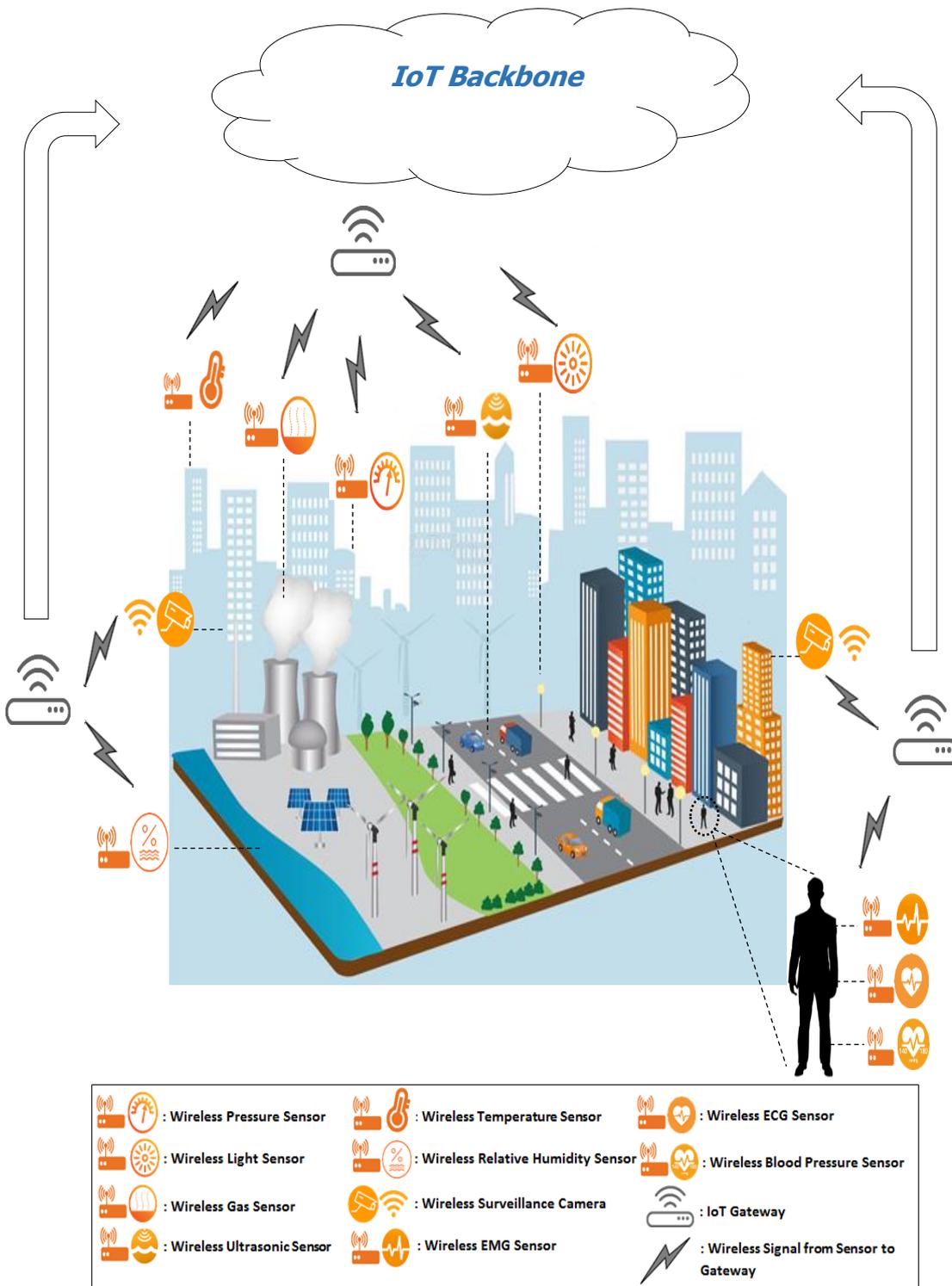


Figure 3.2: Proposed System Model

3.2 Communication Layers

The communication between IoT perception and network layers involves the following communication layers.

3.2.1 Physical Layer

The data obtained by the sensors are sent wirelessly as a stream of bits to the gateway in the physical layer. Any packet loss is assumed to be less than 1%. This is because we assume that the nodes are stationary; hence, the channel status does not change significantly.

3.2.2 Data Link Layer

In the data link layer, various communication technologies can be adopted to carry IoT data to a nearby or far gateway. Short- or wide-range network communication protocols can be selected (e.g., ZigBee, Bluetooth, Wi-Fi, Institute of Electrical and Electronics Engineers (IEEE) 802.11p, Global System for Mobile Communication (GSM), 3G, and LTE) depending on the application. Table 3.1 provides a set of specifications of the main communication protocols for realizing IoT-based smart cities.

Table 3.1: Communication Protocols for IoT-based Smart Cities [5]

Technology	Operating Frequency	Data Rate	Coverage	Applications
ZigBee	2.4 GHz, 868 MHz, 915 MHz	250 kb/s	50–100 m	Smart metering and indoor e-healthcare
Bluetooth	2.4 GHz	25 Mb/s	10 m	Indoor e-healthcare
Wi-Fi	2.4 GHz, 5 GHz, 802.11 n	54 Mb/s, 6 Gb/s	140 m, 100 m	Metering, waste management automation, energy management, infotainment, and automation
IEEE 802.11p	5.85–5.925 GHz	6 Mb/s	1000 m	Vehicular communication (vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I)) and infotainment
GSM/General Packet Radio Service (GPRS)	850, 900, 1800, 1900 MHz	80–384 kb/s	5–30 km	Intelligent transportation system (ITS), smart metering, mobile health, energy management, logistics, and infotainment
3G	850 MHz	3 Mb/s	5–30 km	ITS, smart metering, energy management, mobile health, logistics, and infotainment
LTE/LTE-Advanced	700, 750, 800, 1900, 2500 MHz	1 Gb/s, 500 Mb/s	5–30 km	ITS, smart metering, mobile health, logistics, and infotainment

All the technologies in Table 3.1 are considered suitable to implement the system model because the data rate of the deployed sensors is low.

The traffic characteristics of an IoT network using Wi-Fi technology with IEEE 802.11 standard are analyzed given that Wi-Fi is currently among the most widely used technologies and is common in various markets [47].

3.2.2.1 IEEE 802.11n

IEEE 802.11n is a popular and common standard that is supported by many devices. It is one of IEEE 802.11's wireless standards, which are developed by IEEE.

IEEE 802.11n defines a set of physical (PHY) and medium access control (MAC) layers specifications for wireless local area network (WLAN).

This standard is considered an extension of IEEE 802.11a/g, with a few modifications to the specifications of the PHY and MAC layers. These modifications have significantly improved range and reliability, and the overall throughput can now reach up to 600 Mbps for WLAN.

Orthogonal frequency-division multiplexing (OFDM) is the modulation technique used in this standard and also in previous ones. However, multiple-input multiple-output (MIMO) technology is added to the PHY layer. MIMO uses several transmitters and receivers to transmit up to four parallel data streams on the same transmission channel. At the MAC layer, frame aggregation and block acknowledgment mechanisms are introduced to maximize the efficiency of the layer [48].

To ensure backward compatibility with pre-existing 802.11a/b/g deployments, the standard can operate either in the 2.4 GHz or 5 GHz frequency bands. Table 3.2 shows the IEEE 802.11n PHY standards [49].

Table 3.2: IEEE 802.11n PHY Standards

Frequency Band (GHz)	2.4 or 5
Bandwidth (MHz)	20 or 40
Modulation	OFDM
Advanced Antenna Technologies	MIMO, up to 4 spatial streams
Maximum Data Rate (Mbps)	600

3.2.3 Transport Layer

The transport layer provides end-to-end message delivery and offers reliable connection-oriented or connectionless best-effort communication depending on the application.

3.2.3.1 Transmission Control Protocol

Unlike in the traditional Internet, the adaptation of the TCP as a transport layer protocol in IoT networks has more challenges and is inadequate due to the following reasons [3] [16]:

1. Connection setup

TCP is connection-oriented, and every session begins with a connection setup procedure (three-way handshake). A small amount of data is transmitted between objects; thus, this setup is unnecessary in IoT. During the connection setup phase, data are processed and transmitted by end terminals, which in most cases, have limited energy and communication resources, such as sensor nodes and RFID tags.

2. Congestion control

Congestion control is a challenge in the wireless medium, which is the medium of IoT systems. This control mechanism is not required because a small amount of information is exchanged among IoT devices.

3. Data buffering

This particular protocol requires storing data in a memory buffer at the source for retransmission in case any information is lost. Data should also be buffered at the destination to ensure an orderly delivery of data to the application. Managing such buffers is costly, particularly for battery-less devices, such as RFID tags.

3.2.3.2 User Datagram Protocol

UDP is a simple transport protocol that is built on top of IP. Unlike TCP, UDP is connectionless because this protocol does not require establishing a connection between the transmitter and the receiver. UDP has no mechanism to control flow, error, or congestion, and thus, no guarantee is provided that all the transmitted packets will reach their destinations without error and in order. The length of a UDP header is smaller compared with that of TCP.

UDP is suitable and preferable over TCP for real-time multimedia applications that require fast connections and low delay, such as video streaming. In the proposed model, the UDP is employed with the assumption that the network is not fully loaded to avoid congestion. In [43], three different reliable UDP-based transport protocols are evaluated for IoT applications.

Chapter 4: Results and Discussion

In this chapter, the input network traffic to an IoT gateway is characterized using real traffic data generated for three different IoT applications, namely, healthcare, smart cities, and video surveillance. First, the experimental setup including procedures, devices, and software tools used to collect the IoT data is described and explained in detail. After that, the experimental results in addition to the simulation findings are highlighted.

4.1 Experimental Setup

In order to mimic the system model, a laboratory-based experimental setup is prepared. Initially, a Wi-Fi network consists of 6 nodes is built. Each IoT-emulation node wirelessly sends a set of packet capture (pcap) files almost at the same time. This traffic is aggregated at the gateway as demonstrated in Figure 4.1. The gateway is configured to operate at 2.4 GHz with 20 MHz channel bandwidth.

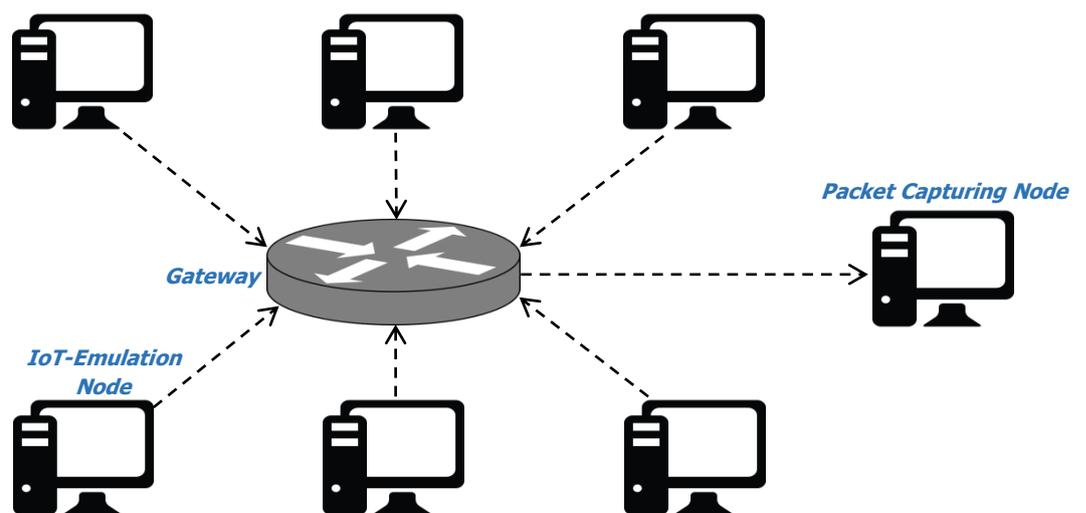


Figure 4.1: Experimental Setup Diagram

The network creates seven different scenarios that are likely to be seen in IoT networks serving the applications under study, namely, healthcare, smart cities, and video surveillance. For each scenario, the experiment is repeated at least 20 times for sufficiently accurate statistics. After that, the traffic load on the gateway is increased by increasing the number of nodes in steps of 3 until reaching 15 nodes.

Each one of these nodes replays a packet trace file that has been recorded by Wireshark (packet capture and protocol analyzer) software tool. Wireshark is used to capture these files in “pcap” format from real IoT systems for medical, smart cities, and video surveillance applications. In order for each node to replay a pcap file, a software tool named Bit-Twist is used. It is a powerful tool that is capable of regenerating any captured packets saved in a pcap file in order to be sent on a live network. Moreover, it comes with a trace file editor that allows modifying the contents of these pcap files [50].

The details of the experimental setups used to generate and capture the trace file for each application are described in the sequel. They have been set to generate a pcap file of five minutes duration. The trace files used in the experiment are all UDP-based traffic.

These experimental setups are implemented based on Waspnote version 1.5, and Intel Galileo Gen 1 boards.

Intel Galileo is a microcontroller board based on the Intel Quark system-on-a-chip X-1000 application processor. It is classified as the first board based on Intel architecture designed to be hardware pin-compatible with Arduino Uno R3 shields. To ensure the software compatibility, it can be programmed using Arduino Integrated Development Environment (IDE) [51].

Wasmote is an open source wireless sensor platform specially focused on the implementation of low power consumption sensor nodes to be completely autonomous and battery powered. Its architecture is modular based meaning that all the modules (e.g. radios and sensor boards) are plugged in through sockets. Wasmote Pro IDE is the software for writing and uploading codes to the board [52].

The data generated by Wasmote sensors are transmitted as ASCII characters encapsulated in UDP packets. The main advantage of ASCII frames is that their payload fields can be easily understood and interpreted. Figure 4.2 shows the structure of Wasmote ASCII frame.

Header									
<=>	<i>Frame Type</i>	<i>Num. Fields</i>	#	<i>Serial ID</i>	#	<i>Wasmote ID</i>	#	<i>Sequence</i>	#
Payload									
<i>Sensor_1</i>	#	<i>Sensor_2</i>	#	...			<i>Sensor_n</i>	#	

Figure 4.2: Wasmote ASCII Frame Structure

The data obtained from Intel Galileo board are also sent as ASCII characters in order to be consistent with Wasmote. The following subsections describe in detail the procedures, devices, and sensors involved in IoT data collection.

4.1.1 Healthcare Traffic

e-Health sensor shield version 2.0 is manufactured by Cooking Hacks [53]. It is designed to gather various medical data for research and testing purposes. It is compatible with Raspberry Pi, Arduino, and Intel Galileo boards.

There are ten sensors can be connected to the shield for obtaining different biometric parameters including pulse and oxygen in blood, airflow, body temperature, ECG, glucose, galvanic skin response, blood pressure, body position, and EMG. These measurements can be used either to monitor patients' state in real-time or to send critical data for further analysis. Furthermore, they can be wirelessly transmitted using various connectivity technologies including Wi-Fi, 3G, GPRS, Bluetooth, 802.15.4, or ZigBee depending on the application [53].

In the experiment, three medical sensors are selected to generate the medical traffic; ECG, EMG, and blood pressure sensors. ECG and EMG sensors provide real-time measurements while the blood pressure device only retrieves the stored readings. Moreover, the shield is placed over Intel Galileo Gen 1 board.

4.1.1.1 ECG Sensor

The ECG sensor is an analog sensor that returns a value from 0 to 5 V to represent the ECG waveform. It is used to study the heart's electrical and muscular functions. The accuracy of this sensor depends on the condition being tested. Moreover, it is commonly used to detect or measure the following:

1. Heart's orientation in the chest cavity.
2. Heart's underlying rate and rhythm mechanism.
3. Any damage in the heart muscle.
4. An increase in thickness of the heart muscle.
5. Insignificant impaired blood flow to the heart muscle.
6. Abnormal electric activity that may lead to abnormal cardiac rhythm disturbances.

It consists of three leads; positive, negative, and neutral [54]. They are connected to the e-health shield from one side and to the electrodes from the other side. In experiment, the electrodes are attached to normal person with no heart issues as illustrated in Figure 4.3.

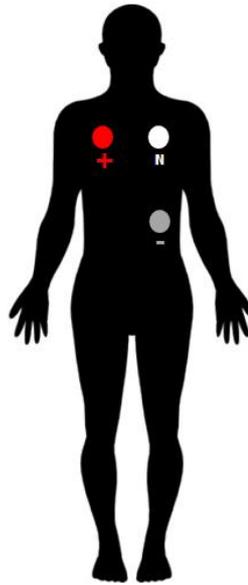


Figure 4.3: ECG Sensor Placement

The Intel Galileo board is programmed such that it reads from the sensor with a sampling rate of 2000 Hz. Then it sends a UDP packet with 500 samples to ensure that there are adequate measurements for technicians or doctors to interpret meanwhile the next sample is being transmitted. As mention in Chapter 3, the sampling rate is chosen according to the recommendations of the European Society of Cardiology and North American society of Pacing and Electrophysiology [42].

A local area network (LAN) is set up in order to wirelessly transfer the ECG signal in UDP packets from the Galileo board to a personal computer (PC). Two ASUS RT-N66U dual-band wireless-N900 gigabit routers are used. One of them is configured as a 2.4 GHz router in legacy mode.

Since the Intel Galileo board has only wired interface and we are interested to emulate the case of wirelessly sending data from IoT sensors, the other router is configured as media bridge mode. This mode grants Wi-Fi connectivity to the devices, which are not equipped with Wi-Fi interface as illustrated in Figure 4.4.



Figure 4.4: Media Bridge Mode

As depicted in Figure 4.5, the packets are sent through the Ethernet cable from the Galileo board to the media bridge router that wirelessly forwards them to the PC through the access point (AP), which is implemented using ASUS RT-N66U router.

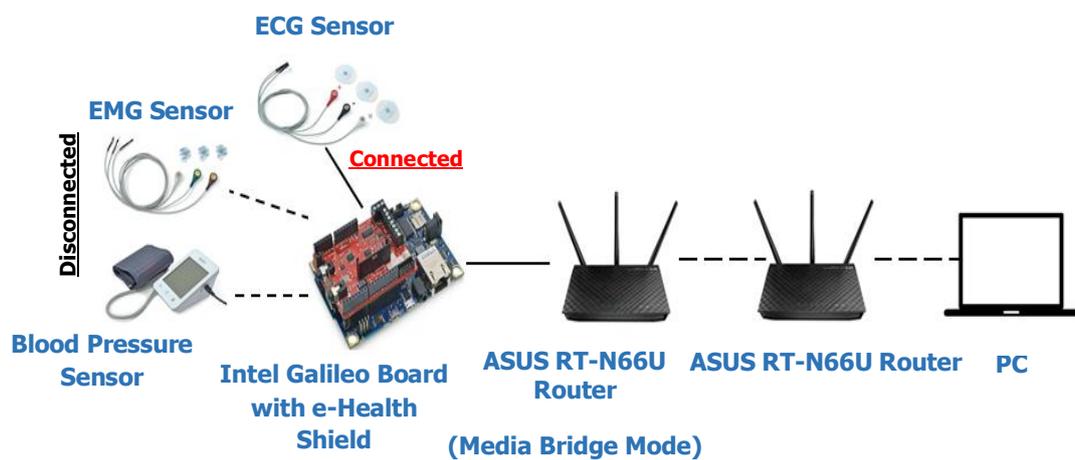


Figure 4.5: LAN for ECG Measuring System

Wireshark is running in the PC to capture the traffic in the LAN for duration of five minutes. The total number of packets received during the experiment time is 982. The size of each packet varies from 923 to 950 bytes as a result of sending 500 readings as characters in one packet and evaluating the heart's activity of a person with no heart disease.

Furthermore, we do not anticipate any difference in the packet sizes with persons with heart diseases since mostly heartbeat frequency changes. Figure 4.6 shows a plot of the ECG signal using the captured ECG values received in the first 9 seconds.

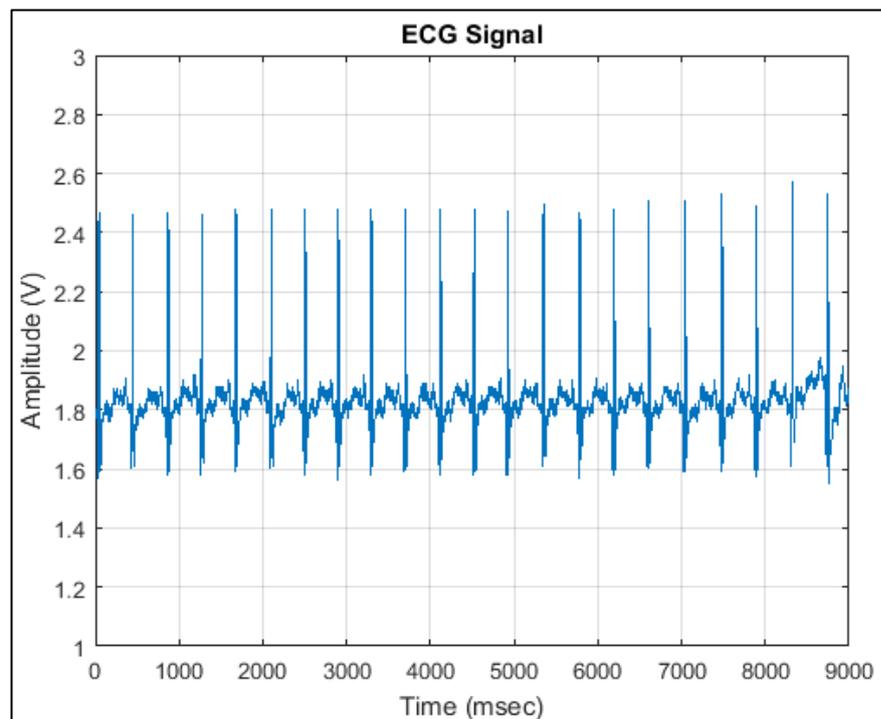


Figure 4.6: ECG Waveform

4.1.1.2 EMG Sensor

EMG is a biomedical signal obtained from the electrical response produced in muscles during its contraction/relaxation representing neuromuscular activities [41]. This signal helps in identifying neuromuscular diseases as well as assessing low-back pain. Also, it can be considered as a control signal for prosthetic devices (e.g., prosthetic hands, arm, and lower limbs) [54].

This particular sensor measures the filtered and rectified electrical activity of a muscle. It returns an integer value in V and the e-health shield takes the readings directly from the analog-to-digital converter (ADC). The value of these readings is in the range from 0 to 1023. Moreover, it is made of three leads, which are named as M, E, and GND. The sensor's leads are placed using pre-gelled electrodes as illustrated in Figure 4.7.

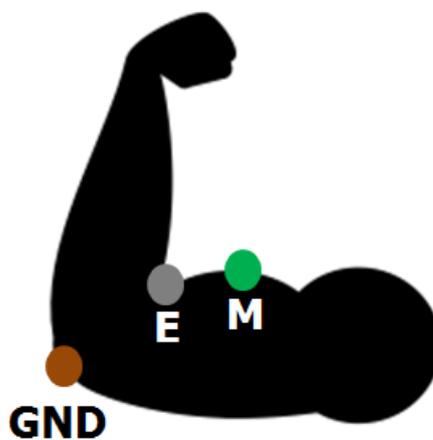


Figure 4.7: EMG Sensor Placement

The same setup in Figure 4.5 is used for obtaining EMG traffic. The only difference is that the ECG sensor is replaced by the EMG sensor. The Intel Galileo board is programmed to take a reading from the sensor every 0.2 millisecond which is equivalent to use 5000 Hz sampling rate. As mentioned in Chapter 3, the EMG signal should be sampled at rate that satisfies Nyquist criterion in order to avoid aliasing [41]. Moreover, 100 EMG readings are placed in one UDP packet to ensure that there are sufficient amount of measurements offered to the receiver to interpret and play smoothly time-varying EMG graph. This is necessary to correctly analyze the graph and immediately detect any critical condition.

The received EMG traffic is captured for five minutes. During this time period, 994 packets are received with 10 different packet sizes. The minimum size is 1042 bytes while the maximum size reaches 1066 bytes. This range of packet length is due to writing 100 readings as characters over the same packet in addition to the muscle activity during the capture time. Moreover, a plot of the EMG waveform is presented in Figure 4.8; the vertical axis in the graph represents the output of the ADC.

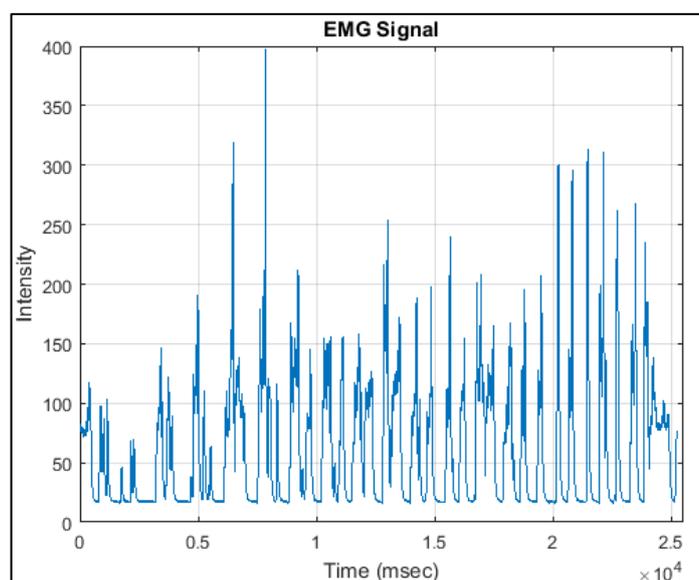


Figure 4.8: EMG Waveform

4.1.1.3 Blood Pressure Sensor

Blood pressure is defined as the pressure exerted by the blood in the blood vessels as it is pumped around the body by the heart. It is expressed as two numbers; the systolic pressure (as the heart beats) over the diastolic pressure (as the heart relaxes between beats). Monitoring this pressure is crucial for many people especially for those with high blood pressure [54].

The sensor provides automatic measurements of systolic, diastolic, and pulse with time and date information. When it is connected to the microcontroller, it only sends the history stored in the device's memory that can save up to 80 measurements. This means that the provided data are in a non-real-time fashion.

The LAN with the same configuration as in the case of EMG and ECG is used (Figure 4.5). The only difference is that one UDP packet is sent every 20 seconds and each contains 7 readings. The number of readings is selected such that the packet length of blood pressure is in the same range of other medical sensors.

During five minutes, 15 packets are received and captured by Wireshark. They have a fixed size, which is 939 bytes. This is because all contain identical readings.

4.1.2 Smart Cities Traffic

To create a real traffic that represents smart cities application in the experiment, Waspote gases version 3.0 board in addition to smart cities pro board are used. They are both manufactured by Libelium and compatible with Waspote version 1.5 [55] [56].

4.1.2.1 Gases Sensors

Waspote gases board enables the user to monitor various environmental parameters including temperature, humidity, and atmospheric pressure in addition to fourteen other gases [56].

Four gases sensors which are CO₂, NO₂, CO, and air pollutants II are connected to the board's sockets two, three, four, and six, respectively as in Figure 4.9. The experiment held in an indoor location with normal air concentration. Every one second, a reading is obtained from each sensor in parts per million (ppm) [57]. These values are saved in one UDP packet with certain format as in Table 4.1.

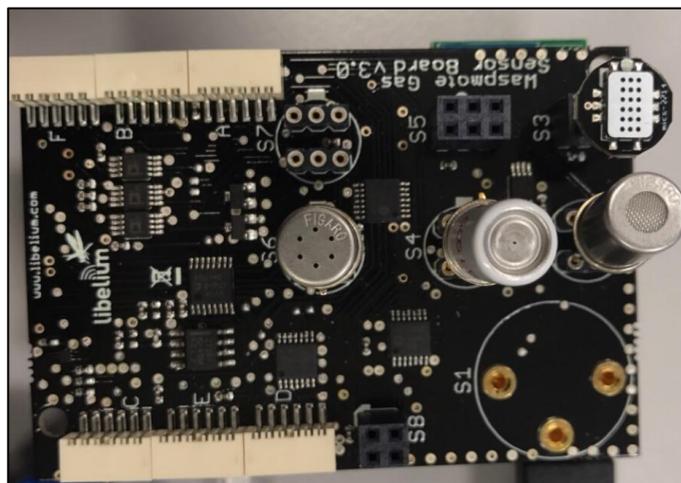


Figure 4.9: Waspote Gases Board

Table 4.1: Gases Sensors Format [58]

Sensor	Sensor ID	Number of Fields	Default Decimal Precision
CO	CO	1	3
CO ₂	CO2	1	3
NO ₂	NO2	1	3
Air Pollutants 2	AP2	1	3

Wasmote Wi-Fi module is connected to the Wasmote's socket zero to wirelessly transfer the packets to the PC through a gateway for five minutes.

In five minutes, 53 packets are received to the PC. This number is due to the network delays. The size of these packets is from 122 to 125 bytes. This variation in the size is because two of the header fields which are Wasmote ID and Frame Sequence have a variable size, from 0 to 16 bytes for Wasmote ID and from 1 to 3 bytes for Frame Sequence [58]. Moreover, the default maximum frame size is 255 bytes per frame [58].

4.1.2.2 Smart Cities Sensors

Wasmote smart cities pro board is designed to extend the monitoring functionalities from indoor environments to outdoor. Nine sensors can be connected simultaneously to the board [55].

Temperature, humidity, and pressure sensor is placed in the first socket of the board. It is a digital sensor that measures temperature in °C, relative humidity in percentage, and atmospheric pressure in Pa. Also, ultrasound (proximity) sensor is added by connecting it to the board's socket two. The purpose of such sensor is to determine the distance to an object in cm. The board is tested in an indoor location because the usage of the ultrasound sensor is in indoor only [55]. The readings are taken from both sensors with a sample rate of 40 Hz which is the maximum sampling rate that the ultrasound sensor can work with [59]. This rate is selected in order to count for the worst-case scenario of network loading. During five minutes, the UDP packets generated by the Wasmote board are sent wirelessly to the PC through a gateway as illustrated in Figure 4.10. Furthermore, Table 4.2 shows how the data for each sensor are represented in the frame.



Figure 4.10: LAN for Smart Cities Sensors

Table 4.2: Smart Cities Sensors Format [58]

Sensor	Sensor ID	Number of Fields	Default Decimal Precision
Temperature	TC	1	2
Humidity	HUM	1	1
Pressure Atmospheric	PRES	1	2
Ultrasound	US	1	0

The length of these packets varies from 113 to 115 bytes as there are two fields in the frame header have a variable size.

4.1.2.3 Light Sensor

Light sensor is a resistive sensor whose resistance depends on the intensity of the light received on its photosensitive part. It is connected in series with 10 k Ω resistor as illustrated in Figure 4.11. As the sensor changes its resistive value due to the light intensity, the output voltage can be determined using voltage divider as in (11).

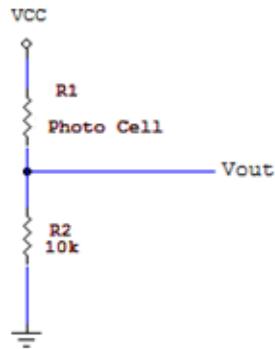


Figure 4.11: Light Sensor Circuit Diagram

$$V_{out} = V_{cc} \times \frac{R_1}{R_1 + R_2} \quad (11)$$

This luminosity sensor is connected to the Wasp mote as indicated in Figure 4.12. For five minutes, one sample is taken from the sensor approximately every second. Then it is wirelessly transmitted to the PC. In transmitted UDP packets, the luminosity value is expressed as a percentage.

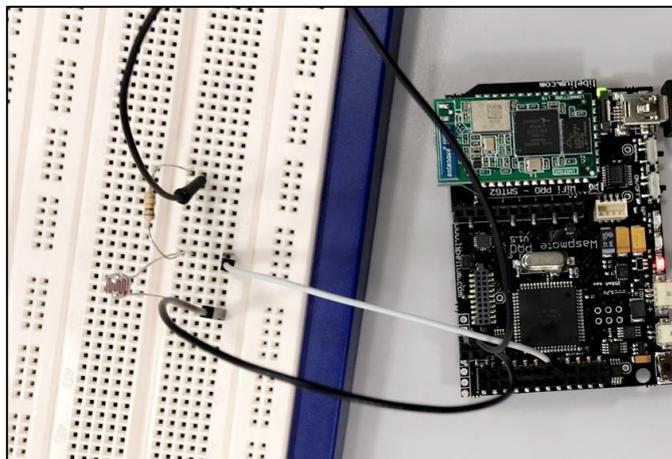


Figure 4.12: Light Sensor Connection

Due to the delays in the network, 218 packets are received by the PC during the capture time (five minutes). Although the size of Wasp mote ID and Frame Sequence in the header is variable, the variation in the packet size is fairly limited (76-77 bytes).

4.1.3 Video Surveillance Traffic

The video surveillance experiment is performed by a network camera of DCS-930L manufactured by D-Link, which can generate a live streaming video (real-time traffic). This camera supports different networking protocols such as TCP, UDP, Internet Control Message Protocol (ICMP), and File Transfer Protocol (FTP) client [60].

A WLAN that consists of ASUS RT-N66U router, smart phone (or PC), and DCS-930L camera is constructed as in Figure 4.13.



Figure 4.13: WLAN for Video Streaming

The camera is configured to send UDP live video streaming using VideoLAN Client (VLC) media player. Figure 4.14 shows the streaming and gives an example of the video's quality.

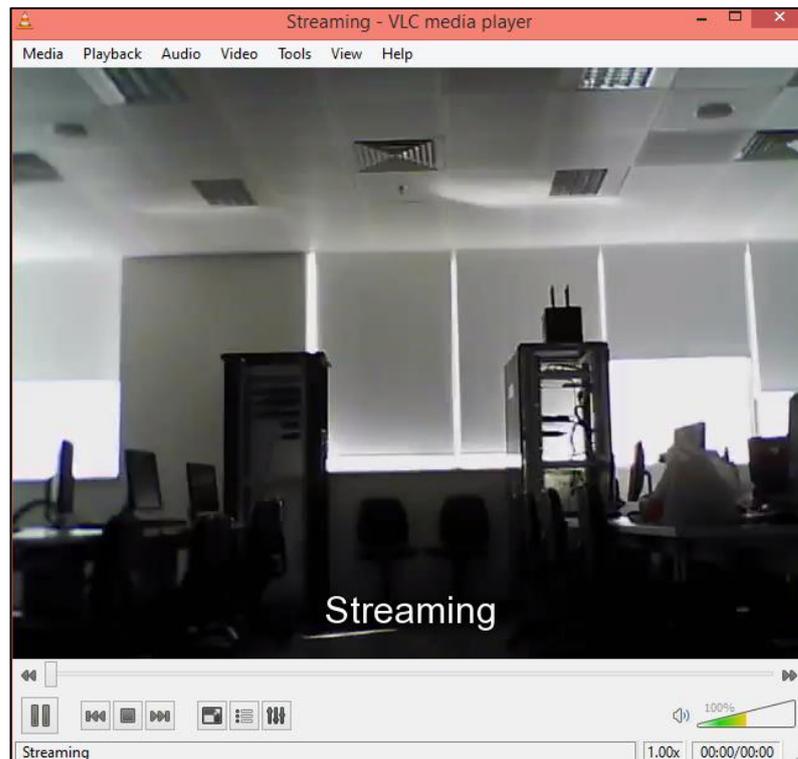


Figure 4.14: Streaming Process

The traffic sent from the surveillance camera to the phone for duration of five minutes is captured. The number of the received packets is 5461. They are all in Moving Picture Expert Group Transport Stream (MPEG TS) format with fixed size (1358 bytes).

4.2 Experimental Results

4.2.1 IoT Packet Inter-arrival Time Distribution

As mentioned before, seven different traffic patterns are observed for each network load. For each pattern, the packet inter-arrival time is recorded and its empirical distribution is obtained.

We are particularly interested in checking the suitability of common distributions that are used in the literature to characterize aggregates traffic at IoT gateways. These three distributions are Exponential, Weibull, and Pareto. By Pareto, we refer to generalized Pareto distribution. These particular distributions are selected since they are commonly used to model the packet inter-arrival time in Internet and M2M [30] [27].

In order to statistically determine which one of the above mentioned distributions fits the IoT gateway packet inter-arrival time, we first followed the statistical approach of applying the three commonly used, goodness-of-fit tests, namely, Kolmogorov-Smirnov, Anderson-Darling, and Chi-Squared. Generally, a goodness-of-fit test compares between the empirical data and the theoretical (fitted) values of the probability distribution. The results of this test either accept or reject one of the following hypotheses [61]:

1. The null hypothesis (H_0), which states that the empirical samples follow a given distribution.
2. The alternative hypothesis (H_1), which claims the opposite of H_0 .

Kolmogorov-Smirnov test is the most popular goodness-of-fit test [62]. The test statistic (D) represents the maximum difference between the CDF of the empirical and the suggested distribution. It is mathematically expressed through (12) [62].

$$D = \sup |F_0(x) - F_{Data}(x)| \quad (12)$$

where $F_0(x)$ is the CDF of the hypothesized distribution, whereas $F_{Data}(x)$ represents the empirical CDF.

Anderson-Darling is another hypothesis test. It is sensitive to the discrepancies in the tails of the distribution. Its statistic test (A^2) is computed according to (13) [25].

$$A^2 = -n - \frac{1}{n} \sum_{i=1}^n (2i - 1) \cdot [\ln F(X_i) + \ln(1 - F(X_{n-i+1}))] \quad (13)$$

where n represents the sample size. $F(X)$ is the CDF for the specified distribution and i refers to i^{th} sample when sorting the data in ascending order.

Chi-Squared is a simple test as expressed as in (14) [25]. This test requires an adequate sample size.

$$\chi^2 = \sum_{i=1}^k \frac{(O_i - E_i)^2}{E_i} \quad (14)$$

where O_i is the observed frequency for bin i . E_i represents the expected frequency for bin i and it is calculated as follows [25]:

$$E_i = F(x_2) - F(x_1) \quad (15)$$

where F is the CDF of the tested probability distribution and x_1, x_2 represent the limits for bin i .

Unfortunately, the results from performing the above standard tests on the packet inter-arrival time data reveal a rejection of the null hypothesis for all the seven patterns for all tests except of the Chi-Squared test, which gave unreliable results.

Therefore, another statistical approach is adopted. It is based on computing the mean and the standard deviation of the absolute distance between the empirical CDF and the CDF of each suggested probability distribution as expressed in (16).

$$AD = |F_E(x) - F_F(x)| \quad (16)$$

where AD is the absolute distribution distance. $F_E(x)$ represents the empirical CDF, whereas $F_F(x)$ is the fitted CDF.

The empirical distribution is then matched to the distribution with the lowest absolute distribution distance parameters. These parameters are the average and the standard deviation.

4.2.1.1 Traffic Pattern 1: Equal Percentage of the Three Applications

In the first pattern, the network load is equally shared among the three categories such that one third of the load is sending data related to the healthcare, the other third is sending the packets of smart cities application, and the last third is replaying camera's captures.

Figures 4.15, 4.16, 4.17, and 4.18 show the empirical CDF when the load is 6, 9, 12, and 15, respectively. At the same time, these figures show the fitted CDF of the Exponential, Weibull, and Pareto distributions. It can be noticed that as the load increases, the empirical CDF becomes closer in shape to the three distributions.

The inter-arrival time is recorded in millisecond. In addition, each of the fitted distributions has its own parameters. Exponential distribution has only one parameter which is the mean. The parameters of Pareto distribution are scale, shape and threshold. While Weibull distribution is defined via scale and shape. Tables 4.3, 4.4, 4.5, and 4.6 display the parameters of the three distributions used in the fitting tests for 6, 9, 12, and 15 nodes, respectively.

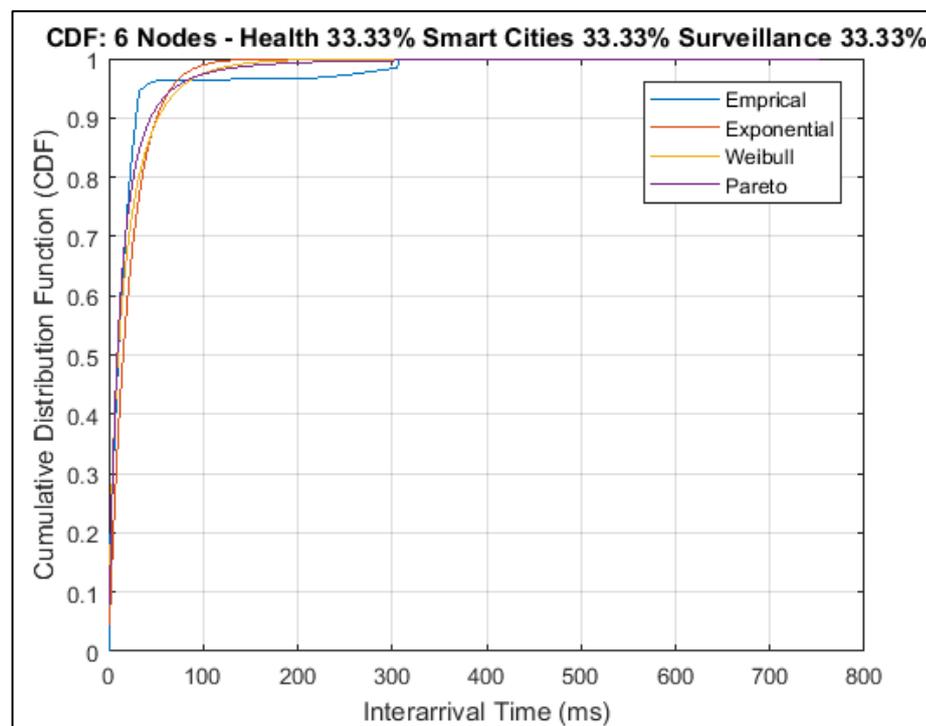


Figure 4.15: CDF of Inter-arrival Time for Pattern 1 & 6 Nodes

Table 4.3: Distributions' Parameters for Pattern 1 & 6 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	22.02	0.4358	11.1960	0	16.6420	0.7264

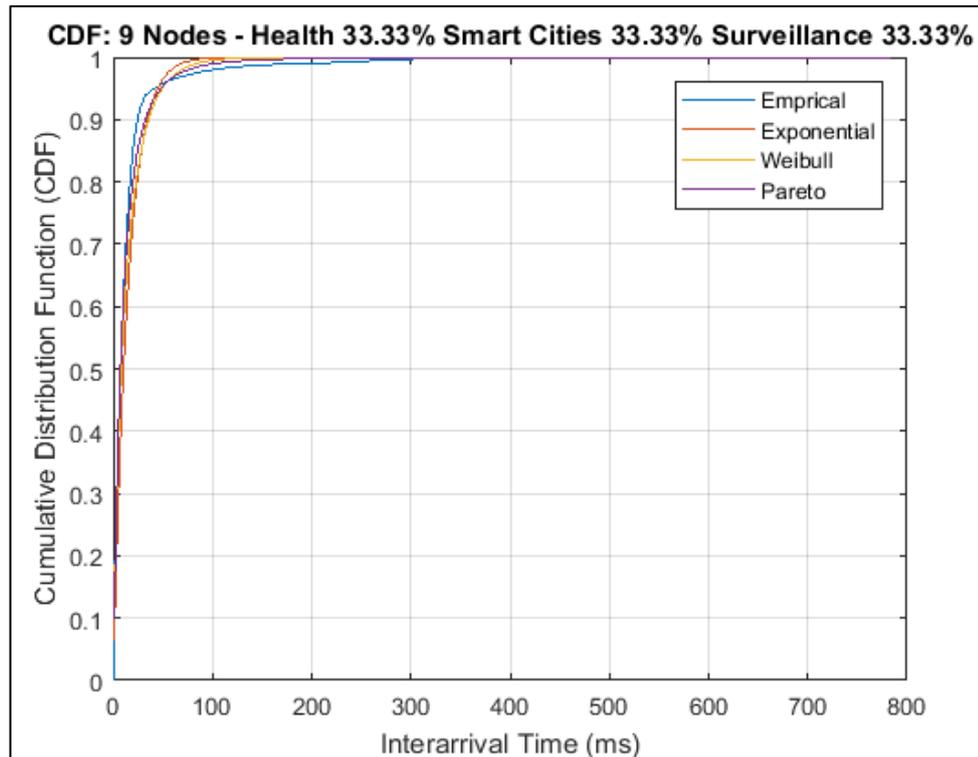


Figure 4.16: CDF of Inter-arrival Time for Pattern 1 & 9 Nodes

Table 4.4: Distributions' Parameters for Pattern 1 & 9 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	14.9250	0.3420	9.2182	0	12.7384	0.8082

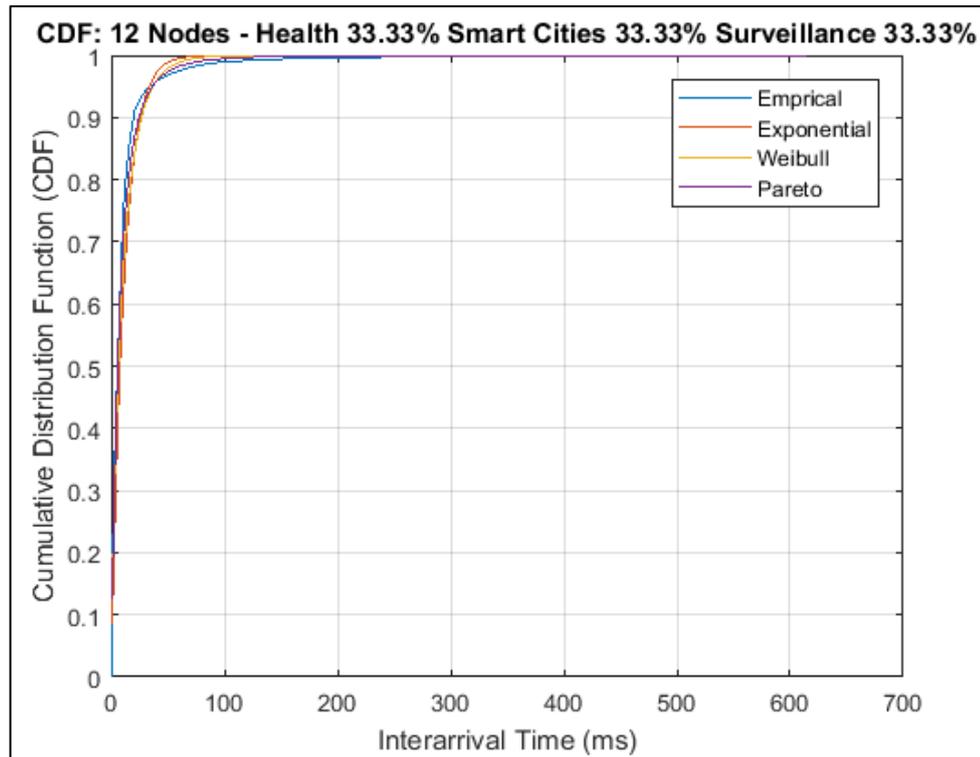


Figure 4.17: CDF of Inter-arrival Time for Pattern 1 & 12 Nodes

Table 4.5: Distributions' Parameters for Pattern 1 & 12 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	11.2309	0.3257	7.1971	0	9.8103	0.8275

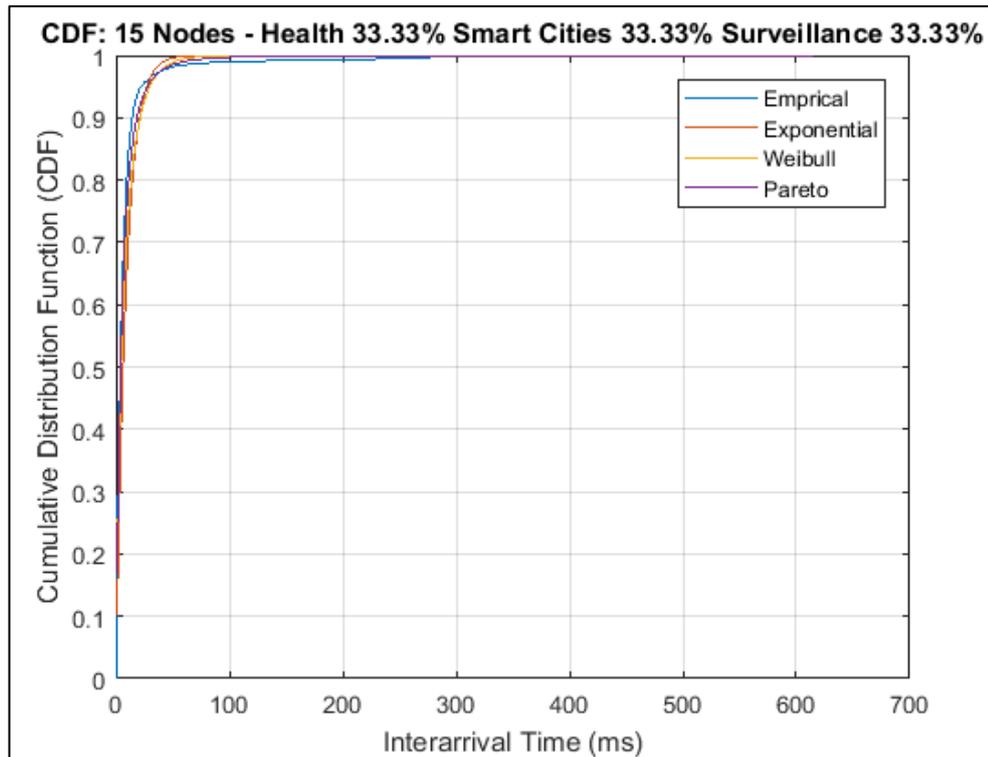


Figure 4.18: CDF of Inter-arrival Time for Pattern 1 & 15 Nodes

Table 4.6: Distributions' Parameters for Pattern 1 & 15 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	9.0828	0.3501	5.2356	0	7.3919	0.7852

When comparing the empirical CDF to the CDF of the expected distributions, it is found that Pareto achieves the minimum average as well as the minimum standard deviation of the absolute distribution distance among the other distributions as indicated in Figure 4.19. We infer that Pareto distribution is the best candidate to describe this scenario for 6 Nodes.

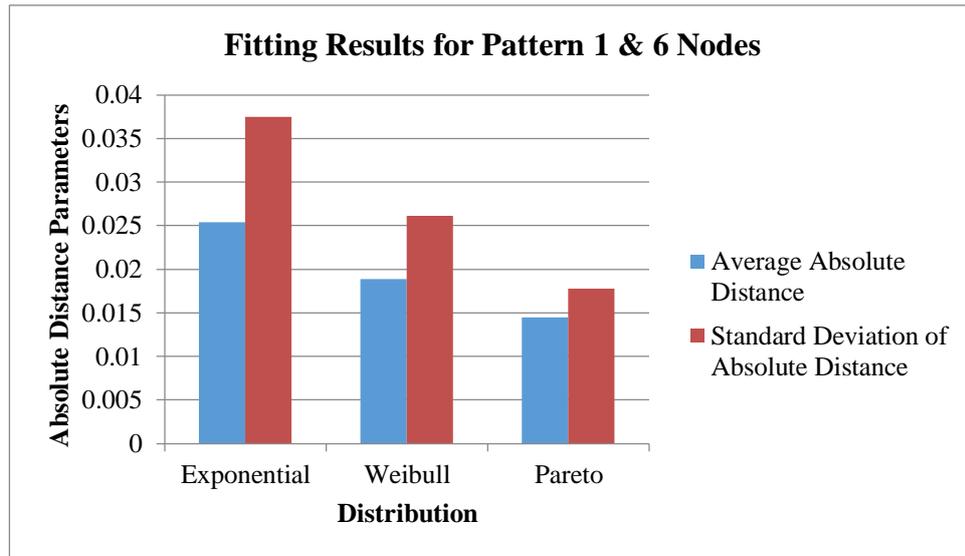


Figure 4.19: Distribution Fitting Results for Pattern 1 & 6 Nodes

In order to check the effect of the gateway load on the distribution, the gateway load is increased gradually from 9 to 15 nodes for the same traffic pattern. Apparently, the lowest average absolute distribution distance and the standard deviation are still found to be for Pareto distribution as shown in Figures 4.20, 4.21, and 4.22.

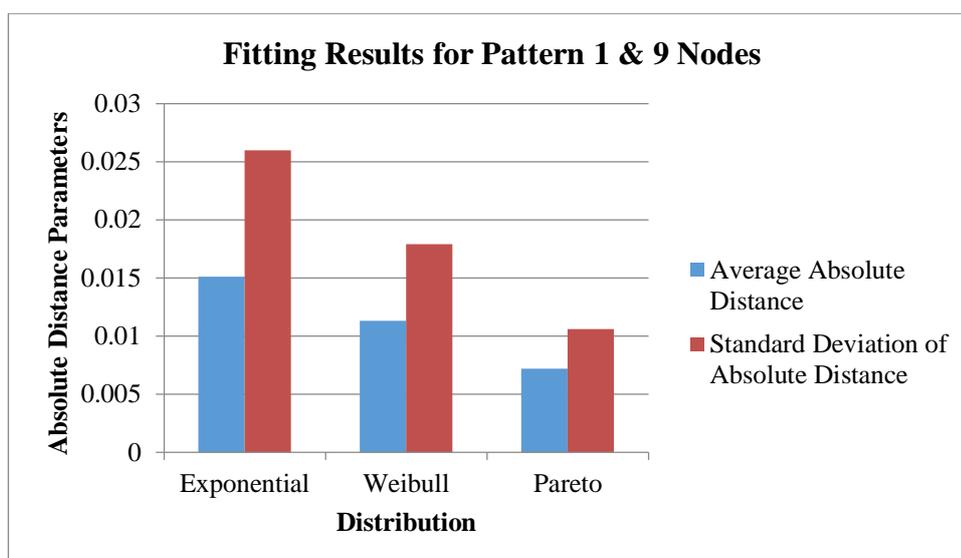


Figure 4.20: Distribution Fitting Results for Pattern 1 & 9 Nodes

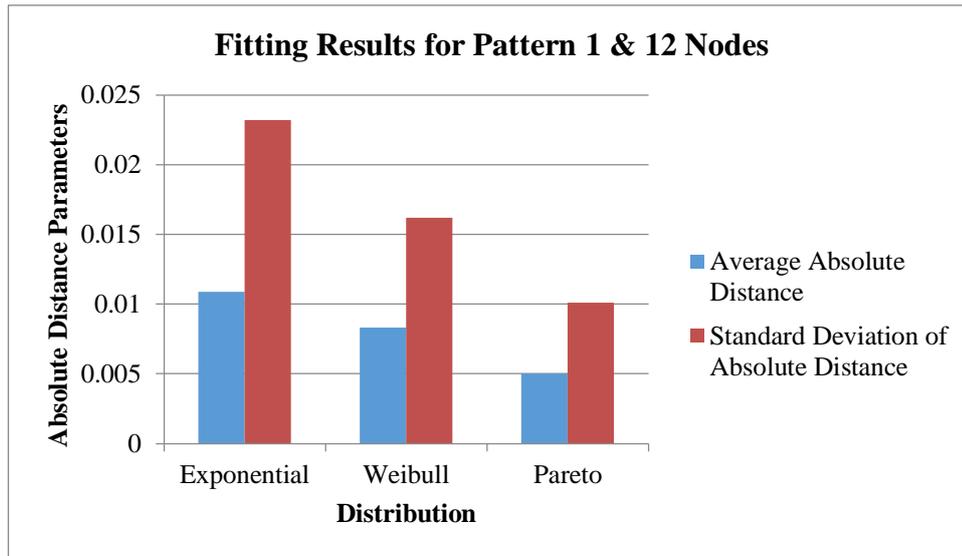


Figure 4.21: Distribution Fitting Results for Pattern 1 & 12 Nodes

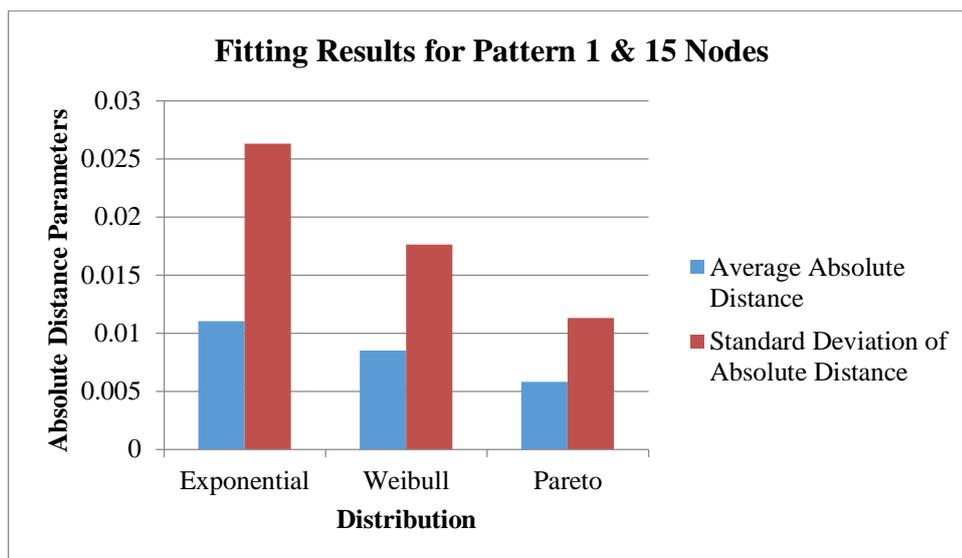


Figure 4.22: Distribution Fitting Results for Pattern 1 & 15 Nodes

4.2.1.2 Traffic Pattern 2: Higher Percentage of Healthcare Application

The second traffic pattern represents the case in which the majority of the traffic comes from medical sources. The four network loads send the same medical data but with slight difference in the percentage to match the number of nodes. In case of 6 and 12 nodes, 66.67% of the nodes are sending health data while the remaining 33.33% is divided equally between the traffic of smart cities and video surveillance applications. The percentage of the health data is 77.78% and 73.33% for the network of 9 and 15 nodes, respectively.

For this pattern, the CDF of the empirical data as well as the CDF of the three fitted distributions are presented in Figures 4.23, 4.24, 4.25, and 4.26. Furthermore, the parameters of these distributions for this certain pattern are shown in Tables 4.7, 4.8, 4.9, and 4.10.

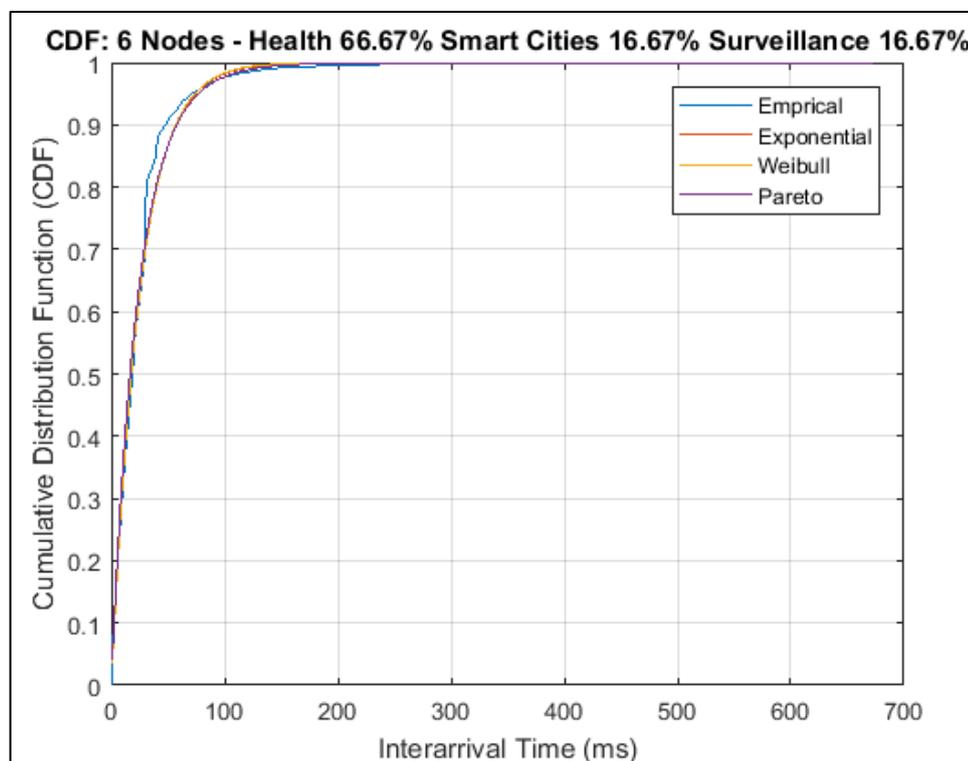


Figure 4.23: CDF of Inter-arrival Time for Pattern 2 & 6 Nodes

Table 4.7: Distributions' Parameters for Pattern 2 & 6 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	24.9425	0.0667	23.2339	0	25.2404	1.0274

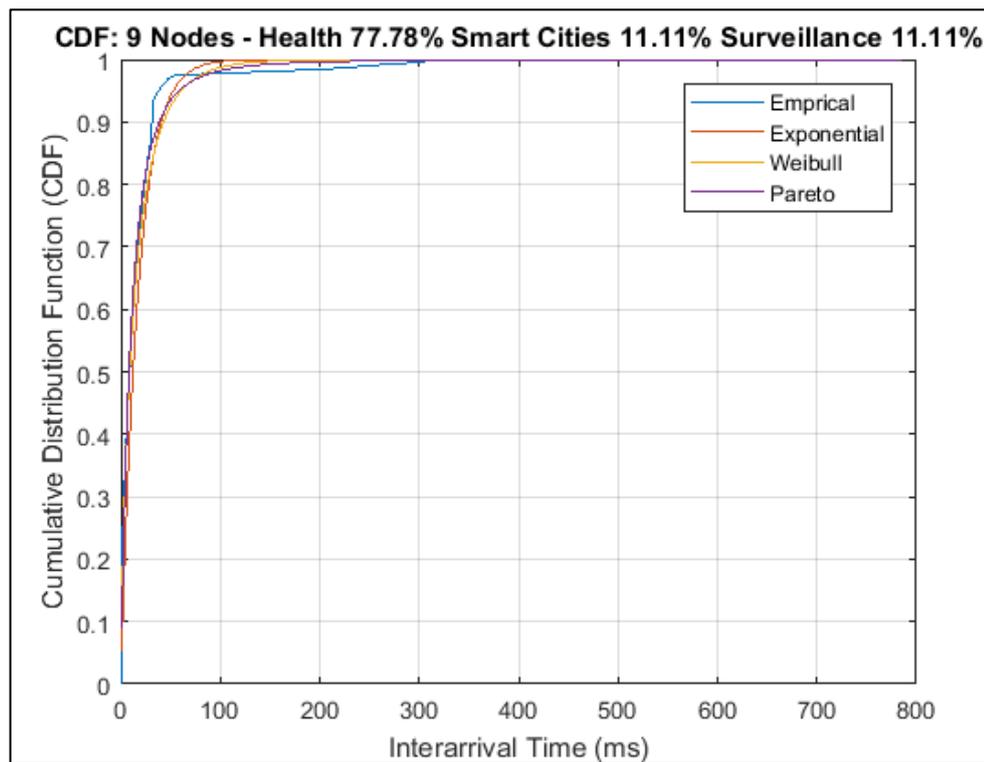


Figure 4.24: CDF of Inter-arrival Time for Pattern 2 & 9 Nodes

Table 4.8: Distributions' Parameters for Pattern 2 & 9 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	17.6358	0.3865	10.3730	0	14.3018	0.7575

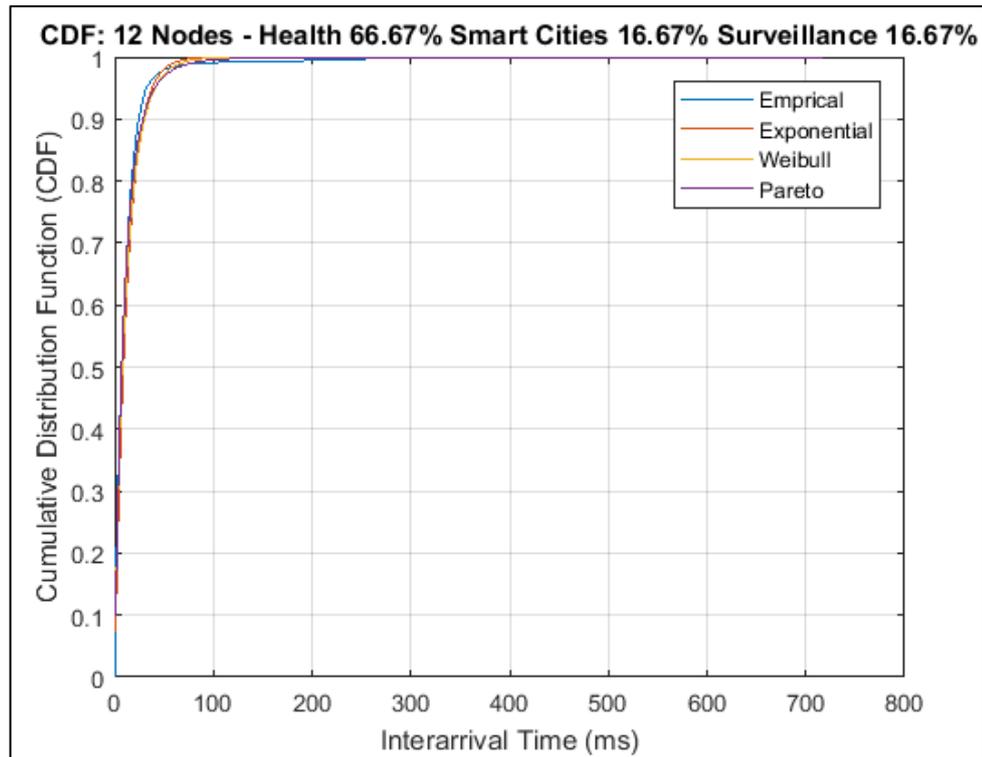


Figure 4.25: CDF of Inter-arrival Time for Pattern 2 & 12 Nodes

Table 4.9: Distributions' Parameters for Pattern 2 & 12 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	12.7355	0.2273	9.4711	0	11.7216	0.8760

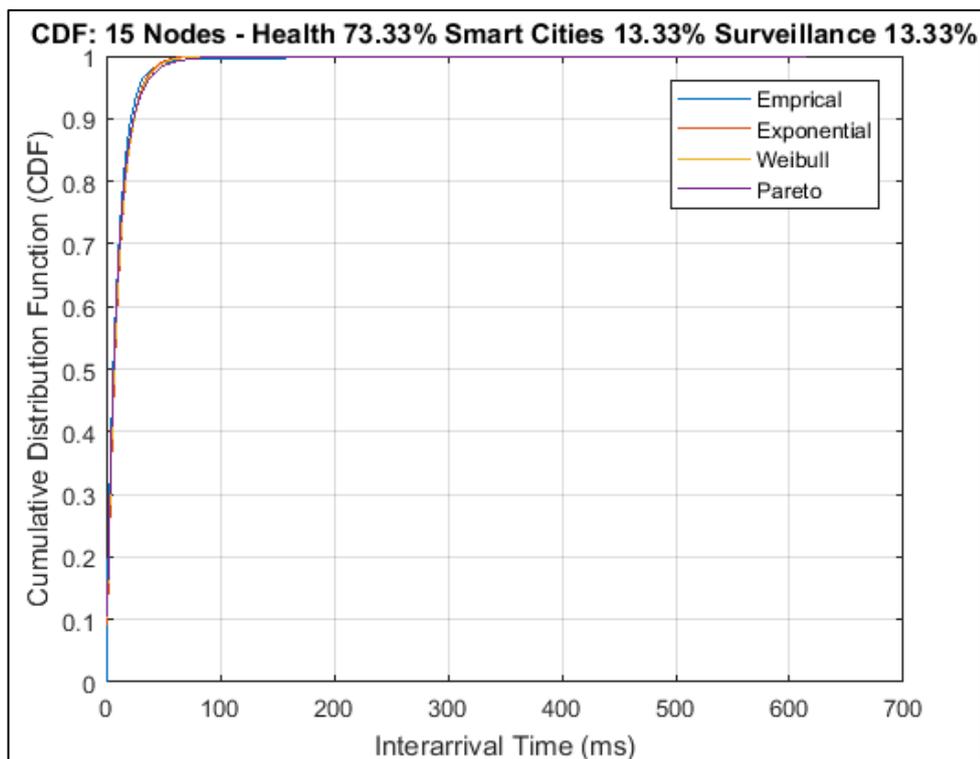


Figure 4.26: CDF of Inter-arrival Time for Pattern 2 & 15 Nodes

Table 4.10: Distributions' Parameters for Pattern 2 & 15 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	10.5686	0.1513	8.8015	0	10.2597	0.9467

Figure 4.27 indicates that when the network load is 6, Exponential and Pareto distributions have the same average which is 0.0094. It also shows that Weibull distribution has the smallest average (0.0091) and the lowest standard deviation (0.0156); thus, it is the closest distribution to describe the pattern for this load. However, as the figure reveals, the difference between the three distributions is slight in this case.

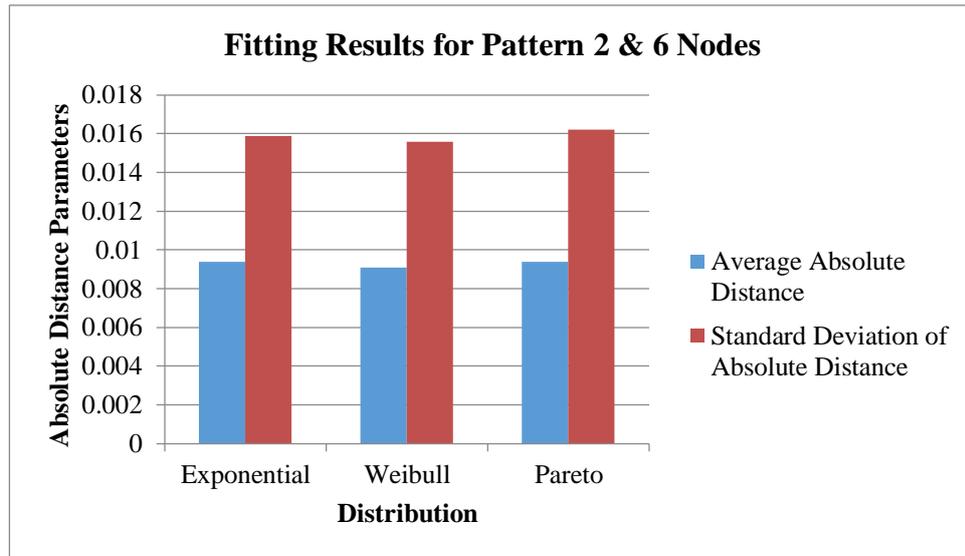


Figure 4.27: Distribution Fitting Results for Pattern 2 & 6 Nodes

It is clear from Figure 4.27 that the distribution has been affected by increasing the network load. Apparently, the results presented in Figures 4.28, 4.29, and 4.30 can be considered in line with Figure 4.27 given the small difference between the three distributions. In the case of 9, 12, and 15 nodes, the average and the standard deviation are both minimum when comparing the empirical CDF with the CDF of fitted Pareto. Therefore, Pareto distribution can be considered appropriate to generally model this traffic.

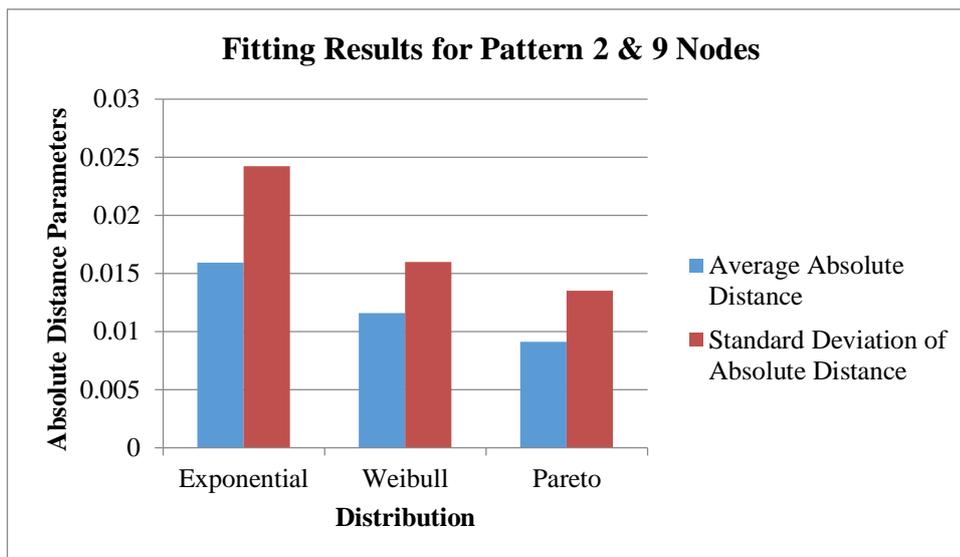


Figure 4.28: Distribution Fitting Results for Pattern 2 & 9 Nodes

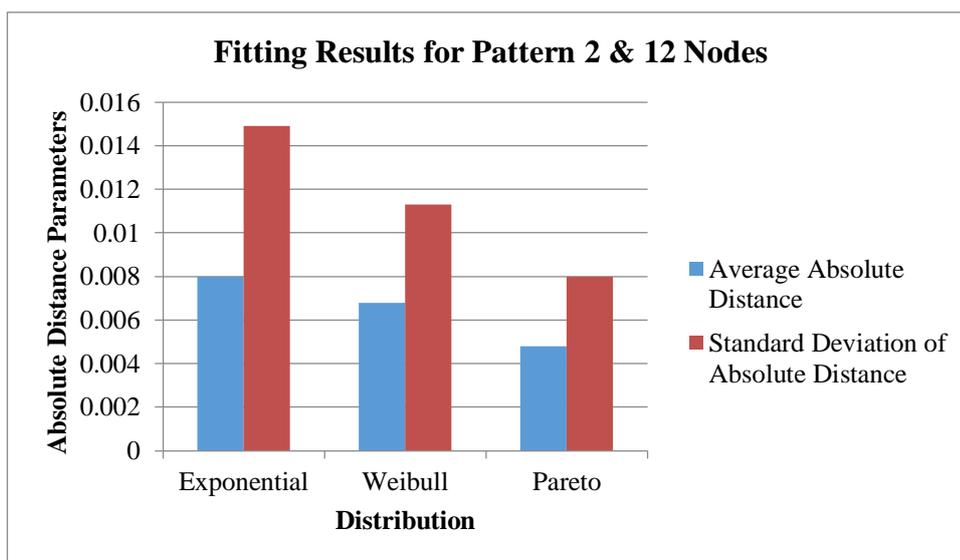


Figure 4.29: Distribution Fitting Results for Pattern 2 & 12 Nodes

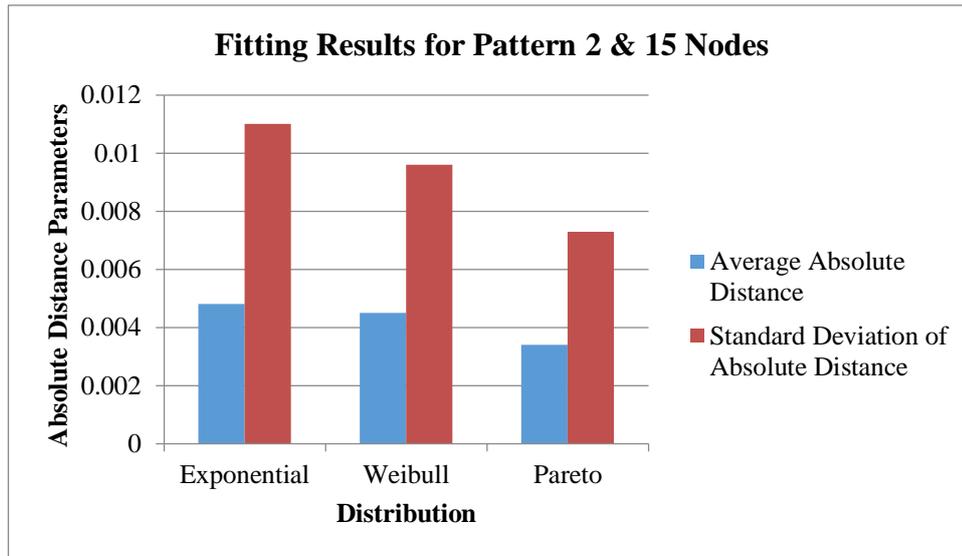


Figure 4.30: Distribution Fitting Results for Pattern 2 & 15 Nodes

4.2.1.3 Traffic Pattern 3: Higher Percentage of Smart Cities Application

In this pattern, most of the traffic received by the IoT gateway is related to smart cities. When the load is 6, four out of the six nodes are sending smart cities data while the remaining nodes are divided equally between the data of health and camera. The same scenario but with a slight difference in percentages is also tested with the other three gateway traffic loads. The CDF of the aggregated traffic is plotted in Figures 4.31, 4.32, 4.33, and 4.34. For each network load, there is a set of parameters defining each of the three distributions. The values of these parameters are displayed in Tables 4.11, 4.12, 4.13, and 4.14.

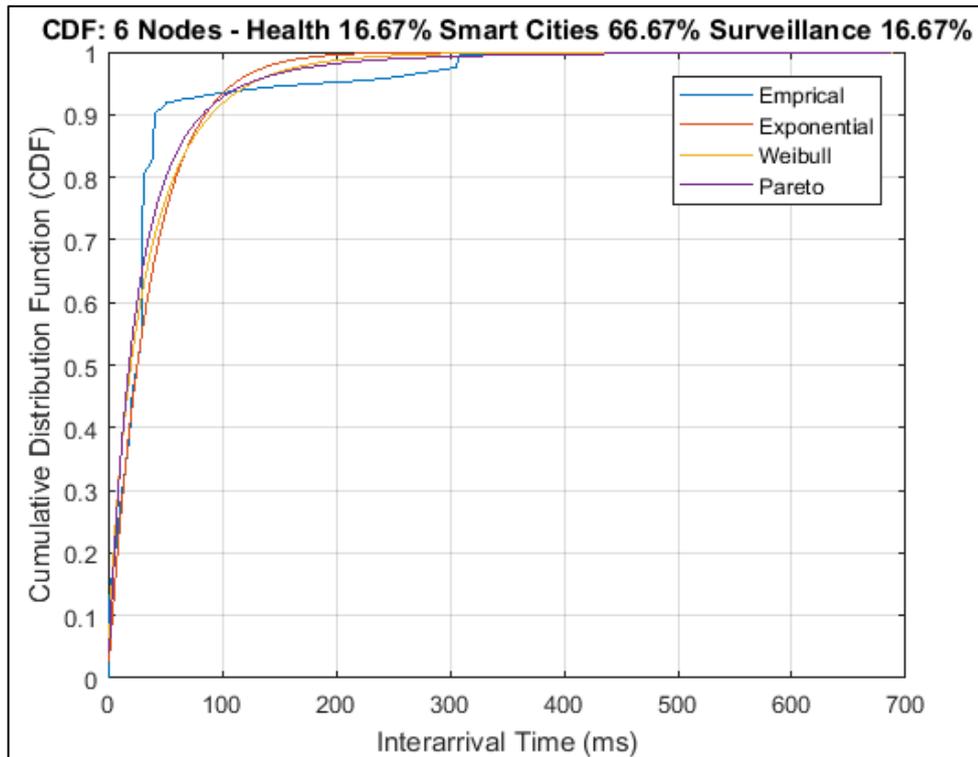


Figure 4.31: CDF of Inter-arrival Time for Pattern 3 & 6 Nodes

Table 4.11: Distributions' Parameters for Pattern 3 & 6 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	37.0296	0.3382	23.7104	0	31.6956	0.7946

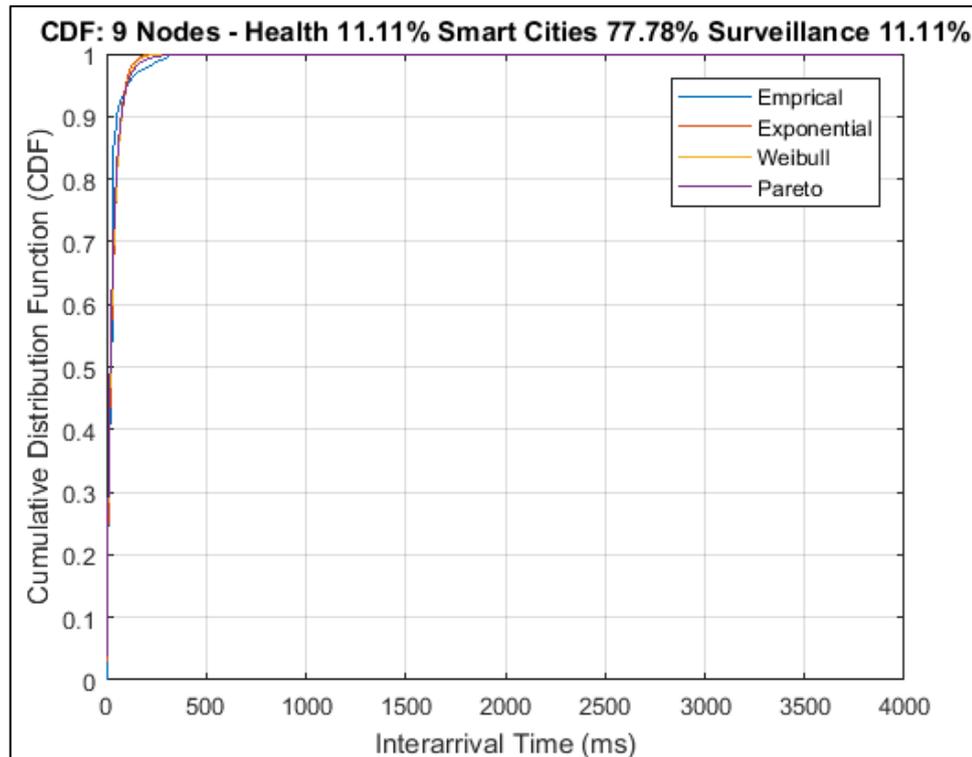


Figure 4.32: CDF of Inter-arrival Time for Pattern 3 & 9 Nodes

Table 4.12: Distributions' Parameters for Pattern 3 & 9 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	32.3134	0.1932	25.6119	0	30.6629	0.9093

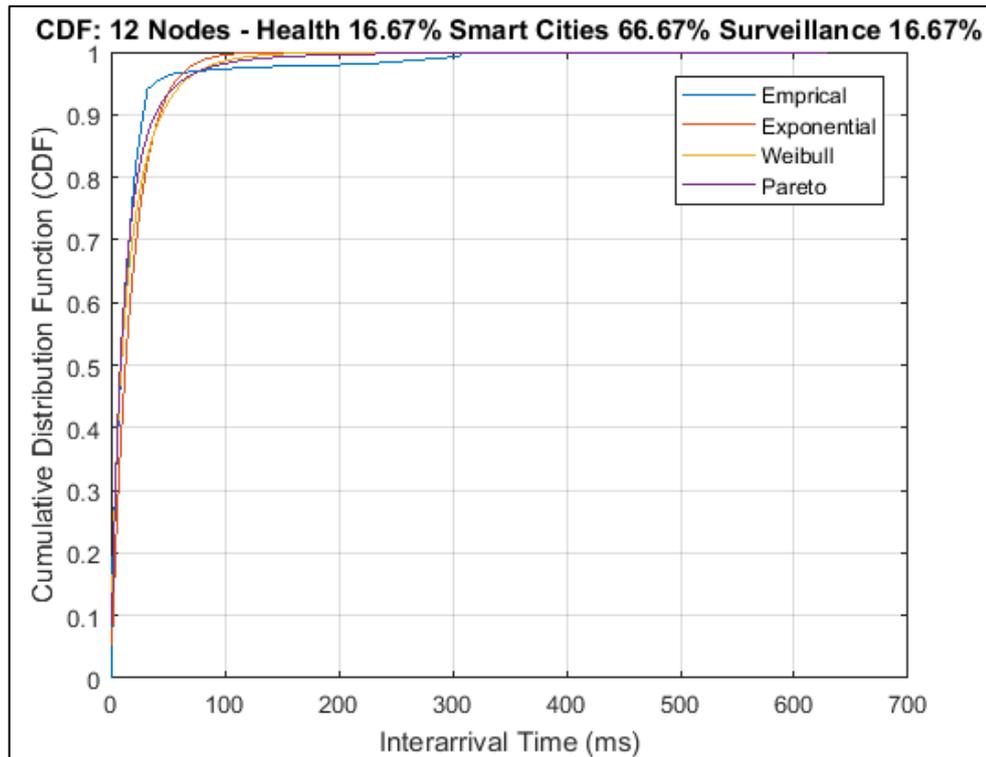


Figure 4.33: CDF of Inter-arrival Time for Pattern 3 & 12 Nodes

Table 4.13: Distributions' Parameters for Pattern 3 & 12 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	18.5435	0.3861	10.4995	0	14.8524	0.7592

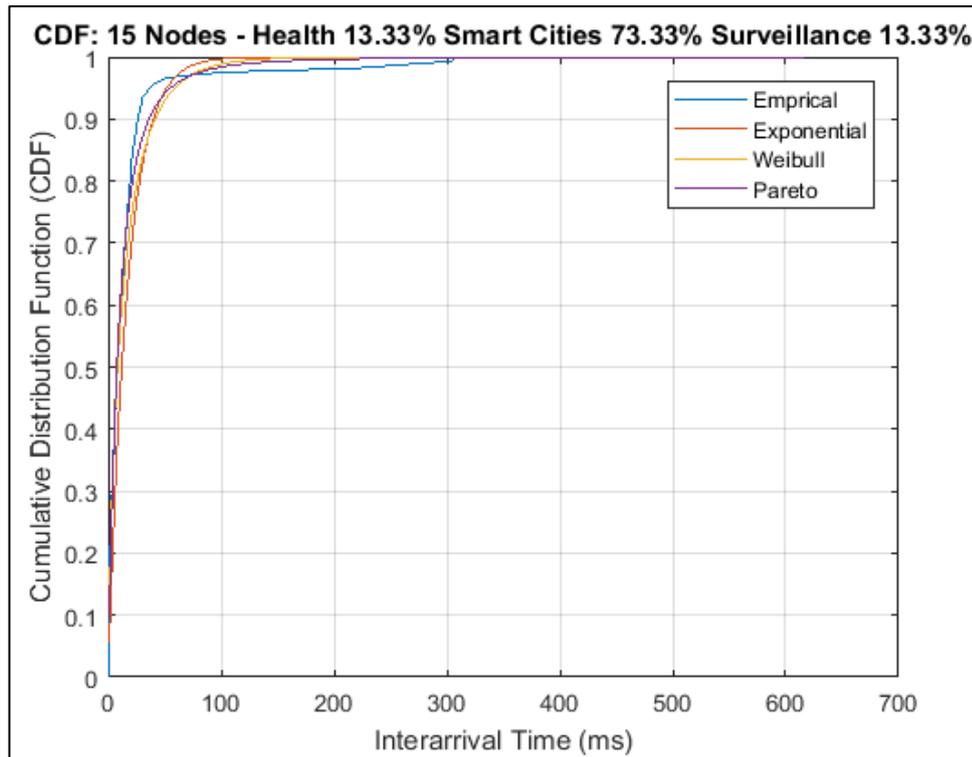


Figure 4.34: CDF of Inter-arrival Time for Pattern 3 & 15 Nodes

Table 4.14: Distributions' Parameters for Pattern 3 & 15 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	17.3333	0.3990	9.5647	0	13.6834	0.7508

Analyzing the fitting results in Figures 4.35, 4.36, 4.37, and 4.38 indicate that Pareto is the closest distribution to characterize this pattern regardless of the network loading. This also implies that the network loading has no significant effect on the distribution.

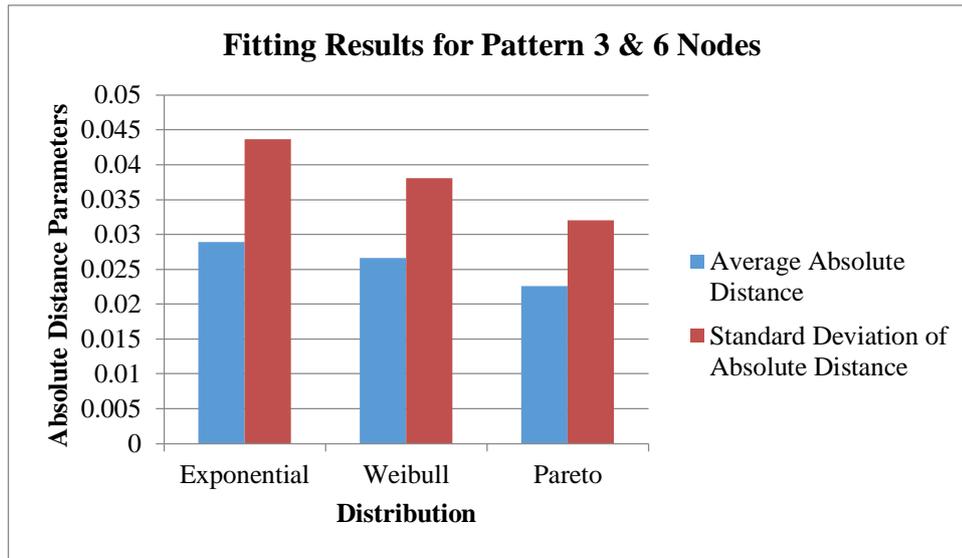


Figure 4.35: Distribution Fitting Results for Pattern 3 & 6 Nodes

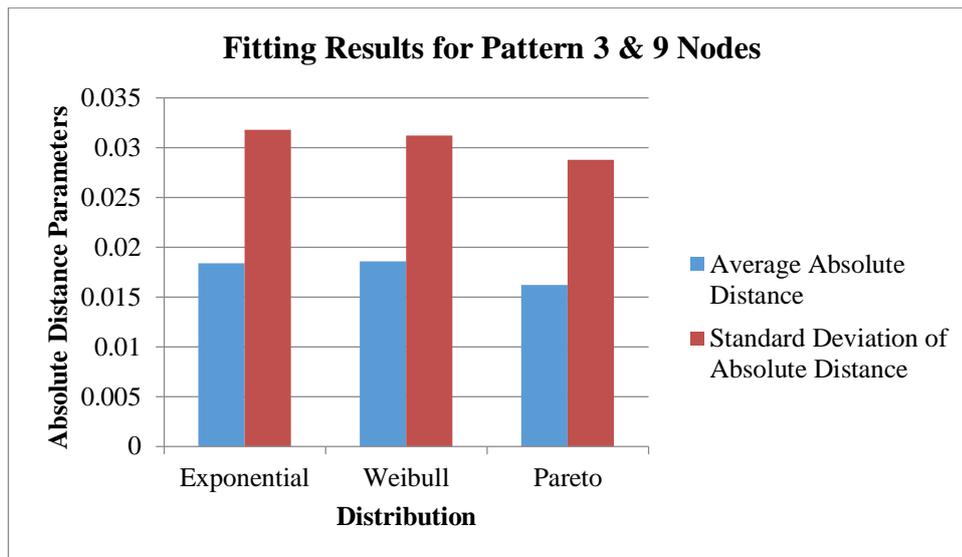


Figure 4.36: Distribution Fitting Results for Pattern 3 & 9 Nodes

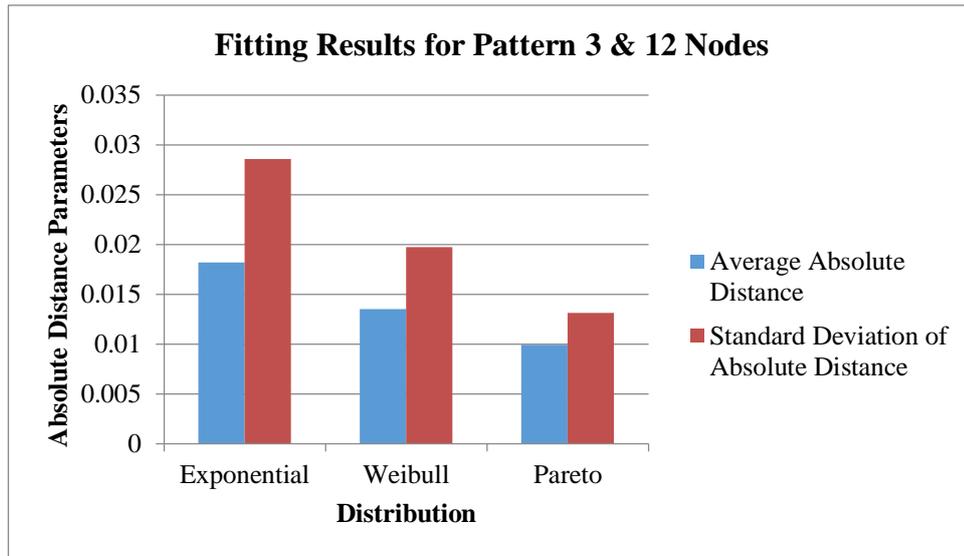


Figure 4.37: Distribution Fitting Results for Pattern 3 & 12 Nodes

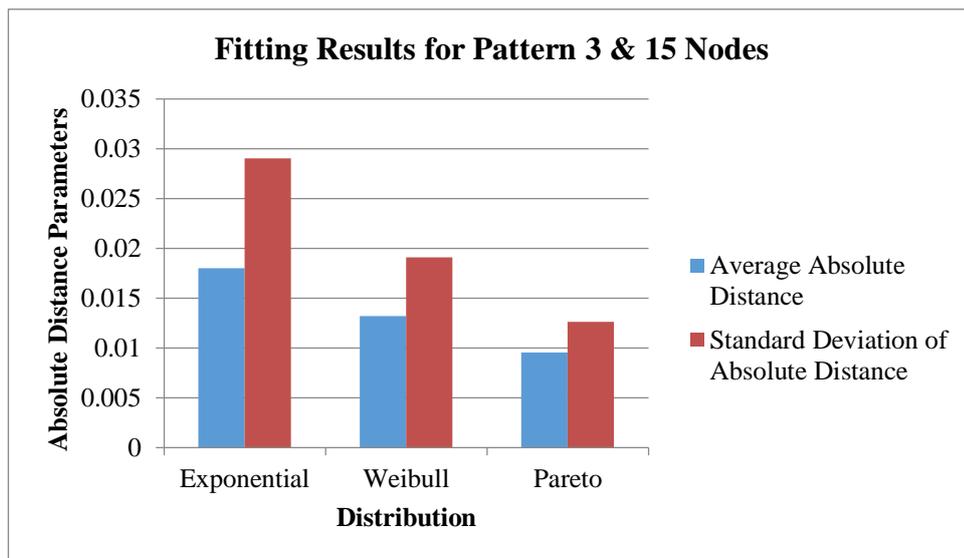


Figure 4.38: Distribution Fitting Results for Pattern 3 & 15 Nodes

4.2.1.4 Traffic Pattern 4: Higher Percentage of Video Surveillance Application

The three different applications are used in this pattern. However, the packets captured from the surveillance camera represent the majority of the output traffic. Figures 4.39, 4.40, 4.41, and 4.42 show the CDF generated using this recorded traffic in addition to the CDF of the fitted distributions for different number of nodes. Moreover, Tables 4.15, 4.16, 4.17, and 4.18 show the parameters used for the three fitted distributions for this pattern.

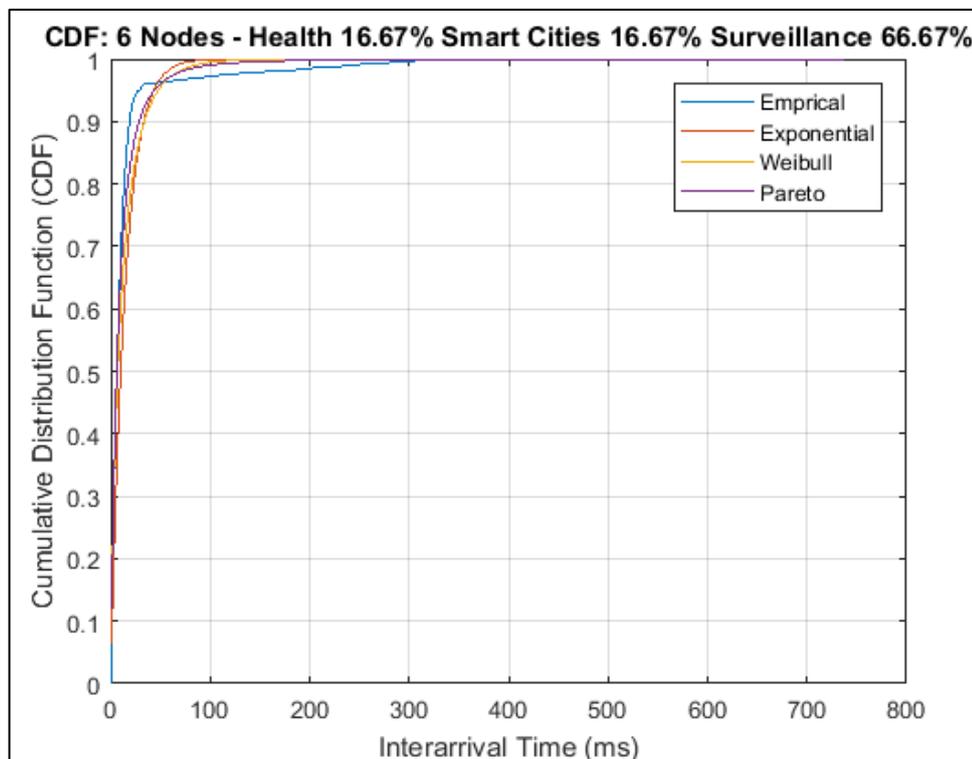


Figure 4.39: CDF of Inter-arrival Time for Pattern 4 & 6 Nodes

Table 4.15: Distributions' Parameters for Pattern 4 & 6 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	14.4400	0.3981	7.5827	0	11.2635	0.7574

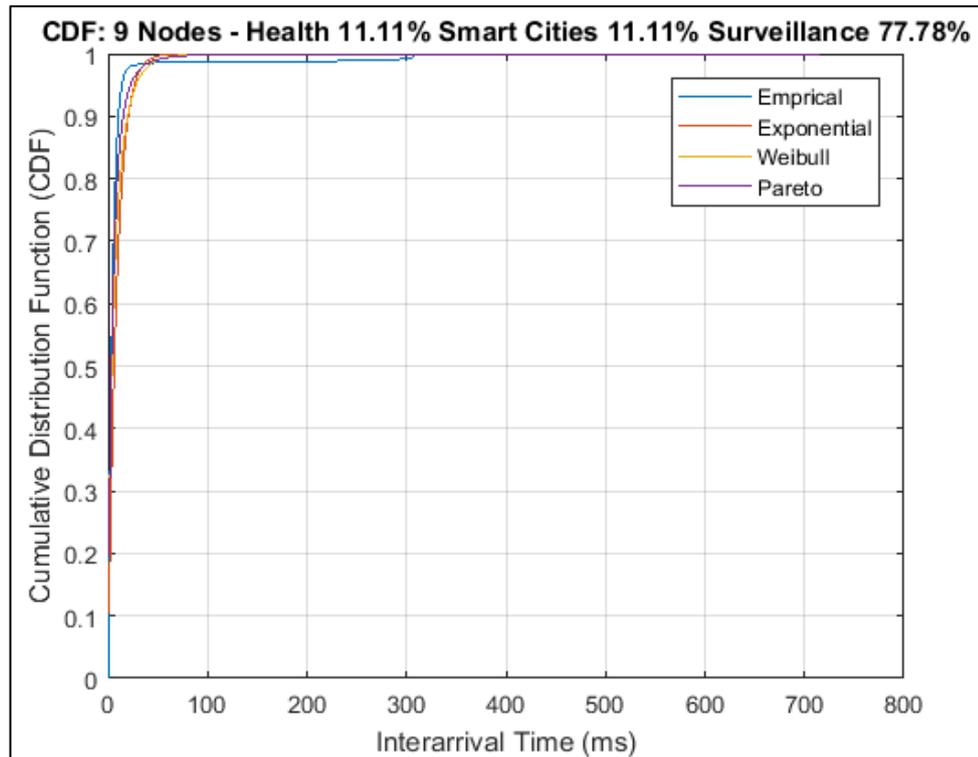


Figure 4.40: CDF of Inter-arrival Time for Pattern 4 & 9 Nodes

Table 4.16: Distributions' Parameters for Pattern 4 & 9 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	8.8879	0.3335	4.4036	0	6.3698	0.7400

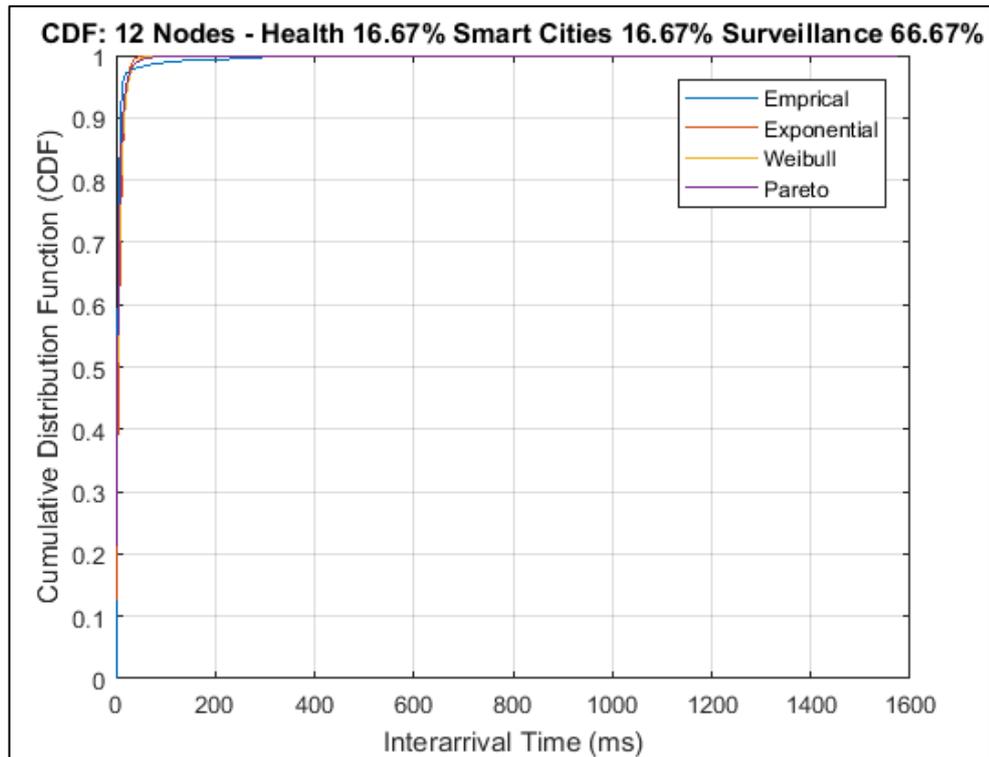


Figure 4.41: CDF of Inter-arrival Time for Pattern 4 & 12 Nodes

Table 4.17: Distributions' Parameters for Pattern 4 & 12 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	7.4252	0.3326	4.0013	0	5.7464	0.7710

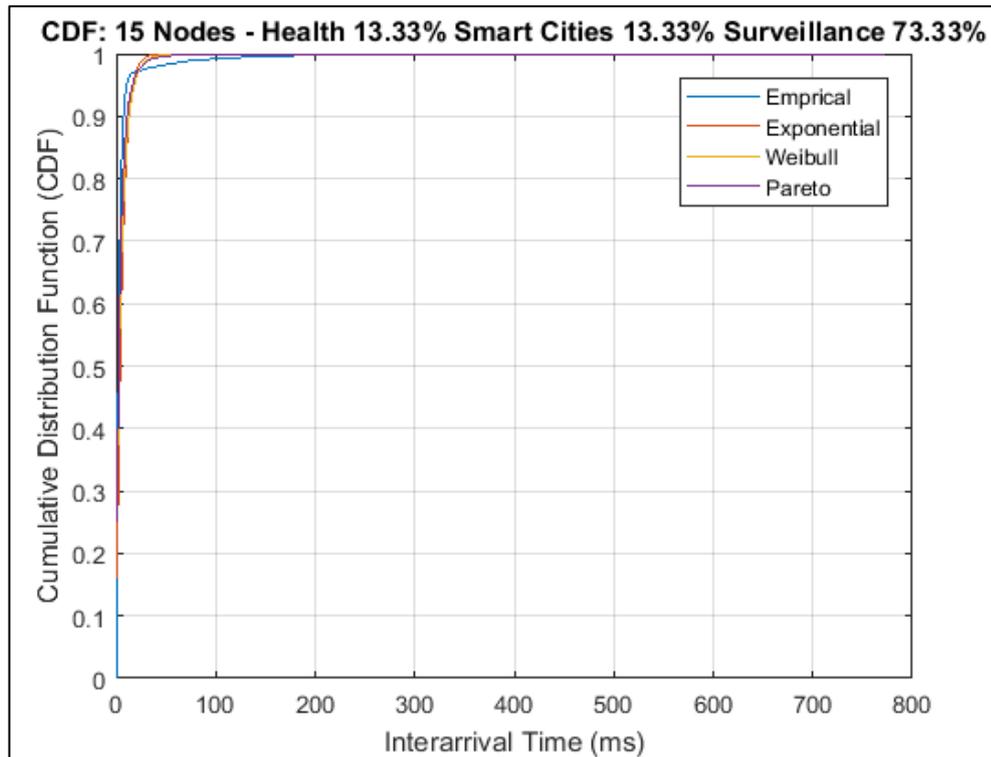


Figure 4.42: CDF of Inter-arrival Time for Pattern 4 & 15 Nodes

Table 4.18: Distributions' Parameters for Pattern 4 & 15 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	5.6787	0.3142	3.2723	0	4.6550	0.8040

The average and the standard deviation of the absolute distance presented in Figures 4.43, 4.44, 4.45, and 4.46 indicate that there is an agreement that Pareto distribution is the best distribution to model this type of traffic regardless of the number of nodes.

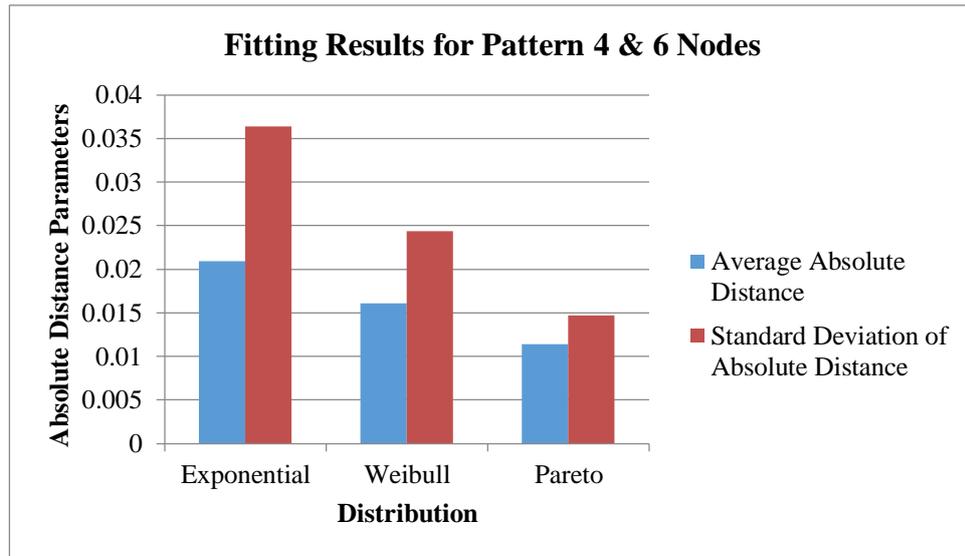


Figure 4.43: Distribution Fitting Results for Pattern 4 & 6 Nodes

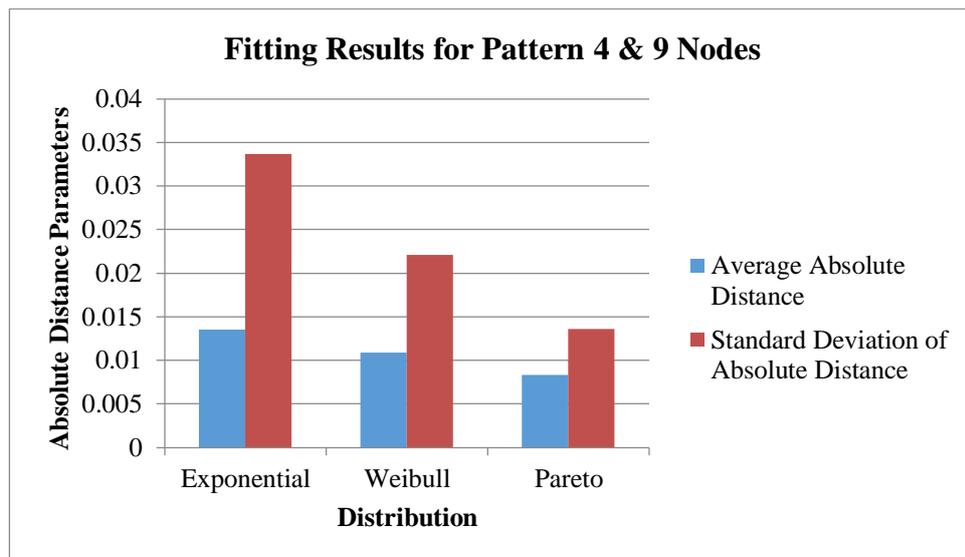


Figure 4.44: Distribution Fitting Results for Pattern 4 & 9 Nodes

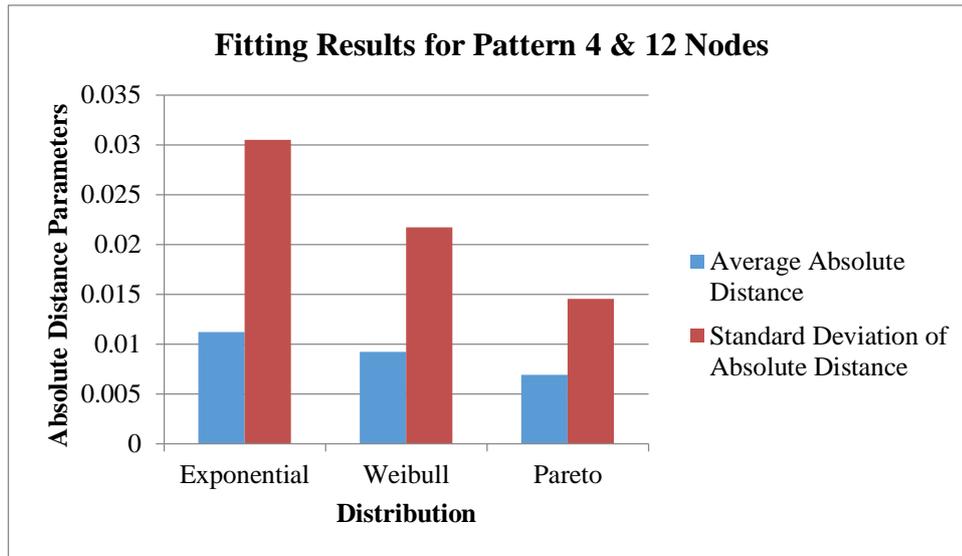


Figure 4.45: Distribution Fitting Results for Pattern 4 & 12 Nodes

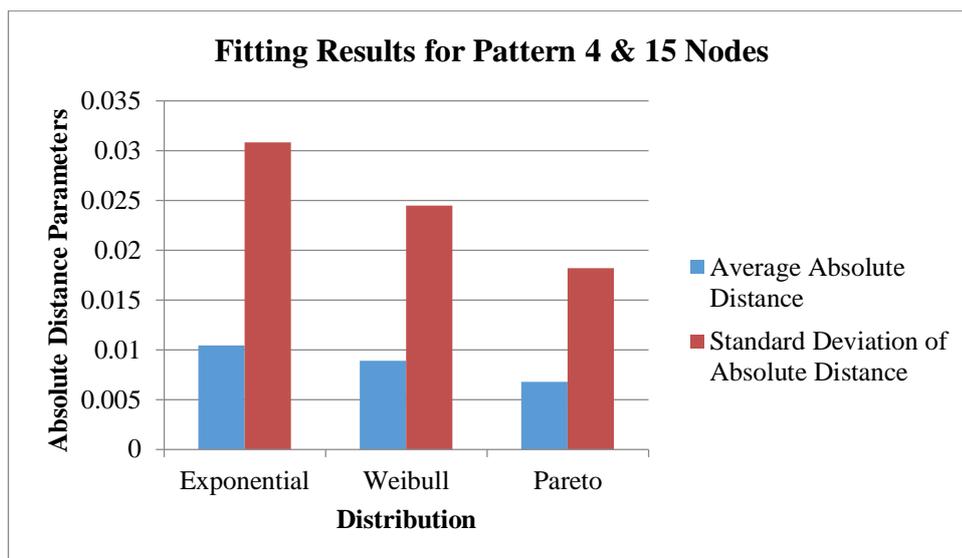


Figure 4.46: Distribution Fitting Results for Pattern 4 & 15 Nodes

4.2.1.5 Traffic Pattern 5: Video Surveillance Application only

Figures from 4.47 to 4.50 display the CDF generated when camera packets are only replayed in all the nodes. This means that 100% of the load sends the same type of data to the gateway. The distributions' parameters used for this pattern are shown in Tables 4.19, 4.20, 4.21, and 4.22.

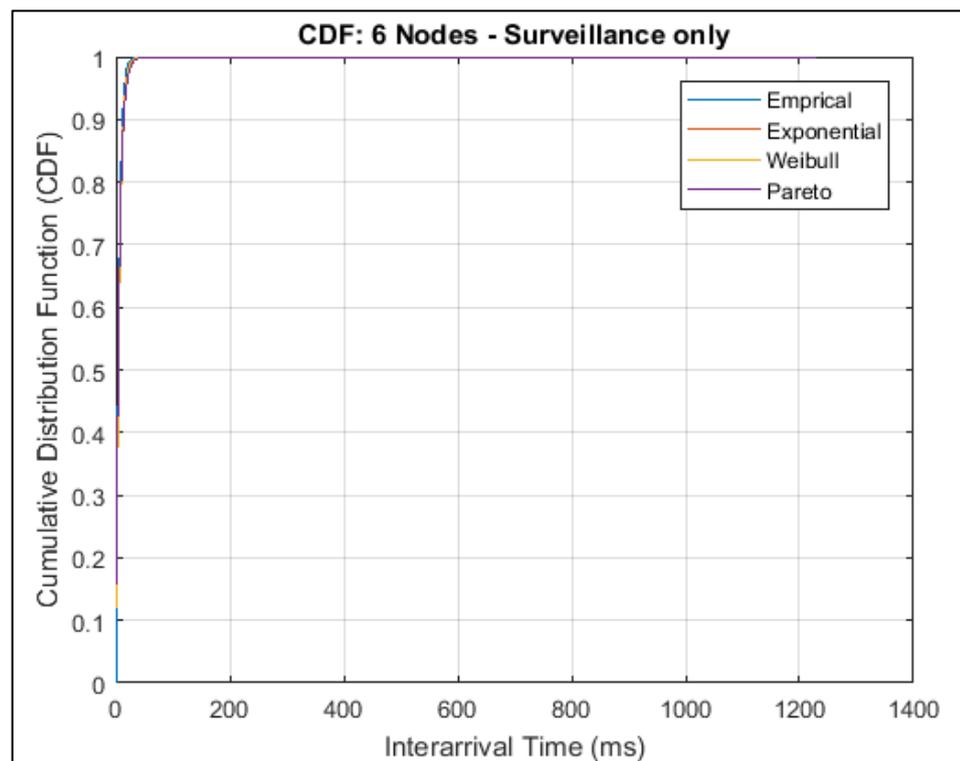


Figure 4.47: CDF of Inter-arrival Time for Pattern 5 & 6 Nodes

Table 4.19: Distributions' Parameters for Pattern 5 & 6 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	6.0538	0.0475	5.7249	0	6.3330	1.1090

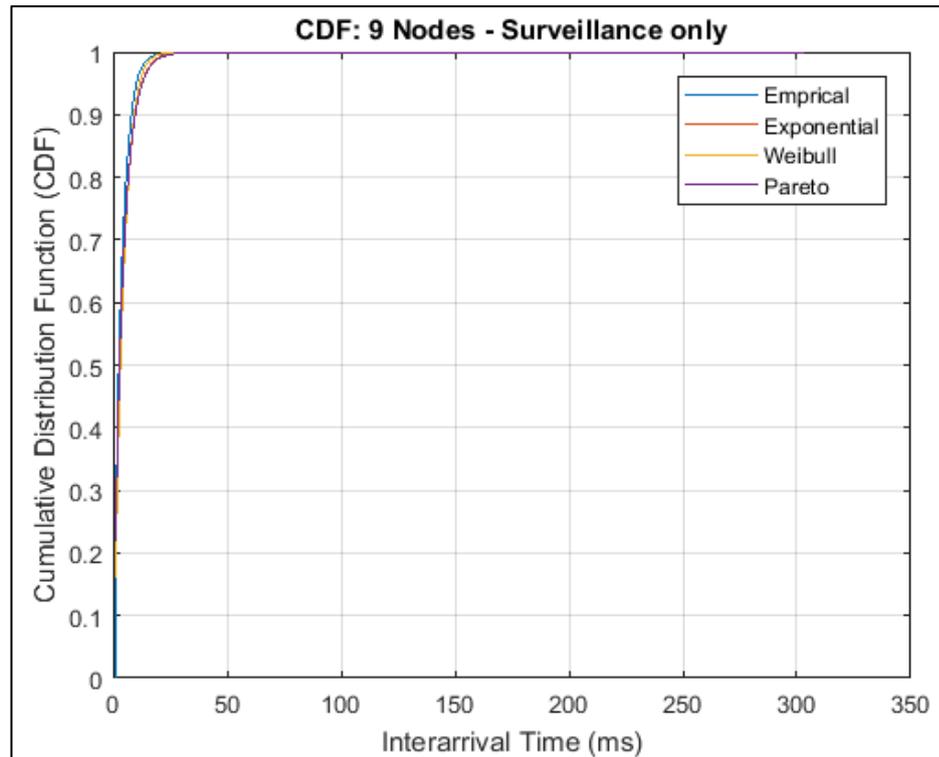


Figure 4.48: CDF of Inter-arrival Time for Pattern 5 & 9 Nodes

Table 4.20: Distributions' Parameters for Pattern 5 & 9 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	4.2369	0.0405	4.0347	0	4.4988	1.1511

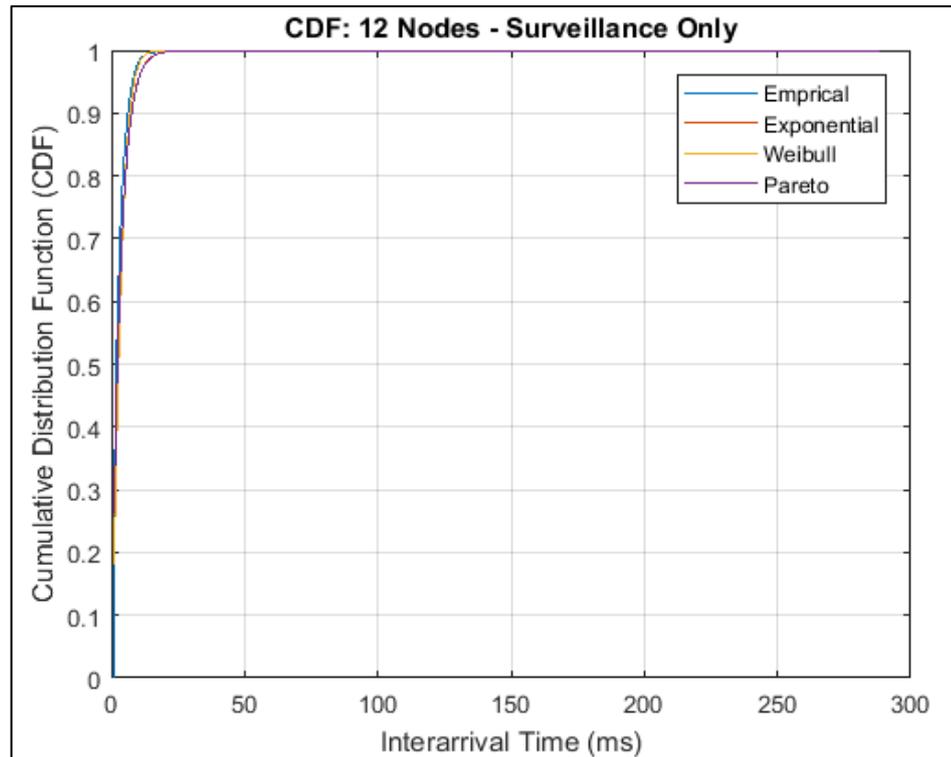


Figure 4.49: CDF of Inter-arrival Time for Pattern 5 & 12 Nodes

Table 4.21: Distributions' Parameters for Pattern 5 & 12 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	3.2988	0.0127	3.2542	0	3.5888	1.2623

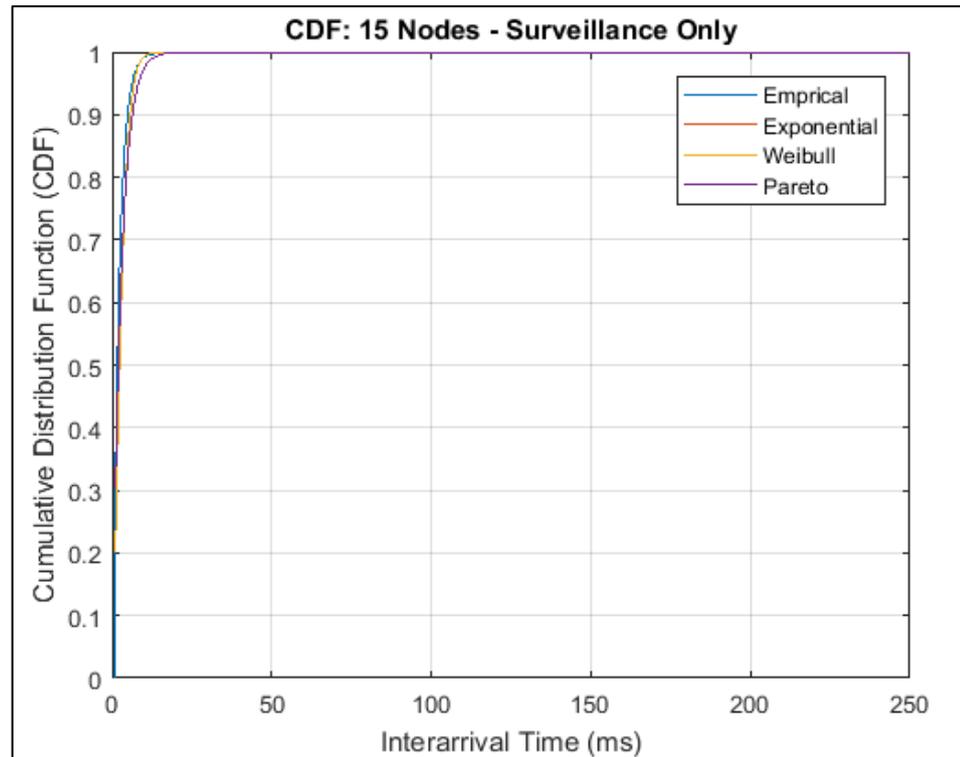


Figure 4.50: CDF of Inter-arrival Time for Pattern 5 & 15 Nodes

Table 4.22: Distributions' Parameters for Pattern 5 & 15 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	2.7449	- 0.00034	2.7458	0	3.0251	1.3436

The same behavior is noticed when the gateway is loaded with either 6 or 9 nodes (6 – 9 surveillance cameras). Figures 4.51 and 4.52 reveal that the absolute difference between the CDF of the experimental data and the fitted Pareto has the lowest average as well as the lowest standard deviation. Therefore, Pareto distribution appears to be the most appropriate model to characterize these two cases. Also, it can be observed from Figure 4.52 that the parameters of the Exponential and Weibull distributions are almost the same. In addition, they are very close to those of Pareto, the difference between them does not exceed 0.0001.

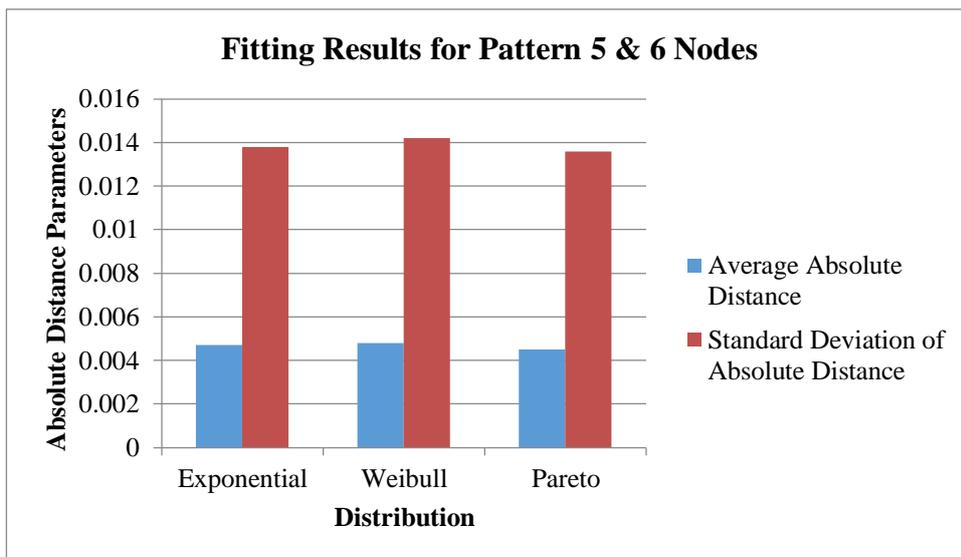


Figure 4.51: Distribution Fitting Results for Pattern 5 & 6 Nodes

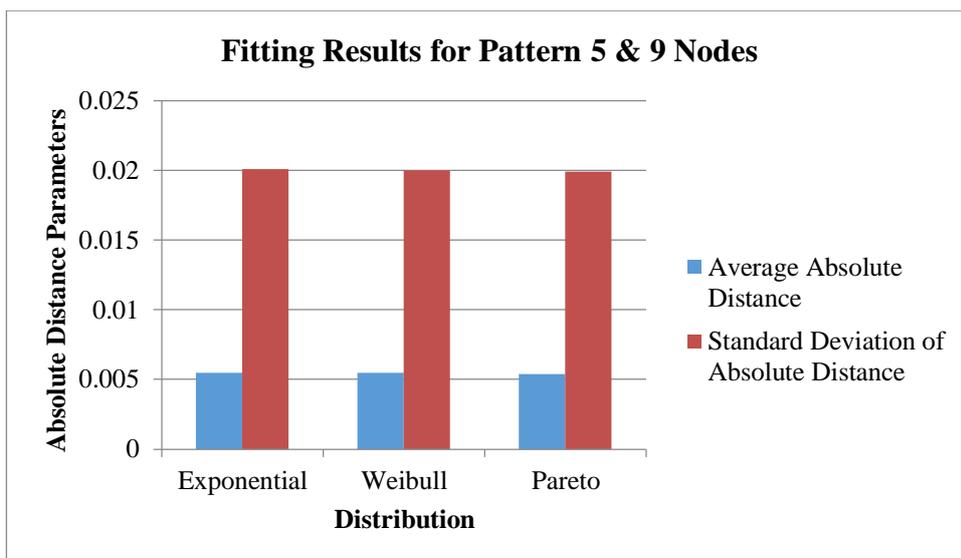


Figure 4.52: Distribution Fitting Results for Pattern 5 & 9 Nodes

The results are slightly changed when the load of the gateway increases to 12 and 15 nodes. It can be clearly noticed from the results presented in Figures 4.53 and 4.54 that Weibull distribution better models the camera traffic for these two cases.

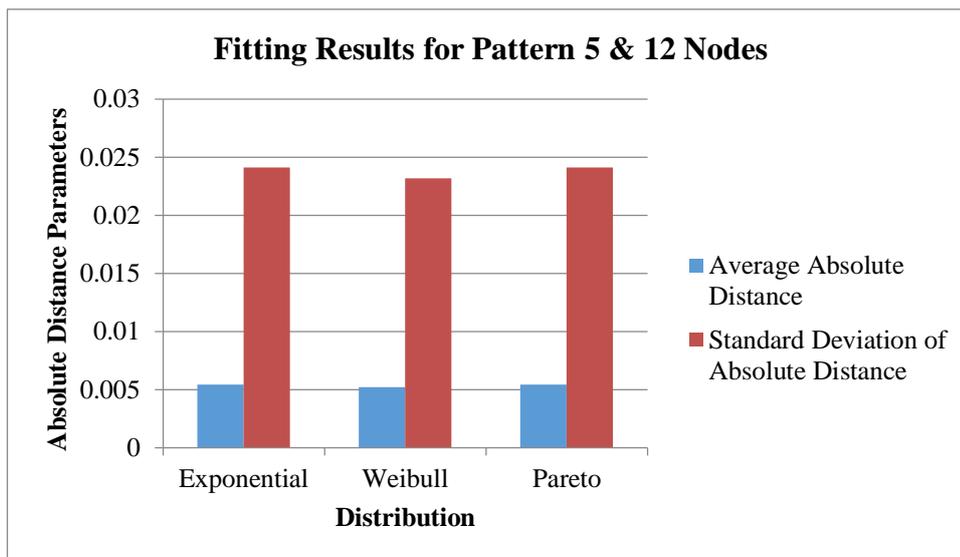


Figure 4.53: Distribution Fitting Results for Pattern 5 & 12 Nodes

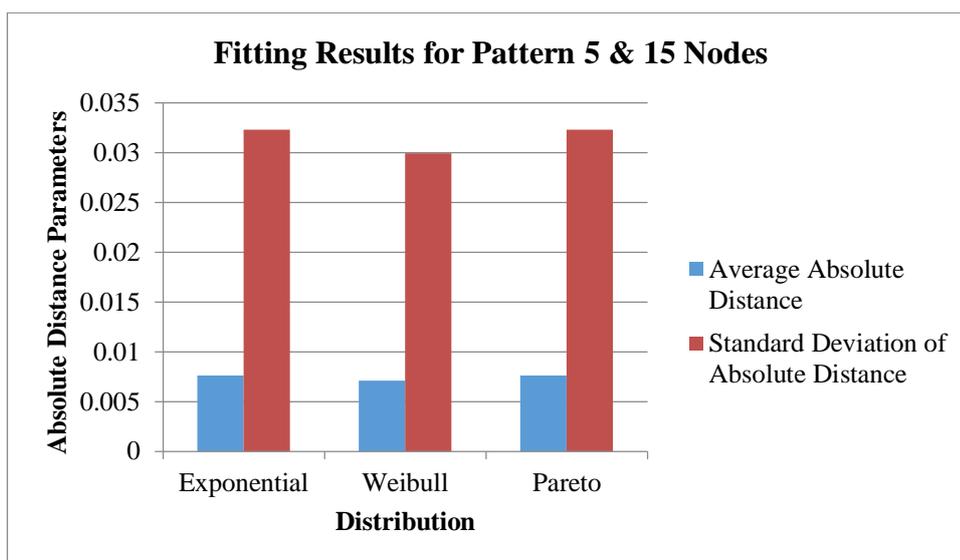


Figure 4.54: Distribution Fitting Results for Pattern 5 & 15 Nodes

4.2.1.6 Traffic Pattern 6: Healthcare Application only

The data for this pattern is selected to emulate the case when the traffic is purely health with zero contribution of any other applications. Figures 4.55, 4.56, 4.57, and 4.58 contain the CDF plots of the health traffic along with the fitted CDFs as the gateway load increases from 6 to 15 nodes. In addition, the parameters' values describing each of the fitted distributions for this particular scenario are found in Tables 4.23, 4.24, 4.25, and 4.26.

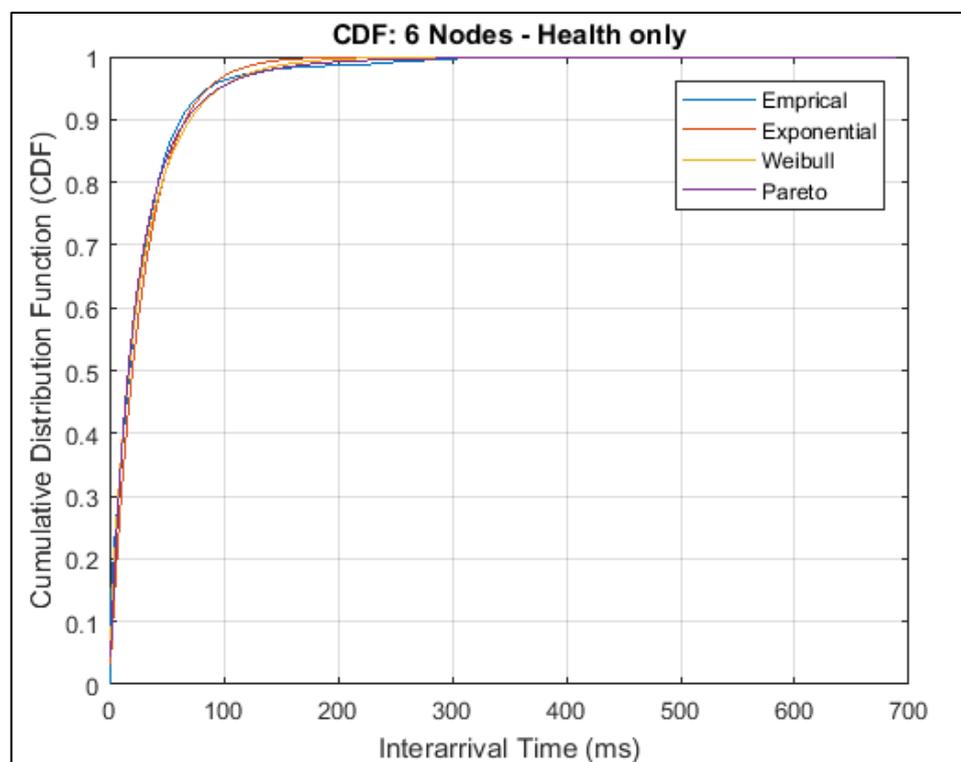


Figure 4.55: CDF of Inter-arrival Time for Pattern 6 & 6 Nodes

Table 4.23: Distributions' Parameters for Pattern 6 & 6 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	28.9095	0.2469	21.7539	0	26.0718	0.8337

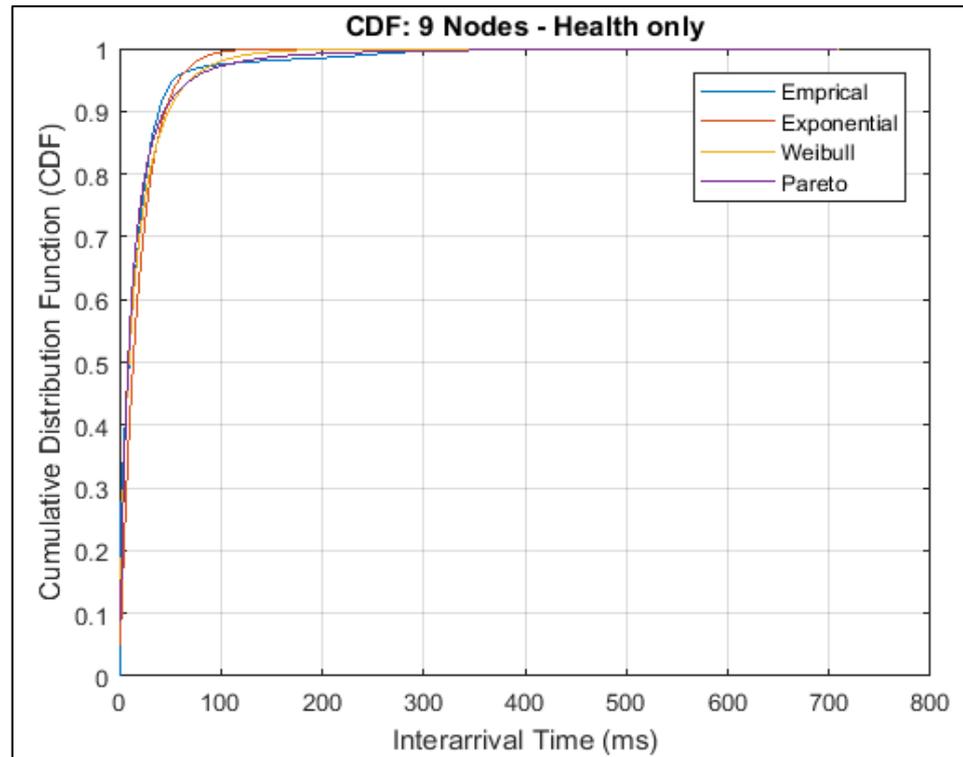


Figure 4.56: CDF of Inter-arrival Time for Pattern 6 & 9 Nodes

Table 4.24: Distributions' Parameters for Pattern 6 & 9 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	19.5904	0.4858	10.4320	0	15.4173	0.7270

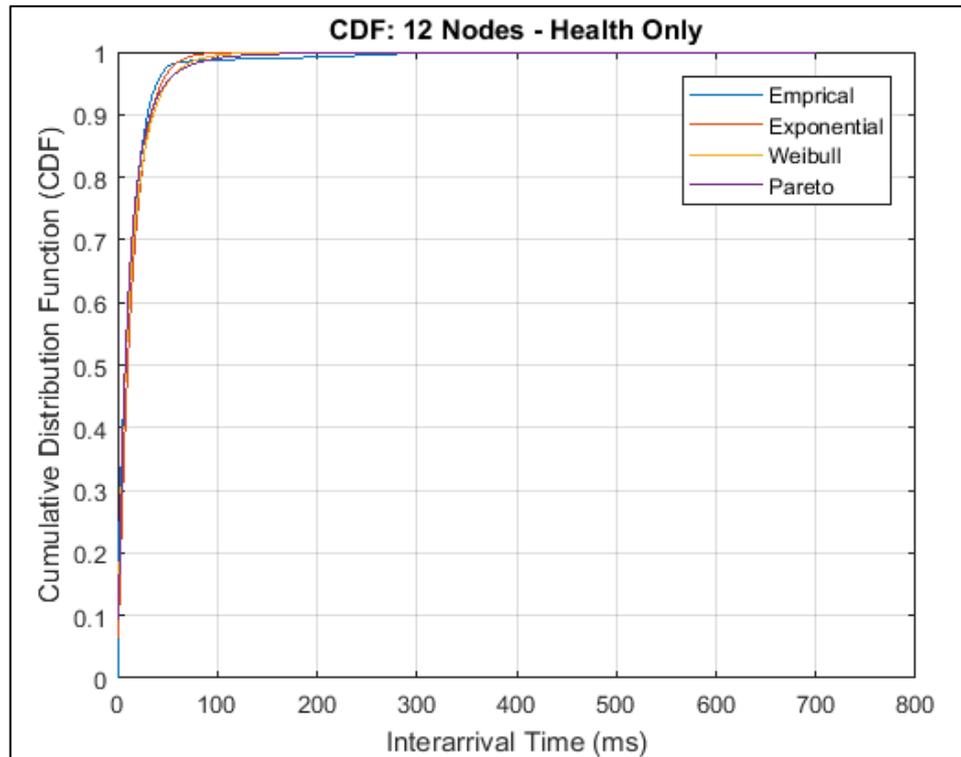


Figure 4.57: CDF of Inter-arrival Time for Pattern 6 & 12 Nodes

Table 4.25: Distributions' Parameters for Pattern 6 & 12 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	14.7376	0.3063	9.9059	0	12.7732	0.8084

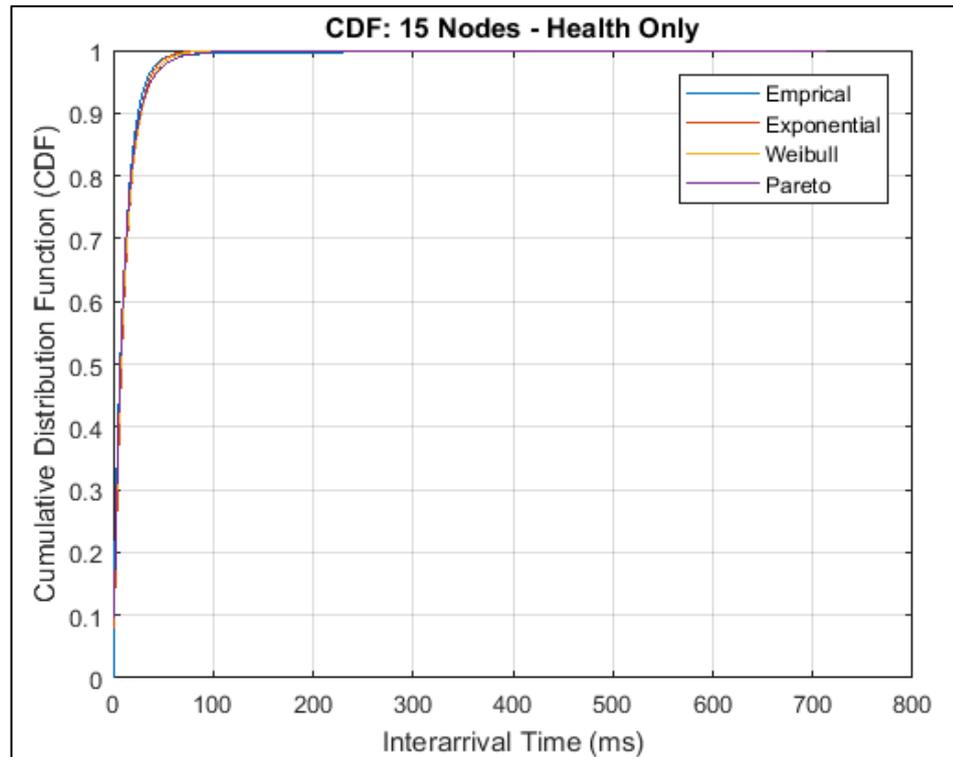


Figure 4.58: CDF of Inter-arrival Time for Pattern 6 & 15 Nodes

Table 4.26: Distributions' Parameters for Pattern 6 & 15 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	11.8701	0.1764	9.5720	0	11.2817	0.9136

Pareto distribution appears to closely fit the empirical CDF according to Figures 4.59, 4.60, 4.61, and 4.62. This indicates that Pareto distribution can be used to model the packet inter-arrival time for this pattern. Furthermore, it can be observed that Exponential has the farthest absolute distribution distance among all distributions from the empirical CDF irrespective of the gateway load.

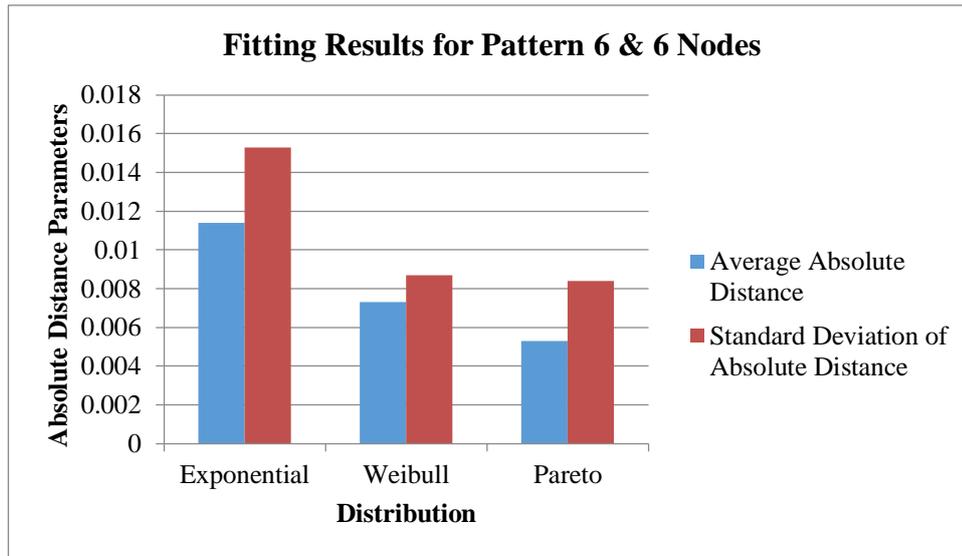


Figure 4.59: Distribution Fitting Results for Pattern 6 & 6 Nodes

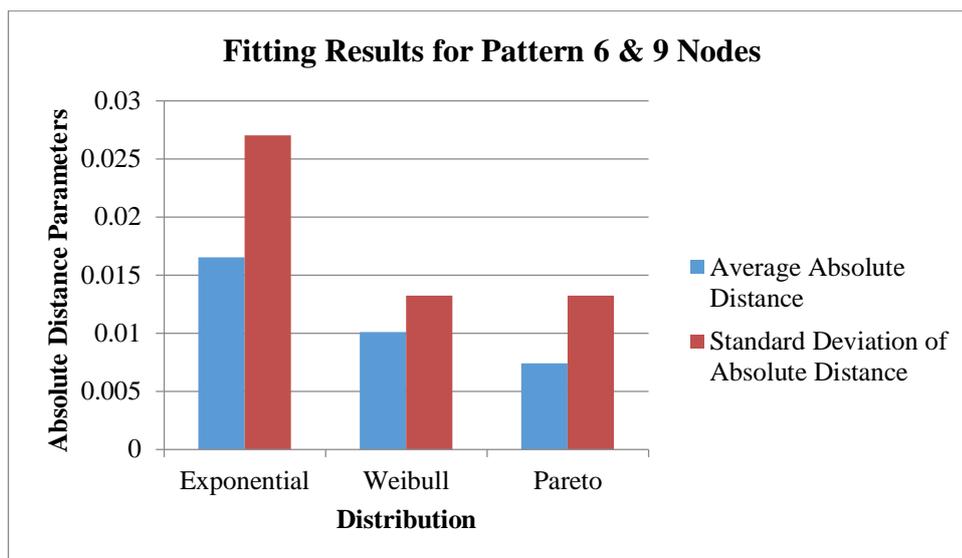


Figure 4.60: Distribution Fitting Results for Pattern 6 & 9 Nodes

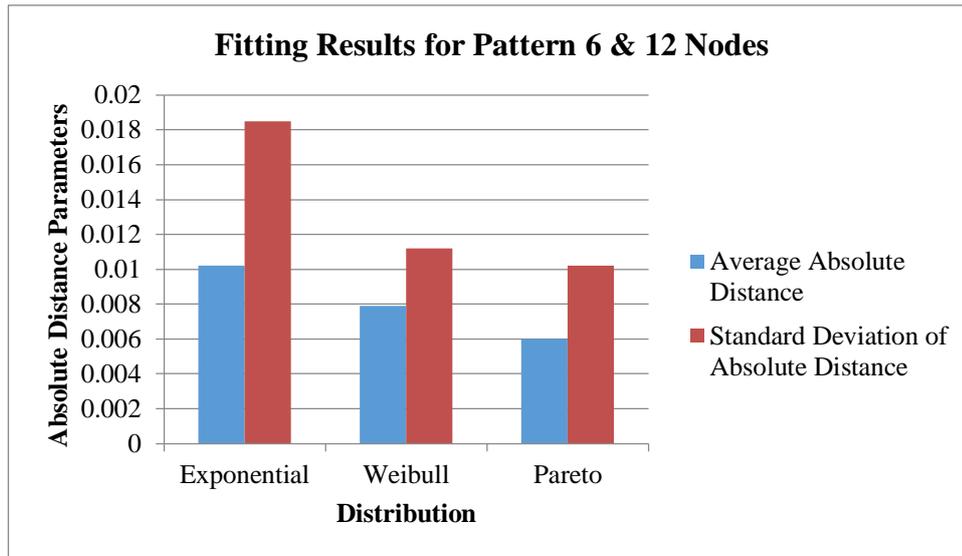


Figure 4.61: Distribution Fitting Results for Pattern 6 & 12 Nodes

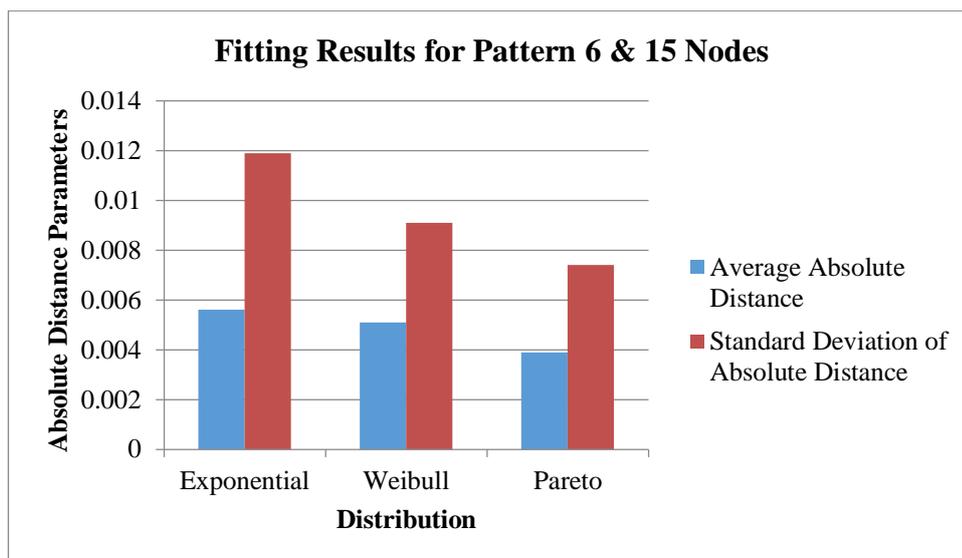


Figure 4.62: Distribution Fitting Results for Pattern 6 & 15 Nodes

4.2.1.7 Traffic Pattern 7: Smart Cities Application only

The last case evaluates the pattern when the traffic comes only from smart cities sensors. Figures from 4.63 to 4.66 plot the CDF of the observed values as well as the CDF for Exponential, Weibull and Pareto distributions. Tables 4.27, 4.28, 4.29, and 4.30 show the parameters used for distribution fitting.

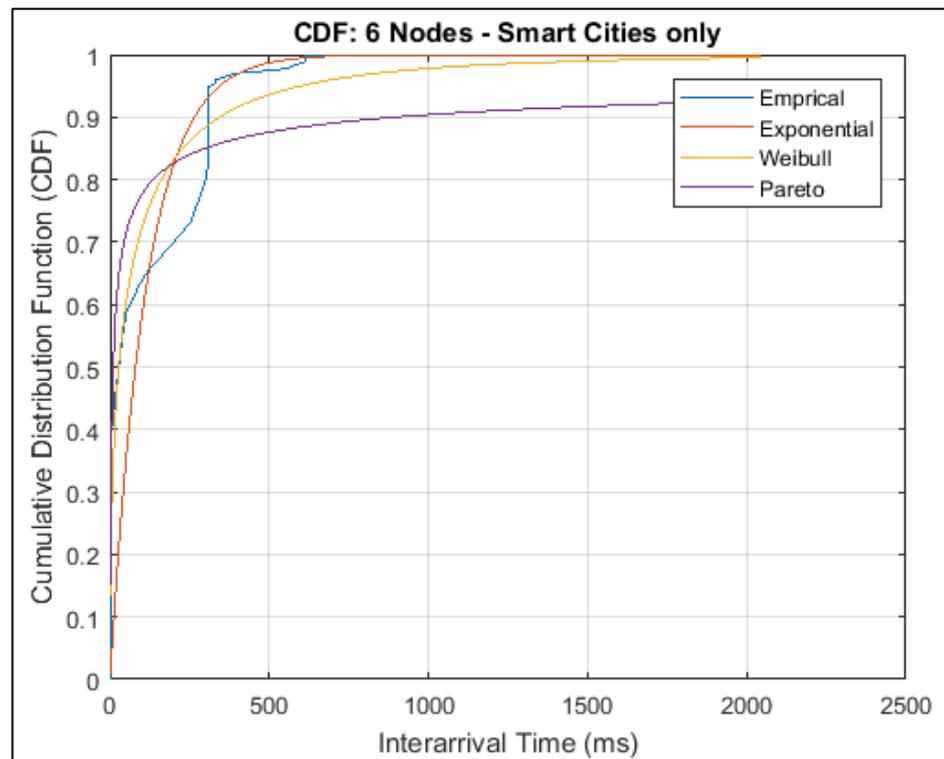


Figure 4.63: CDF of Inter-arrival Time for Pattern 7 & 6 Nodes

Table 4.27: Distributions' Parameters for Pattern 7 & 6 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	114.9089	2.7080	4.7558	0	59.0134	0.4736

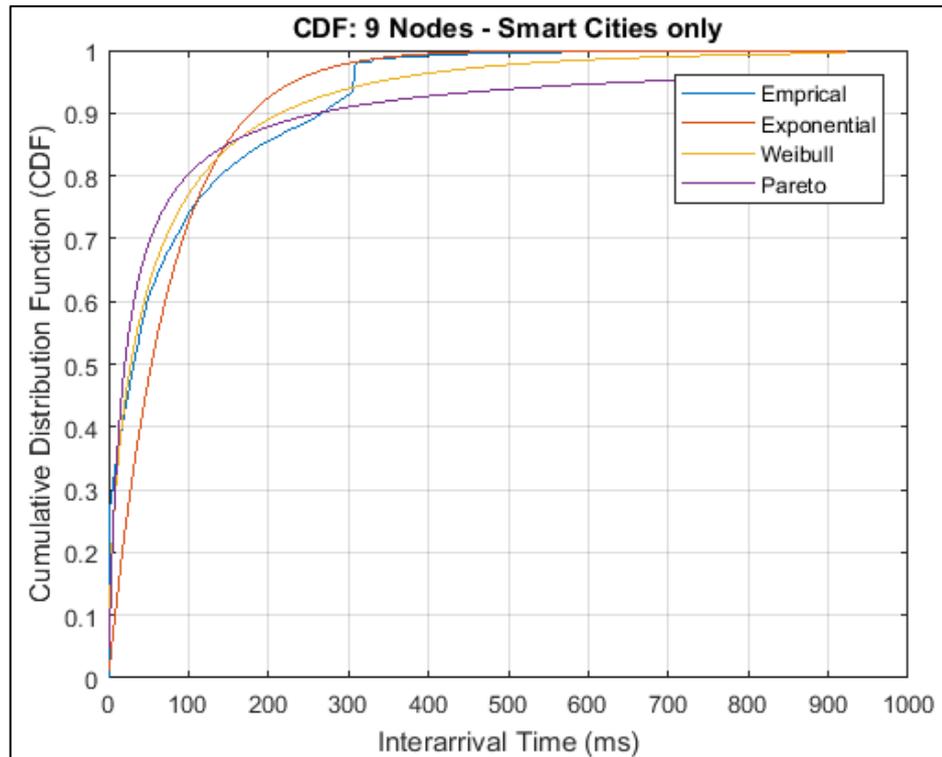


Figure 4.64: CDF of Inter-arrival Time for Pattern 7 & 9 Nodes

Table 4.28: Distributions' Parameters for Pattern 7 & 9 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	77.3453	1.2965	18.0471	0	51.7662	0.5852

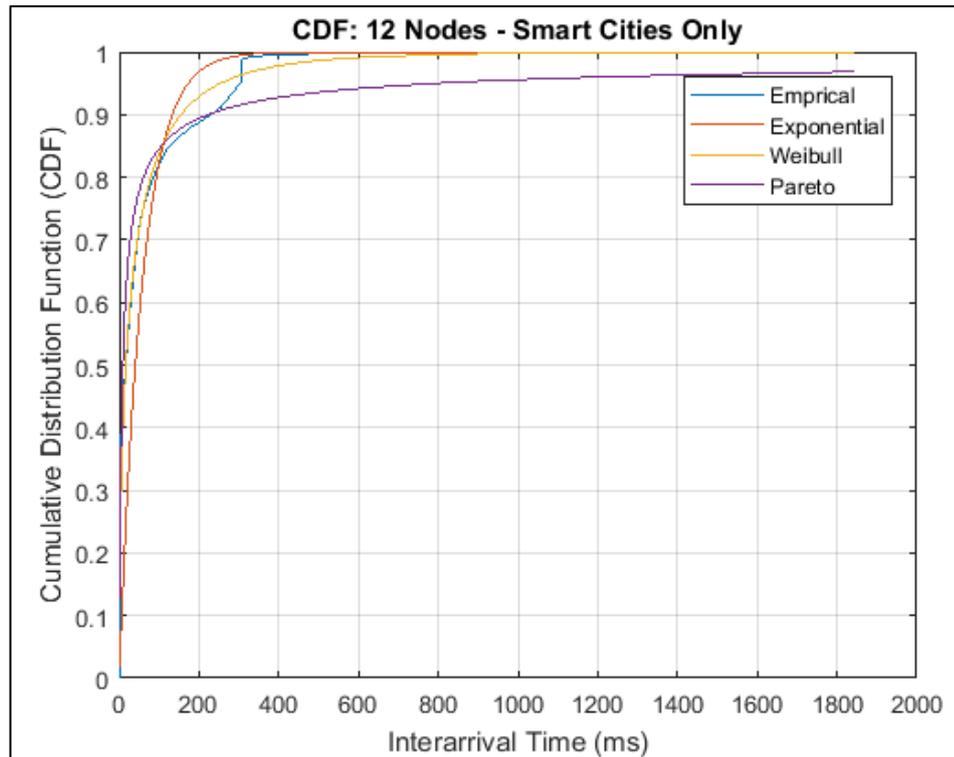


Figure 4.65: CDF of Inter-arrival Time for Pattern 7 & 12 Nodes

Table 4.29: Distributions' Parameters for Pattern 7 & 12 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	57.8475	1.8094	6.3578	0	32.2962	0.5321

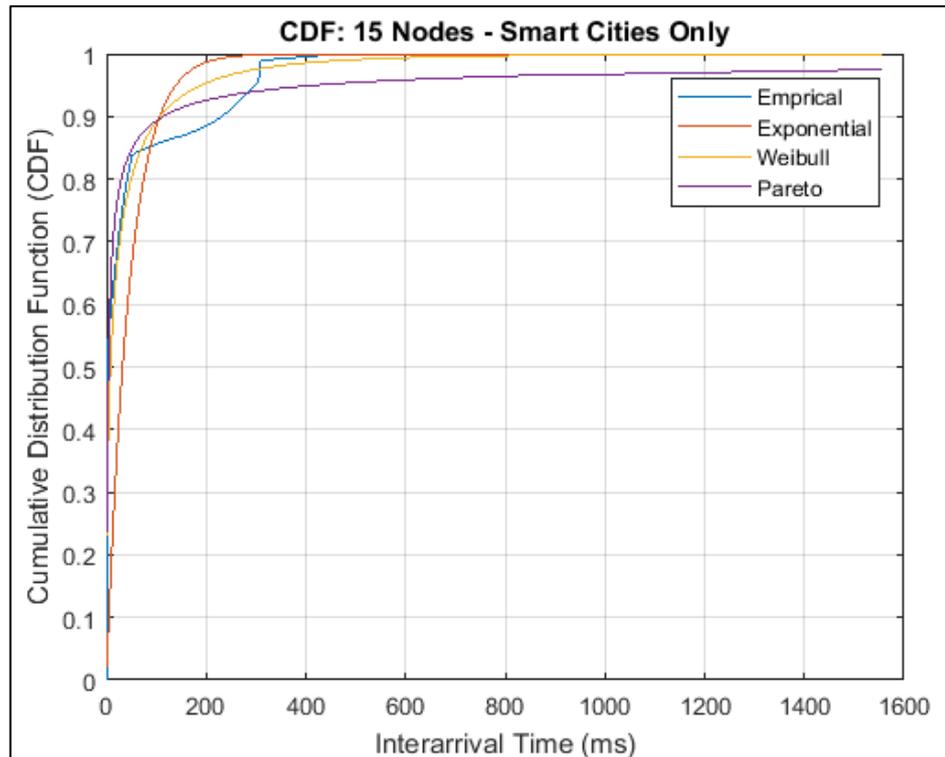


Figure 4.66: CDF of Inter-arrival Time for Pattern 7 & 15 Nodes

Table 4.30: Distributions' Parameters for Pattern 7 & 15 Nodes

Distribution	Exponential		Pareto		Weibull	
Parameter Name	Mean	Shape	Scale	Threshold	Scale	Shape
Parameter Value	46.4199	1.8807	2.8424	0	17.7821	0.4635

According to Figures 4.67, 4.68, 4.69, and 4.70, the Weibull distribution appears to be the best candidate regardless of the gateway traffic load. In case of 6, and 15 nodes, its average is the lowest while the standard deviation is very close to the lowest value (Pareto). When the gateway load is either 9 or 12 nodes, Weibull achieves the smallest average and standard deviation values of the absolute distribution distance.

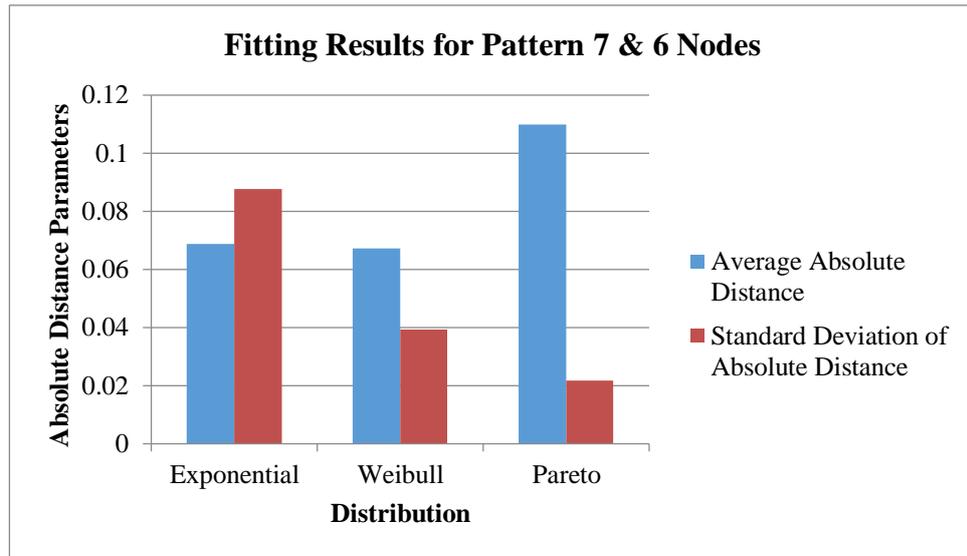


Figure 4.67: Distribution Fitting Results for Pattern 7 & 6 Nodes

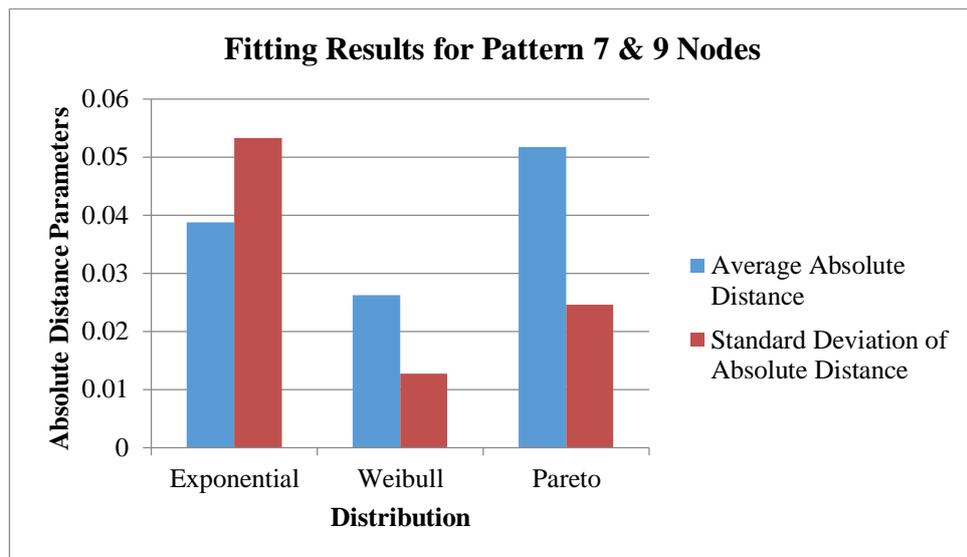


Figure 4.68: Distribution Fitting Results for Pattern 7 & 9 Nodes

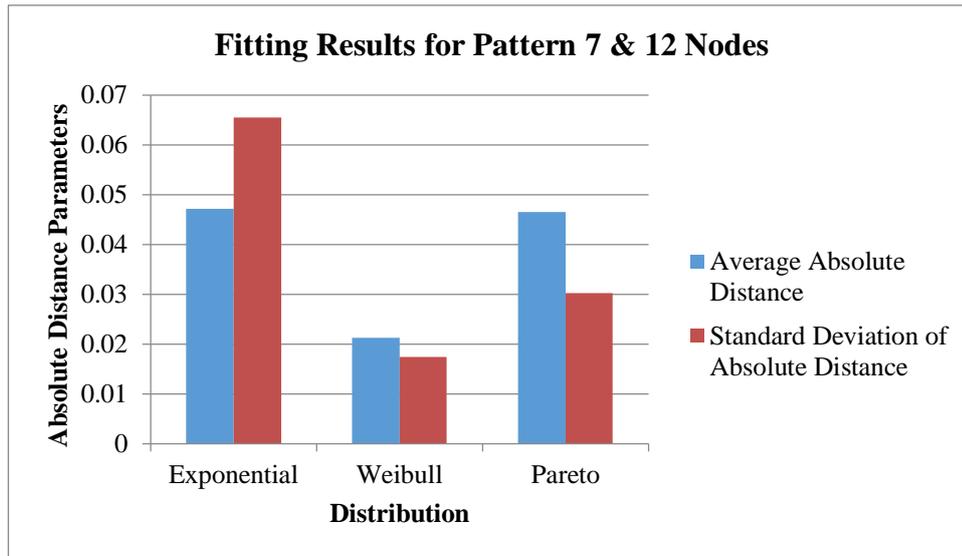


Figure 4.69: Distribution Fitting Results for Pattern 7 & 12 Nodes

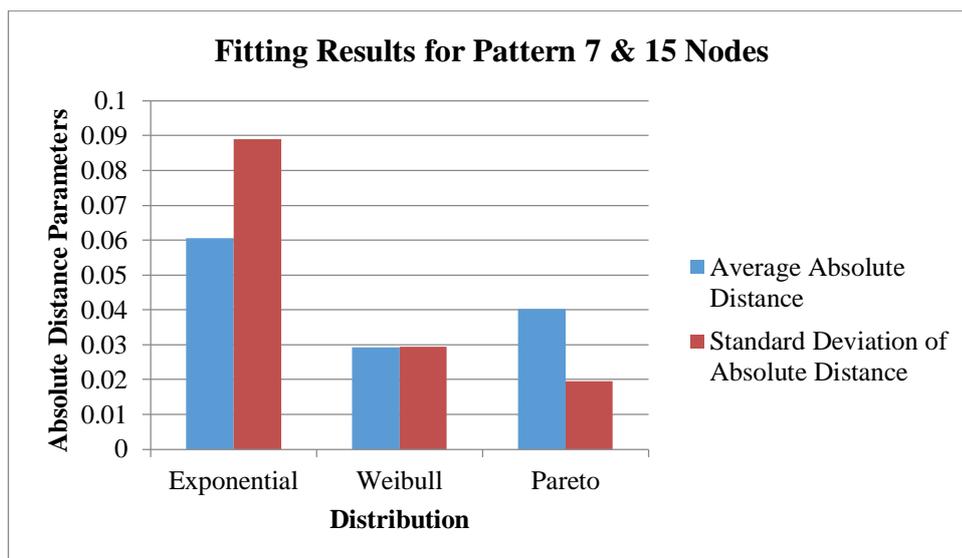


Figure 4.70: Distribution Fitting Results for Pattern 7 & 15 Nodes

4.2.2 IoT Packet Size Distribution

As mentioned before, the size of the generated packets varies over a range of different values. This actually depends on the type of the sensor, its precision, and the tested condition.

When the health of a normal person is monitored, there are 23 different packet sizes obtained from the ECG sensor. They are between 923 and 950 bytes. The packet length generated from monitoring the ECG of people with irregular heartbeat is to be expected within this range since only the heart rate is either faster or slower than a healthy normal heart but the range of the signal values remains the same [63].

Furthermore, the EMG sensor generates 10 different packet sizes in the range of 1042 to 1066 bytes. While the blood pressure sensor has only one size of 939 bytes because only 7 measurements are stored in its memory.

Using the Wasmote ASCII frame with certain decimal precision for each sensor, the light packets are either 76 or 77 bytes while the size of gases packets takes a value between 122 and 125 bytes. Moreover, there are only three different sizes obtained from the smart cities sensors, which are 113, 114, and 115 bytes.

Finally, the packets received from the surveillance camera are all in the size of 1358 bytes.

Admittedly, the IoT packet size is a random variable and its distribution is discrete. Furthermore, Geometric distribution is a discrete distribution that is commonly used for traffic characterization of networks other than IoT such as M2M [27].

In order to study the applicability of using the Geometric distribution to characterize the packet size distribution of the aggregate traffic of an IoT gateway, we have conducted the study in the sequel. For each previously mentioned traffic pattern with variable packet length, the CDF of a Geometric distribution is generated using a probability of success that is calculated based on the average of the empirical data. After that, the average and the standard deviation of absolute distribution distance between the CDF of the empirical and Geometric distribution are calculated to determine how far the empirical CDF from the Geometric CDF.

4.2.2.1 Traffic Pattern 1: Equal Percentage of the Three Applications

Figure 4.71 shows the CDF of empirical and Geometric distribution when the network load is distributed equally among the three applications. According to Figure 4.72, the absolute difference between the CDF of empirical and Geometric distribution is high. Its average reaches 0.4697 with standard deviation equals to 0.2726. It can be seen from Figure 4.71 that the difference is small for small packet sizes but it increases as the packet size gets higher.

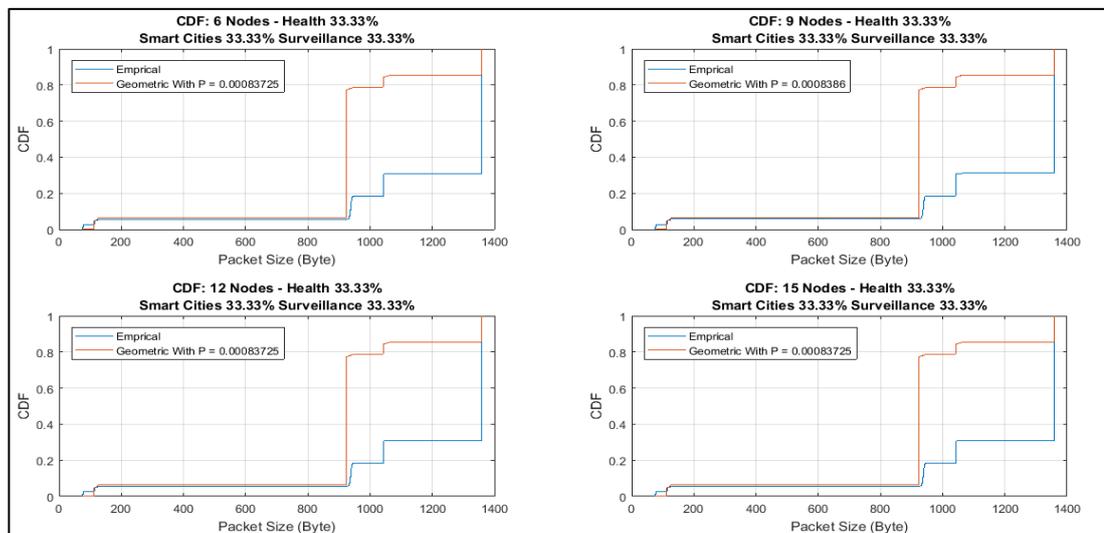


Figure 4.71: CDF of Packet Size for Pattern 1

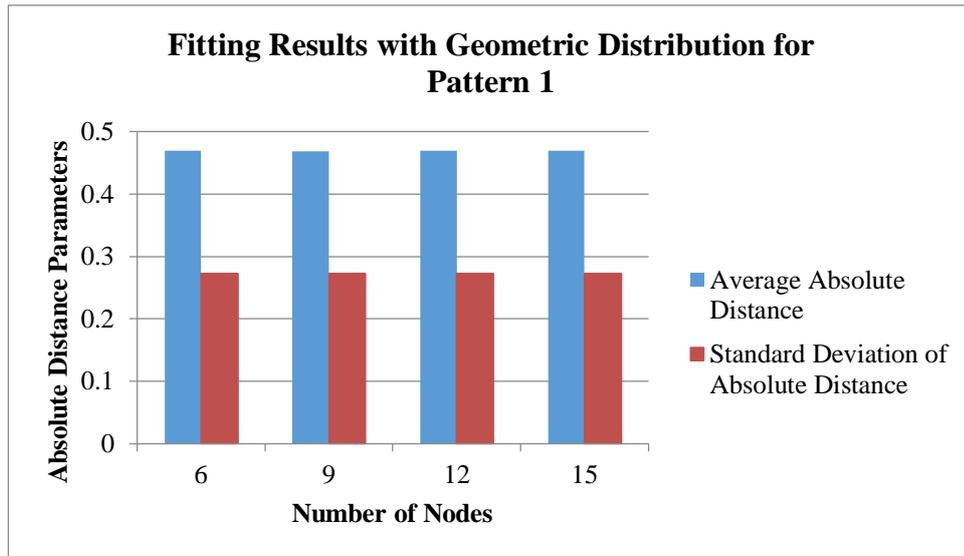


Figure 4.72: Comparison with Geometric Distribution for Pattern 1

4.2.2.2 Traffic Pattern 2: Higher Percentage of Healthcare Application

When the percentage of the healthcare application in the output traffic is the highest, the plots in Figure 4.73 indicate that the absolute distribution distance between empirical CDF is less farther from the Geometric CDF compared with Traffic Pattern 1. For this pattern, the minimum average and standard deviation of the absolute distance between the two CDFs are 0.3451 (for 9 nodes) and 0.2640 (for 6 and 12 nodes), respectively as revealed in Figure 4.74.

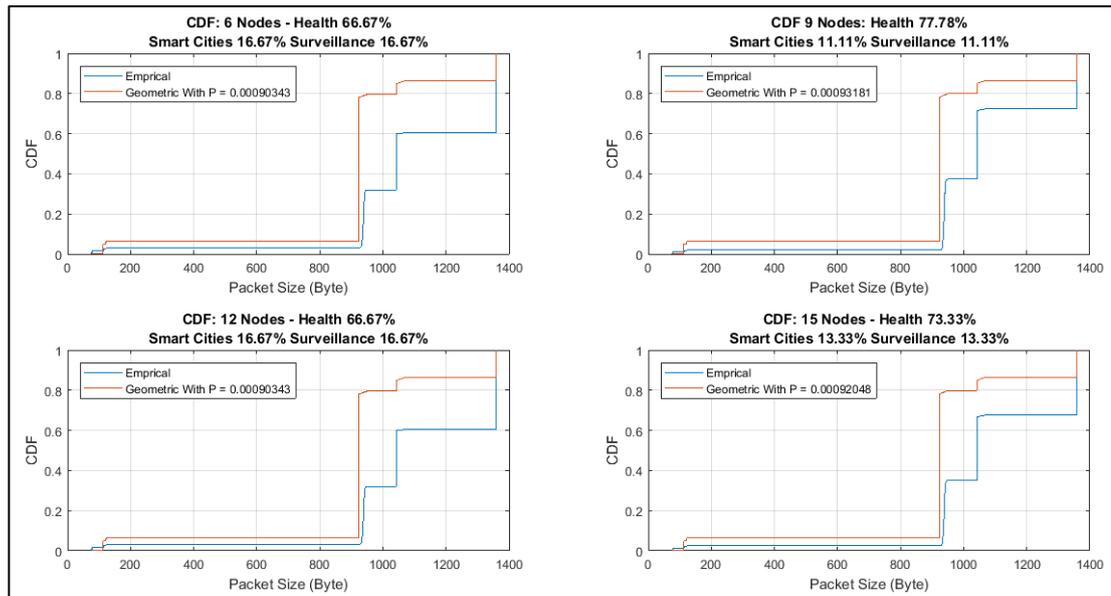


Figure 4.73: CDF of Packet Size for Pattern 2

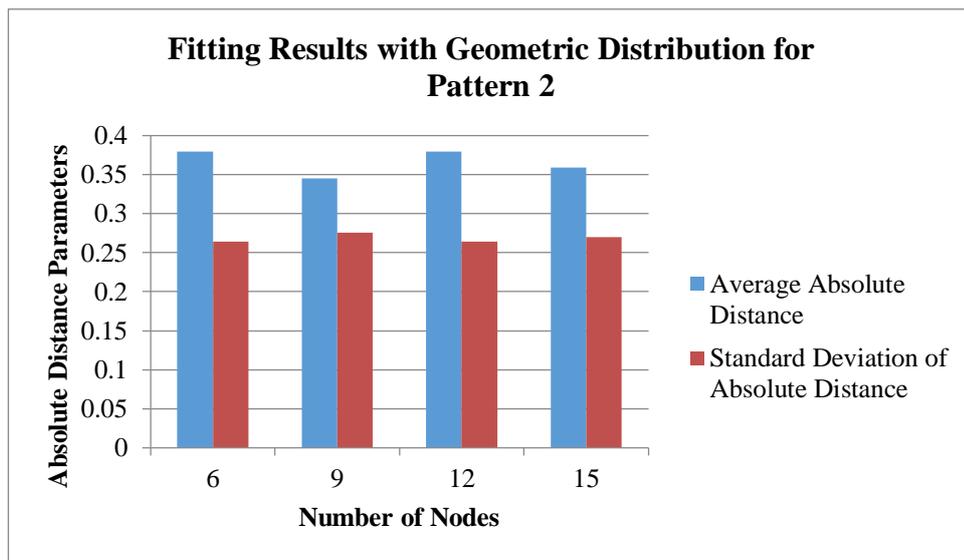


Figure 4.74: Comparison with Geometric Distribution for Pattern 2

4.2.2.3 Traffic Pattern 3: Higher Percentage of Smart Cities Application

Figures 4.75 and 4.76 show that when the majority of the traffic comes from smart cities sensors, Geometric distribution still cannot be used to describe the packet size traffic as the absolute distribution distance between the two CDFs are with high average and standard deviation.

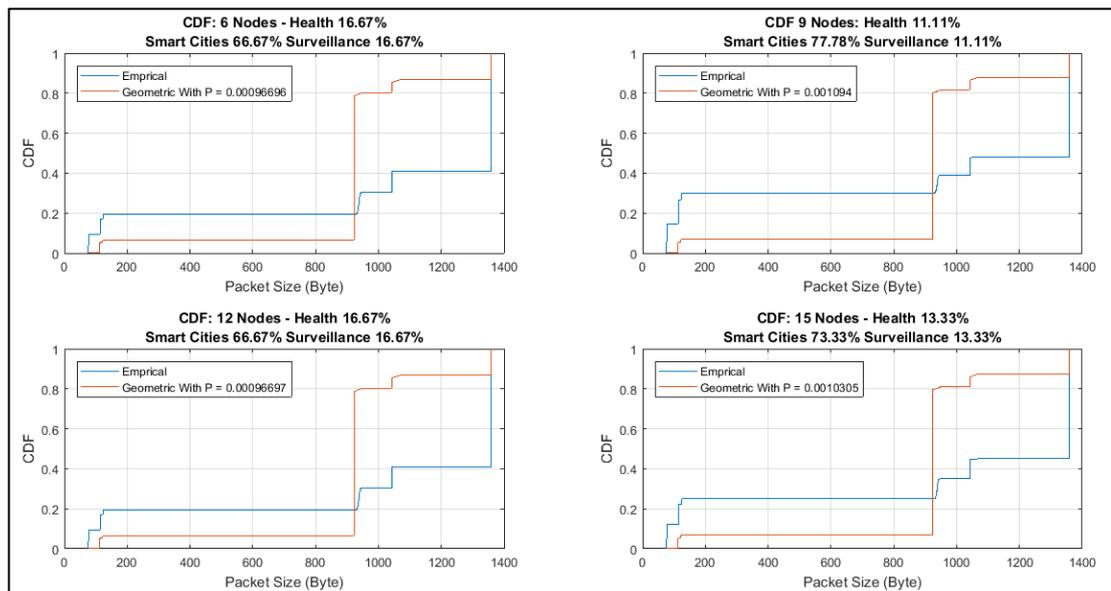


Figure 4.75: CDF of Packet Size for Pattern 3

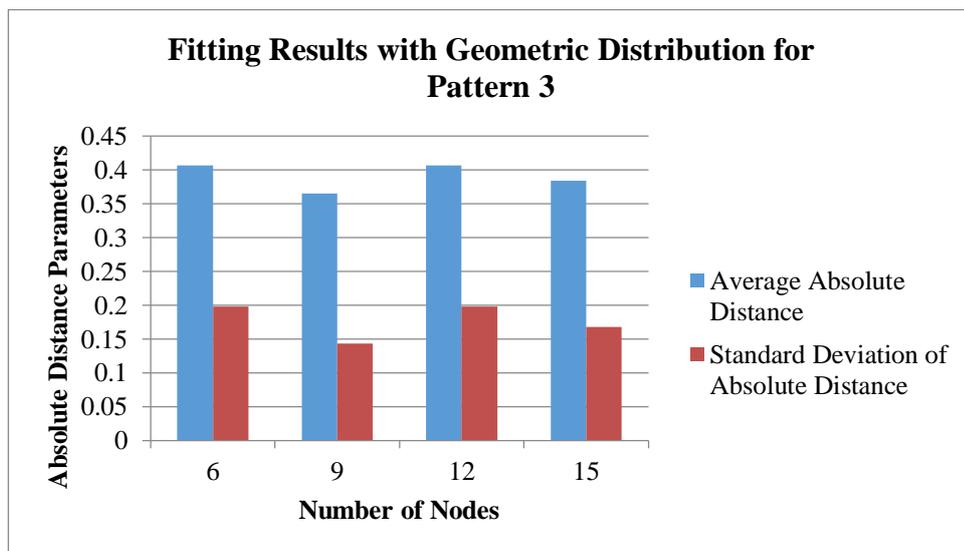


Figure 4.76: Comparison with Geometric Distribution for Pattern 3

4.2.2.4 Traffic Pattern 4: Higher Percentage of Video Surveillance Application

Figure 4.77 shows how far the empirical CDF from the Geometric CDF when the traffic is mostly video packets. This big difference is also numerically shown via the mean and the standard deviation as depicted in Figure 4.78.

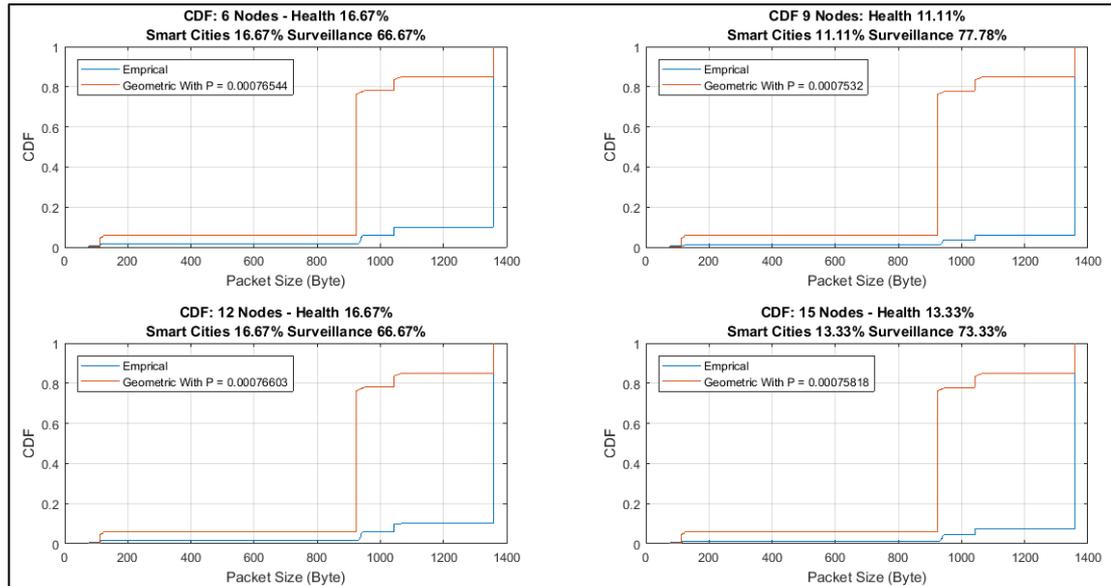


Figure 4.77: CDF of Packet Size for Pattern 4

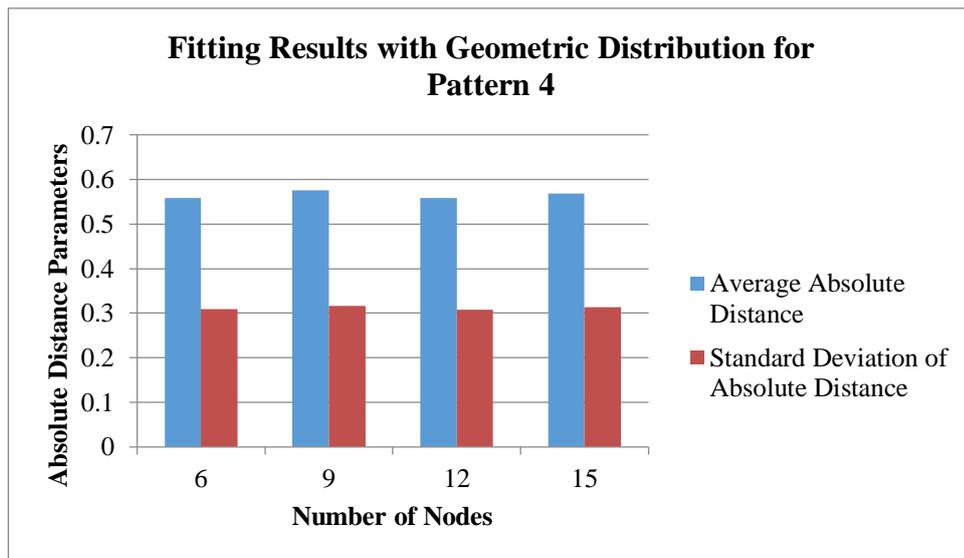


Figure 4.78: Comparison with Geometric Distribution for Pattern 4

4.2.2.5 Traffic Pattern 5: Healthcare Application only

Figure 4.79 shows the CDF of purely health traffic with the CDF of Geometric distribution with probability of success equals to 0.0010089. Figure 4.80 indicates that there is a difference between them. Therefore, Geometric distribution is not appropriate to model the packet size for this IoT traffic pattern.

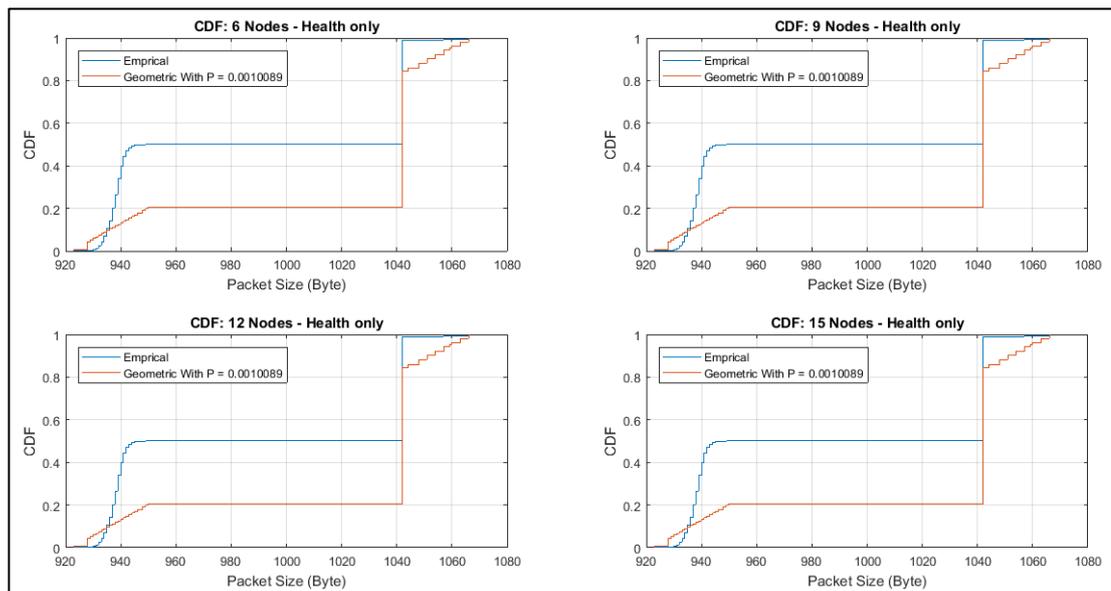


Figure 4.79: CDF of Packet Size for Pattern 5

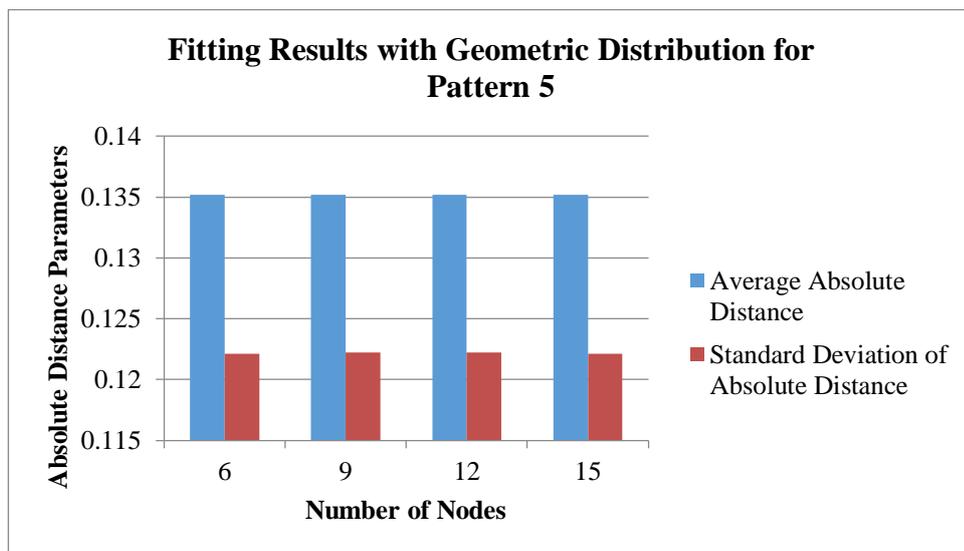


Figure 4.80: Comparison with Geometric Distribution for Pattern 5

4.2.2.6 Traffic Pattern 6: Smart Cities Application only

Figure 4.81 shows that this pattern is not close to Geometric distribution with p approximately equals to 0.010173. This is because the values of the average and the standard deviation of the absolute distance are high. In addition, Figure 4.82 shows graphically how far the CDFs from each other.

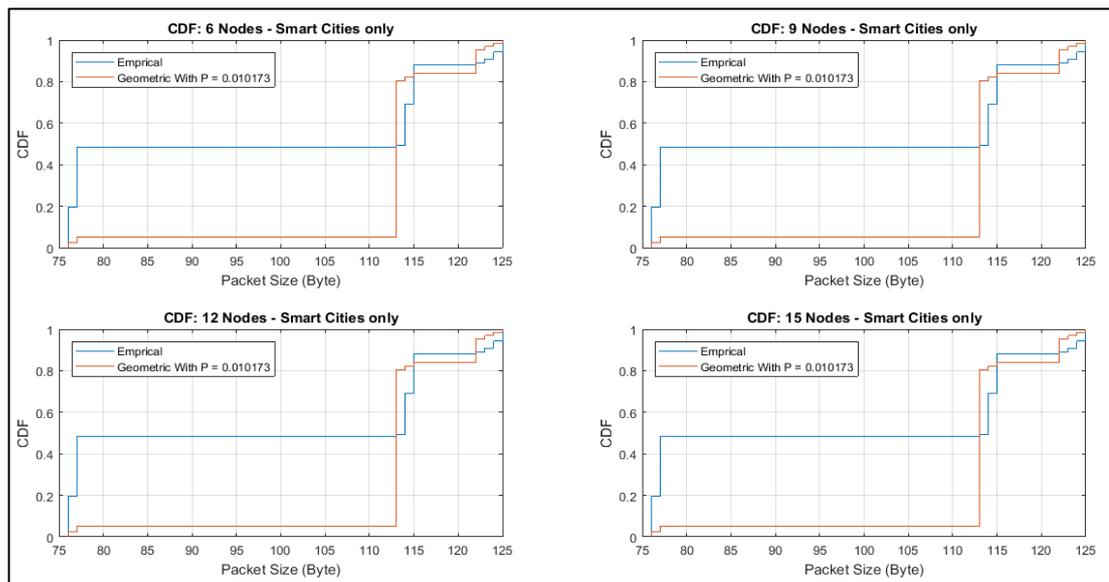


Figure 4.81: CDF of Packet Size for Pattern 6

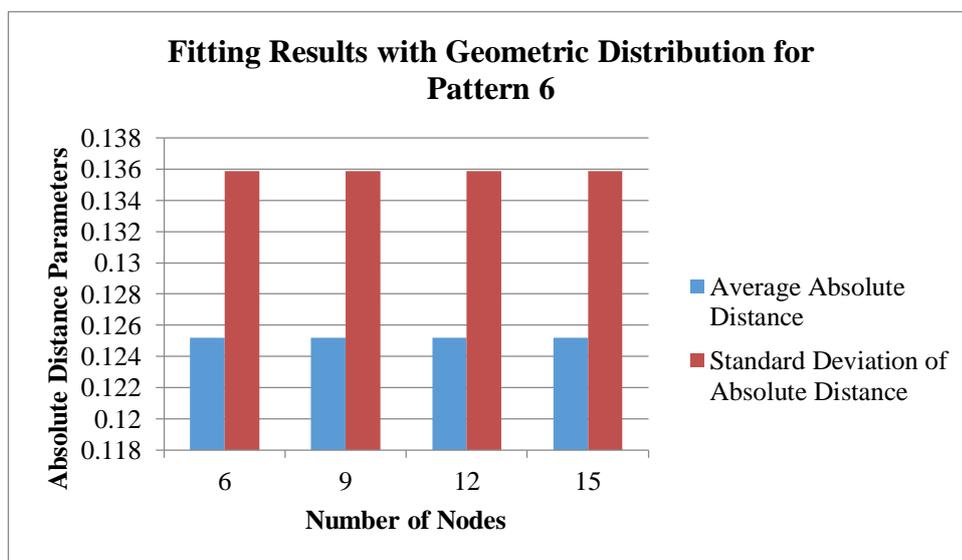


Figure 4.82: Comparison with Geometric Distribution for Pattern 6

In conclusion, the packet size of the observed patterns cannot be modeled accurately using Geometric distribution. Moreover, among the six studied patterns, pattern 5 and 6 have the least absolute distribution distance parameters while pattern 4 has the highest values. For each pattern, the difference between the empirical distribution and Geometric distribution is almost the same for all loads.

4.3 Impact of Traffic Characterization on Resource Allocation

Network Simulator 2 (NS2) is used in order to study the impact of traffic characterization on the network performance. NS2 is an open source discrete event simulation tool. It is a powerful research tool that supports simulating both wired and wireless networks [64].

Our aim is to show the influence of characterizing the IoT gateway packet inter-arrival time distribution by a commonly used distribution such as Exponential on an important metric such as end-to-end packet delay. In this study, we investigate the performance of a network of IoT gateways fed by an aggregate traffic of two selected traffic patterns (out of the seven traffic patterns studied in previous sections). The performance metric is the end-to-end packet delay.

In the simulation, a 100 x 100 m² flat topology is considered. The IoT gateways are uniformly distributed over the area. The gateways are communicating their data wirelessly using Wi-Fi to an AP. In addition, the traffic source model is varied (either to Exponential or to Pareto packet inter-arrival distribution) in order to examine the effect of these two distributions on packet delay given some number of IoT gateways. The simulation mimics a scenario where the network resources allocated to the IoT gateways are the same but the source traffic modeling is different.

Moreover, the parameters used in the simulation are obtained from the experimental results. The goal is to show how allocating resources given Poisson traffic is assumed (a common assumption in the literature) may lead to a completely different conclusion regarding the adequacy of these resources to satisfy certain end-to-end delay performance. Here, we consider the values of the average delay and delay jitter (the standard deviation of packet delay).

4.3.1 Traffic Pattern 1: Equal Percentage of the Three Applications

According to the experimental results, Pareto distribution is found to be the closest distribution to model the traffic generated by this scenario. In the simulation, the average packet size is set as 1225 bytes.

The graphs in Figures 4.83 and 4.84 show that the Poisson assumption generally underestimates the average packet delay and the delay jitter of the network. The figures also reveal that the difference is small when the number of IoT gateways is small since there is a plenty of network resources available in this case. However, as the number of IoT gateways increases, the difference in packet delay and delay jitter becomes very pronounced.

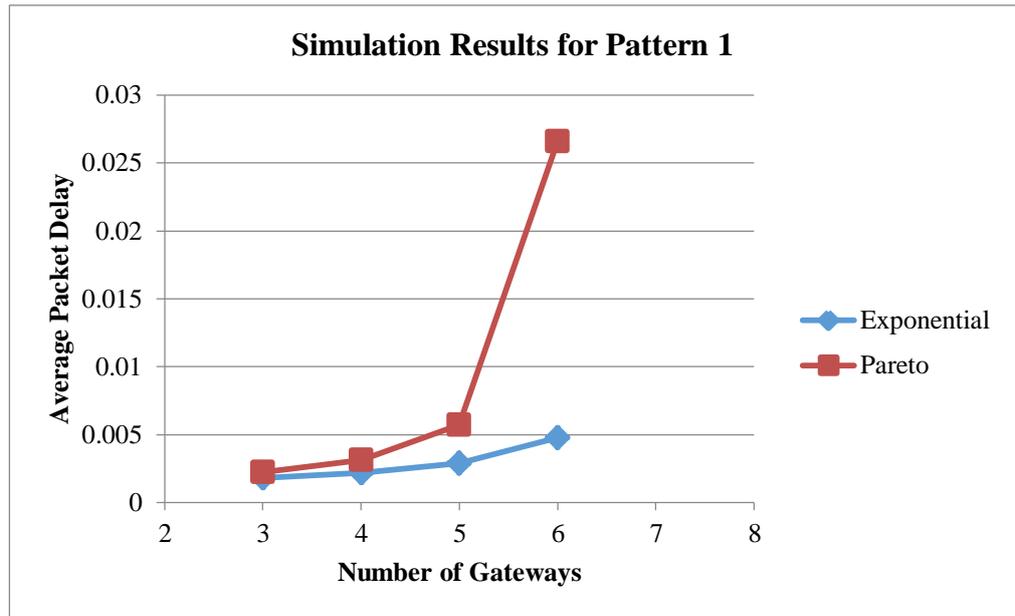


Figure 4.83: Average Packet Delay Performance Comparison for Pattern 1

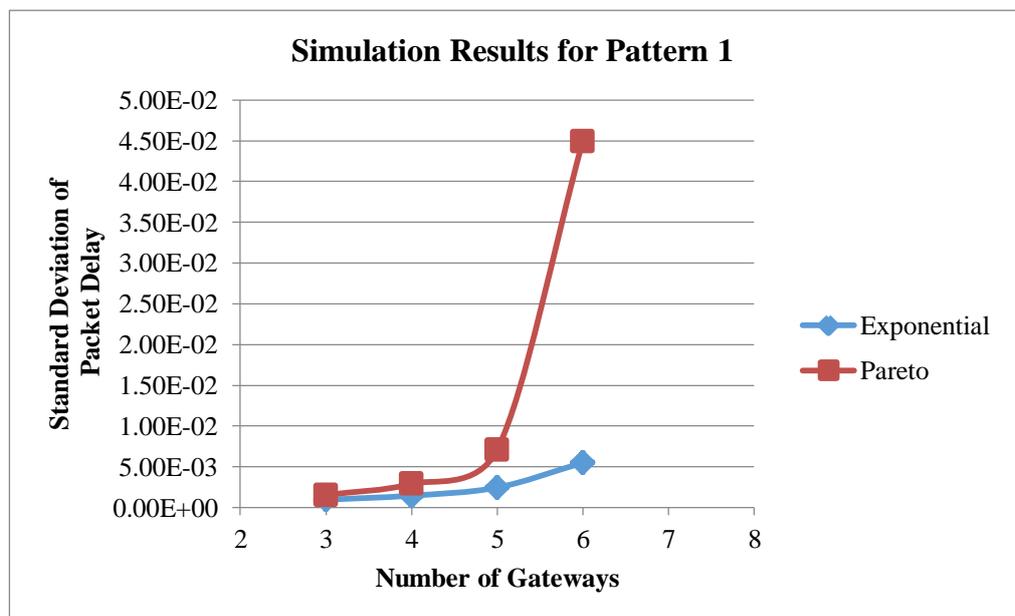


Figure 4.84: Delay Jitter Performance Comparison for Pattern 1

4.3.2 Traffic Pattern 2: Healthcare Application only

When the aggregated traffic is consisted of medical data only, the experimental results indicate that the Pareto distribution can accurately model this traffic pattern.

In the simulation, the packet size is constant (990 bytes). Figures 4.85 and 4.86 show a comparison for the average delay and delay jitter obtained from an exponentially distributed and Pareto distributed packet inter-arrival time. The results indicate that the packet delay and delay jitter of Poisson traffic are generally less than the average delay and packet jitter obtained by Pareto distributed inter-arrival time over the same range of the number network nodes observed in Traffic Pattern 1. This affirms the previous conclusion that Poisson traffic assumption underestimates packet delay and delay jitter given the same availability of network resources. In addition, the difference in the packet delay as well as the delay jitter between these distributions is very small for small number of nodes. For instance, in case of 4 nodes, the difference in average delay is 0.000077 for 4 nodes. However, the difference trend is growing with increasing the number of IoT gateways in the network.

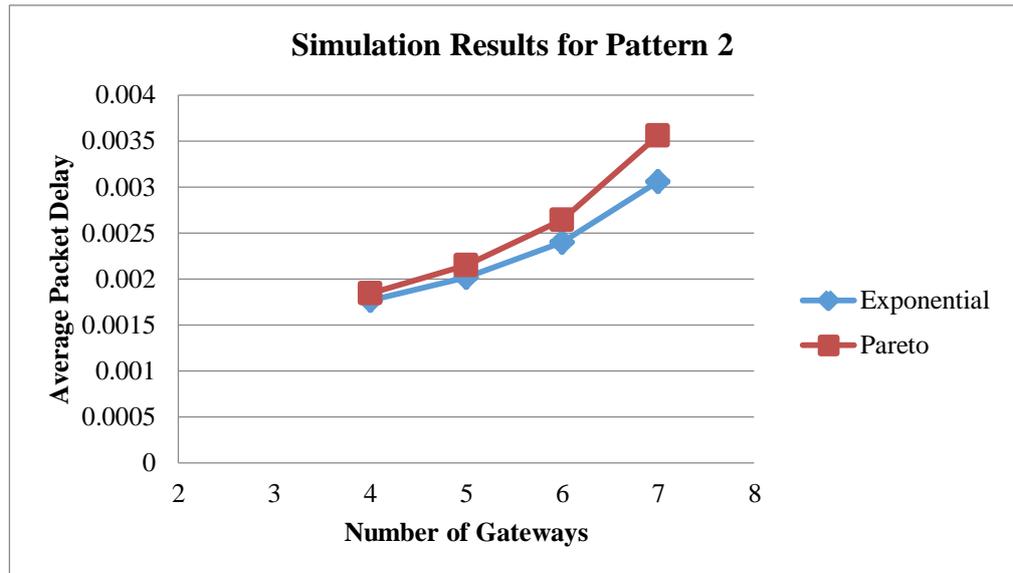


Figure 4.85: Average Packet Delay Performance Comparison for Pattern 2

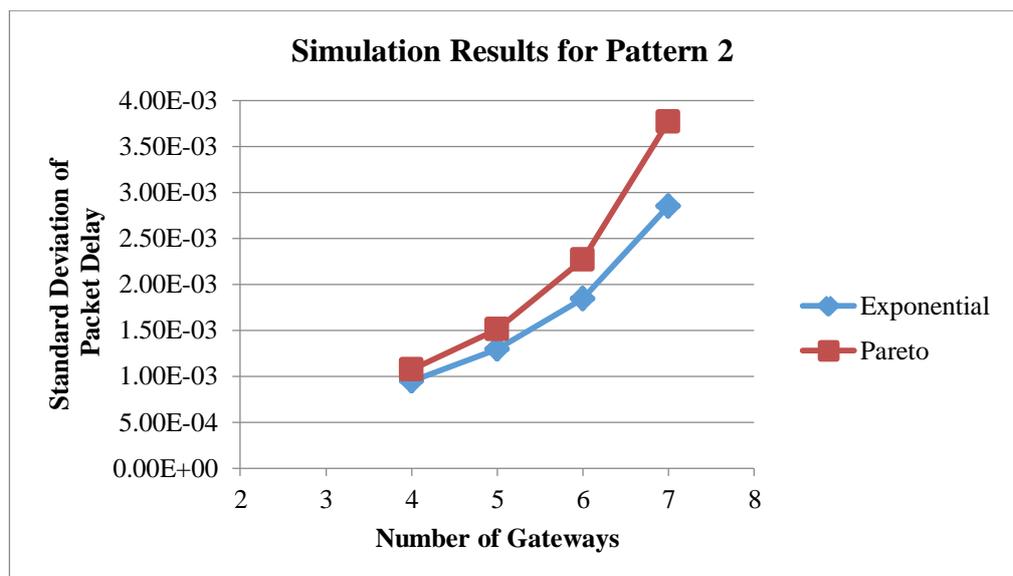


Figure 4.86: Delay Jitter Performance Comparison for Pattern 2

Chapter 5: Conclusion and Future Directions

IoT is a promising and an emerging paradigm. It allows the interaction between various heterogeneous devices through the Internet without the need for human intervention. Indeed, this concept will significantly enhance the quality of human life. In the near future, it will play a major role in a wide range of application domains, for example, transportation, healthcare, logistics, retails, security, emergency services, and smart cities.

Several challenges and issues are associated with this technology. Traffic characterization is among the challenges concerning the networking aspects. This is because IoT is still in its early stages and the traffic characteristics exchanged by various IoT objects are not precisely known. Moreover, for a network architecture, while the IoT traffic is aggregated at an IoT gateway is not yet sufficiently studied. In this thesis, we characterize the aggregated traffic of IoT gateways for three popular IoT-based applications, namely, healthcare, smart cities, and video surveillance.

The study is conducted experimentally in a lab. First, real IoT data with real- and non-real-time requirements are collected from different medical, smart cities and surveillance sources. These data are encapsulated in UDP packets and wirelessly transported through Wi-Fi interface to an IoT gateway. The input traffic to this gateway is modeled. The experiment is conducted for four different sets of gateway loads (i.e., different number of IoT devices sending their data traffic to the gateway). For each load, seven different traffic patterns of the selected applications are observed.

The empirical packet inter-arrival time distribution is matched using a set of goodness-of-fit tests and other statistical analysis. Our experimental results reveal the following:

- When IoT network contains traffic of equal percentage of the three applications, Pareto distribution is found to be the closest to the empirical data for all loads.
- In case the majority of the aggregated traffic is health data, it is found that this traffic follows Weibull distribution for relatively small gateway load (6 IoT devices). For a larger amount of gateway load, the distribution function of the empirical data best fits Pareto distribution.
- When the penetration of smart cities or video surveillance traffic is the highest in the aggregated traffic, the results show that Pareto is the best distribution to model the packet inter-arrival time regardless of the IoT gateway load.
- When the traffic is only generated from surveillance cameras, Pareto distribution is found to model this traffic pattern for relatively low to moderate gateway load (6 to 9 devices). However, Weibull distribution better models this pattern as the traffic load increases.
- When the aggregated traffic is purely health, Pareto is found to be the best distribution to model this scenario irrespective of the IoT gateway traffic load.

- The characteristics of smart cities traffic can be accurately modeled using Weibull distribution compared to Exponential or Pareto distributions.

According to our empirical data considered in this study, we found that Pareto distribution can satisfactorily model the empirical packet inter-arrival time distribution of the different traffic patterns.

Furthermore, the comparison between our empirical distribution of packet size and Geometric distribution indicates that the packet size of the studied IoT applications cannot be properly modeled by Geometric distribution as the absolute distribution distance parameters are high.

Beside the experimental work, NS2 simulator is used to investigate the impact of traffic characterization on the performance of the considered IoT network architecture. The simulation results reveal that there will be an underestimation for the average packet delay and delay jitter if a traffic pattern best matched with Pareto packet inter-arrival time distribution is modeled as Poisson traffic, which is a common traffic model used in many analytical studies.

In the future, we plan to propose an efficient resource allocation scheme for the considered IoT network architecture. In addition, a performance study will be conducted in order to evaluate the efficiency of the suggested solutions.

References

- [1] R. Buyya, S. Marusic, M. Palaniswami, and J. Gubbi, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, 2013.
- [2] S. Sicari, F. De Pellegrini, I. Chlamtac, and D. Miorandi, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497-1516, 2012.
- [3] A. Iera, G. Morabito, and L. Atzori, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787-2805, 2010.
- [4] P. Rajalakshmi, K. Bharadwaj, A. Acharyya, and M. P. R. S. Kiran, "Adaptive rule engine based IoT enabled remote health care data acquisition and smart transmission system," *014 IEEE World Forum on Internet of Things (WF-IoT)*, pp. 253-258, 2014.
- [5] F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, S. Guizani, and Y. Mehmood, "Internet-of-Things-Based Smart Cities: Recent Advances and Challenges," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16-24, 2017.
- [6] I. Yaqoob, and S. H. Shah, "A survey: Internet of Things (IOT) technologies, applications and challenges," *2016 IEEE Smart Energy Grid Engineering (SEGE)*, pp. 381-385, 2016.
- [7] W. De Donato, V. Persico, A. Pescapé, and A. Botta, "Integration of Cloud computing and Internet of Things : A survey," *Future Generation Computer Systems*, vol. 56, pp. 684-700, 2016.
- [8] Z. Baig, O. Bello, S. Zeadally, and M. Chernyshev, "Internet of Things (IoT): Research, Simulators, and Testbeds," *IEEE Internet of Things Journal*, vol. 4662, pp. 1-11, 2017.
- [9] J. Eksteen, and L. Coetzee, "The Internet of Things - promise for the future? An introduction," *IST-Africa Conference Proceedings, 2011*, pp. 1-9, 2011.
- [10] B. Pant, M. Arora, and P. Matta, "All you want to know about Internet of Things (IoT)," *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 1306-1311, 2017.
- [11] V. Bhuvaneswari, and R. Porkodi, "The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview," *2014*

- International Conference on Intelligent Computing Applications*, pp. 324-329, 2014.
- [12] D. Azariadi, V. Tsoutsouras, S. Xydis, and D. Soudris, "ECG signal analysis and arrhythmia detection on IoT wearable medical devices," *2016 5th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, pp. 1-4, 2016.
- [13] D. Kwak, H. Kabir, M. Hossain, K.-S. Kwak, and S. M. R. Islam, "The Internet of Things for Health Care : A Comprehensive Survey," *Access, IEEE*, vol. 3, pp. 678 - 708, 2015.
- [14] P. Tuwanut, and S. Kraijak, "A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends," *1th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015)*, pp. 1-6, 2015.
- [15] W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, and J. Lin, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, October 2017.
- [16] O. Said, and M. Masud, "Towards internet of things: Survey and future vision," *International Journal of Computer Networks*, vol. 5, no. 1, pp. 1-17, 2013.
- [17] O. Alsaryrah, T. Y. Chung, C. Z. Yang, W. H. Kuo, D. P. Agrawal, and I. Mashal, "Choices for interaction with things on Internet and underlying issues," *Ad Hoc Networks*, vol. 28, pp. 68-90, 2015.
- [18] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, "Research on the architecture of Internet of Things," *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICAETE)*, vol. 5, pp. 484-487, 2010.
- [19] S. U. Khan, R. Zaheer, S. Khan, and R. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," *2012 10th International Conference on Frontiers of Information Technology*, pp. 257-260, 2012.
- [20] H. Bidgoli, "Network Traffic Modeling," in *The Handbook of Computer Networks.*: John Wiley & Sons, 2004, pp. 1-46.
- [21] R. Renikunta, R. Dasari, M. R. Perati, and R. Donthi, "Performance Analysis of Internet Switch with Variable Length Packet Input Traffic using Circulant Markov Modulated Poisson Process (CMMPP)," *Proceedings of 3rd*

International Conference on Reliability, Infocom Technologies and Optimization, pp. 1-5, 2014.

- [22] A. Adas, "Traffic models in broadband networks," *IEEE Communications Magazine*, vol. 35, pp. 82-89, 1997.
- [23] A. Florence, C. Benjamin, C. Cletus, M. Folasade, and O. Harrison, "The Desirability of Pareto Distribution for Modeling Modern Internet Traffic Characteristics," *International Journal of Novel Research in Engineering and Applied Sciences (IJNREAS)*, vol. 1, no. February, pp. 2-9, 2014.
- [24] B. Chandrasekaran, "Survey of Network Traffic Models," *Bernoulli*, pp. 1-8, 2009.
- [25] J. Mohorko, Z. Cucej, and M. Fras, "A new goodness of fit test for histograms regarding network traffic packet size process," *2008 International Conference on Advanced Technologies for Communications*, pp. 345-348, 2008.
- [26] M. Wilson, "A Historical View of Network Traffic Models," *IEE Technical Report on Traffic*, pp. 1-15, 2005.
- [27] A. Abdelhadim, C. Clancy, and A. Kumar, "A Delay Efficient MAC and Packet Scheduler for Heterogeneous M2M Uplink," *IEEE Globecom Workshops (GC Wkshps)*, pp. 1-5, 2016.
- [28] A. T. Koc, M. Gupta, R. Vannithamby, and S. C. Jha, "Power Saving mechanisms for M2M communication over LTE networks," *First International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 102-106, 2013.
- [29] B. Vejlggaard, N. Mangalvedhe, A. Ghosh, and R. Ratasuk, "NB-IoT system for M2M communication," *IEEE Wireless Communications and Networking Conference*, pp. 1-5, 2016.
- [30] K. Pawlikowski, D. McNickle, A. Willig, and M. A. Arfeen, "The role of the Weibull distribution in Internet traffic modeling," *Proceedings of the 2013 25th International Teletraffic Congress (ITC)*, pp. 1-8, 2013.
- [31] A. Sivanathan et al., "Characterizing and classifying IoT traffic in smart cities and campuses," *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 559-564, 2017.
- [32] M. Z. Shafiq et al., "A First Look at Cellular Machine-to-Machine Traffic: Large Scale Measurement and Characterization," *Proc. ACM Sigmetrics*, 2012.

- [33] K. Ghavami, M. Naraghi-Pour, and E. Soltanmohammadi, "A survey of traffic issues in machine-to-machine communications over LTE," *IEEE Internet of Things Journal*, vol. 3, pp. 865-884, December 2016.
- [34] F. Metzger, P. Heegaard, and T. Hossfeld, "Traffic Modeling for Aggregated Periodic IoT Data," *21st International Conference on Innovation in Clouds, Internet and Networks (ICIN 2018)*, 2018.
- [35] 3GPP, "Study on RAN Improvements for Machine-type," Technical Report TR 37.868, September 2011.
- [36] P. Svoboda, N. Nikaein, M. Rupp, and M. Laner, "Traffic Models for Machine Type Communications," *SWCS 2013; The Tenth International Symposium on Wireless Communication Systems*, pp. 1-5, August 2013.
- [37] 3GPP, "Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT)," Technical Report TR 45.820, 2015.
- [38] T. Zhang, and Q. Wang, "Source Traffic Modelling in Wireless Sensor Networks for Target Tracking," *5th ACM International Symposium on Performance Evaluation of Wireless*, October 2008.
- [39] A. Feldmann, "Characteristics of TCP Connection Arrivals," in *Self-Similar Network Traffic and Performance Evaluation.: Self-Similar Network Traffic and Performance Evaluation*, John Wiley & Sons, Inc., 2002, pp. 367-399.
- [40] V. Tsoutsouras, S. Xydis, D. Soudris, and D. Azariadi, "ECG signal analysis and arrhythmia detection on IoT wearable medical devices," *2016 5th International Conference on Modern Circuits and Systems Technologies, MOCAS 2016*, pp. 1-4, 2016.
- [41] Y. Zhang, Z. Zhang, Y. Fang, H. Liu, and H. Chen, "Exploring the Relation between EMG Sampling Frequency and Hand Motion Recognition Accuracy," *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 1139-1144, 2017.
- [42] B. Singh, V. K. Banga, and M. Singh, "Effect of ECG sampling frequency on approximate entropy based HRV," *International Journal of Bio-Science and Bio-Technology*, vol. 6, no. 4, pp. 179-186, 2014.
- [43] M. H. Amaran, Y. M. Yusoff, R. A. Rahman, H. Hashim, and M. Masirap, "Evaluation of reliable UDP-based transport protocols for Internet of Things (IoT)," *IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, pp. 200-205, 2016.

- [44] B. Rinner, L. Marcenaro, and S. Ullah, "Smart cameras with onboard signcryption for securing IoT applications," *GIoTS 2017 - Global Internet of Things Summit, Proceedings*, pp. 1-6, 2017.
- [45] B. J. Silva, G. P. Hancke, A. M. Abu-Mahfouz, and G. A. Akpakwu, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*, vol. 6, pp. 3619-3647, 2018.
- [46] S. K. Devar, N. H. Kumar, K. P. Bagadi, and V. Gupta, "Modelling of IoT Traffic and its Impact on LoRaWAN," *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pp. 1-6, 2017.
- [47] B. S. B. Praveen, A. V. S. Reddy, B. B. Sam, and N. V. R. Kumar, "Study on IOT with reference of M2M and WiFi," *2017 International Conference on Information Communication and Embedded Systems, (ICICES)*, pp. 1-6, 2017.
- [48] S. Banerji, and R. S. Chowdhury, "On IEEE 802.11: Wireless Lan Technology," *International Journal of Mobile Network Communications & Telematics*, vol. 3, no. 4, pp. 45-64, 2013.
- [49] "Wi-Fi : Overview of the 802.11 Physical Layer and Transmitter Measurements". [Online]. [Accessed: February 24, 2018].
- [50] A. Heng, "Bit-Twist". [Online]. Available: <http://bittwist.sourceforge.net/index.html>. [Accessed: March 19, 2018].
- [51] "Arduino - IntelGalileo". [Online]. Available: <https://www.arduino.cc/en/ArduinoCertified/IntelGalileo>. [Accessed: February 2, 2018].
- [52] "Wasp mote - Wireless Sensor Networks Open Source Platform". [Online]. Available: <https://www.arduino.cc/en/ArduinoCertified/IntelGalileo>. [Accessed: February 10, 2018].
- [53] S. Solak, E. D. Bolat, and O. Yakut, "Measuring ECG Signal Using e-Health Sensor Platform," *International Conference on Chemistry, Biomedical and Environment Engineering*, pp. 65-69, 2014.
- [54] "e-Health Sensor Platform V2.0 for Arduino and Raspberry Pi [Biometric / Medical Applications]". [Online]. Available: <https://www.cooking-hacks.com/documentation/tutorials/ehealth-biometric-sensor-platform-arduino-raspberry-pi-medical>. [Accessed: January 30, 2018].
- [55] "Smart Cities PRO Technical Guide". [Online]. Available: <http://www.libelium.com/v11-files/documentation/waspote/smart-cities->

sensor-board_eng.pdf. [Accessed: February 10, 2018].

- [56] "Smart Gases 3.0. Technical Guide". [Online]. Available: <http://www.libelium.com/development/waspmote/documentation/gases-board-technical-guide/>. [Accessed: February 10, 2018].
- [57] "Sensors: Proceedings of the Second National Conference on Sensors, Rome 19-21 February, 2014," in *Dario Compagnone, Francesco Baldini, Corrado Di Natale, Giovanni Betta, Pietro Siciliano*. Cham: Springer International Publishing, 2015, p. 453.
- [58] "Waspmote Data Frame Programming Guide". [Online]. Available: http://www.libelium.com/downloads/documentation/data_frame_guide.pdf. [Accessed: February 13, 2018].
- [59] "I2CXL-MaxSonar". [Online]. Available: https://www.maxbotix.com/documents/I2CXL-MaxSonar-EZ_Datasheet.pdf. [Accessed: March 18, 2018].
- [60] "DCS-930L - Wireless N Network Camera". [Online]. Available: <http://www.dlink.com/uk/en/products/dcs-930l-wireless-n-network-camera>. [Accessed: January 30, 2018].
- [61] N. Cackov, S. Vujicic, L. Trajkovic, and B. Vujicic, "Modeling and characterization of traffic in public safety wireless networks," *SPECTS*, pp. 214–223, 2005.
- [62] J. Emerson, and T. Arnold, "Nonparametric Goodness-of-Fit Tests for Discrete Null Distributions," *The R Journal*, pp. 34-39, December 2011.
- [63] R. Plonsey, and J. Malmivuo, "The Basis of ECG Diagnosis," in *Bioelectromagnetism.*, 1995, pp. 437-457.
- [64] I. Haddad, and D. Gordon, "Network Simulator 2: a Simulation Tool for Linux". [Online]. Available: <http://www.linuxjournal.com/article/5929>. [Accessed: March 20, 2018].