



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**PERFORMANCE ANALYSIS OF AN UNMANNED SYSTEMS
COMMUNICATIONS NETWORK USING DATA
DISTRIBUTION SERVICE IN A LOSSY ENVIRONMENT**

by

Yu Kheng Denny Cheng

March 2021

Thesis Advisor:
Second Reader:

Preetha Thulasiraman
Brian S. Bingham

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE March 2021	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE PERFORMANCE ANALYSIS OF AN UNMANNED SYSTEMS COMMUNICATIONS NETWORK USING DATA DISTRIBUTION SERVICE IN A LOSSY ENVIRONMENT			5. FUNDING NUMBERS	
6. AUTHOR(S) Yu Kheng Denny Cheng				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The Ship Integration Program Office (PMW760) is interested in the prospect of having a unified, cohesive communications protocol that can be used by all unmanned systems under their purview. The Data Distribution Service (DDS) is a prime candidate for such cohesive communications using point-to-point links. The objective of this thesis is to assess the performance of DDS in a network architecture that fits the naval use case criteria. We propose a network architecture that incorporates Satellite Communications (SATCOM) and Wireless Fidelity (WiFi) links to test the ability of DDS to execute cohesive communications between the network nodes within constraints of the scenario setup. We use a network emulator, Mininet, to set up the network parameters and investigate the throughput and latency performance of the individual point-to-point links across various data sample sizes. Simulations are conducted to measure throughput and latency under different network configurations (Ideal, Jitter and Multi-Flow) using the Real-Time Innovation PerfTest software tool. For the Ideal and Jitter configurations, the simulations are performed for RELIABLE and BEST EFFORT communications as well as with and without implementation of DDS security. We also conduct simulations in the Multi-Flow configurations to evaluate how simultaneous multi-flow data (traffic data running in parallel within the network nodes) contend for the network resources and impact performance.				
14. SUBJECT TERMS DDS, Mininet, SATCOM, WiFi, throughput, latency, unmanned systems			15. NUMBER OF PAGES 109	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**PERFORMANCE ANALYSIS OF AN UNMANNED SYSTEMS
COMMUNICATIONS NETWORK USING DATA DISTRIBUTION SERVICE IN
A LOSSY ENVIRONMENT**

Yu Kheng Denny Cheng
ME5, Republic of Singapore Navy
Bachelor of Engineering (Electrical and Electronic Engineering),
Nanyang Technological University, 2010

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

**NAVAL POSTGRADUATE SCHOOL
March 2021**

Approved by: Preetha Thulasiraman
Advisor

Brian S. Bingham
Second Reader

Douglas J. Fouts
Chair, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Ship Integration Program Office (PMW760) is interested in the prospect of having a unified, cohesive communications protocol that can be used by all unmanned systems under their purview. The Data Distribution Service (DDS) is a prime candidate for such cohesive communications using point-to-point links. The objective of this thesis is to assess the performance of DDS in a network architecture that fits the naval use case criteria. We propose a network architecture that incorporates Satellite Communications (SATCOM) and Wireless Fidelity (WiFi) links to test the ability of DDS to execute cohesive communications between the network nodes within constraints of the scenario setup. We use a network emulator, Mininet, to set up the network parameters and investigate the throughput and latency performance of the individual point-to-point links across various data sample sizes. Simulations are conducted to measure throughput and latency under different network configurations (Ideal, Jitter and Multi-Flow) using the Real-Time Innovation Perfctest software tool. For the Ideal and Jitter configurations, the simulations are performed for RELIABLE and BEST EFFORT communications as well as with and without implementation of DDS security. We also conduct simulations in the Multi-Flow configurations to evaluate how simultaneous multi-flow data (traffic data running in parallel within the network nodes) contend for the network resources and impact performance.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	THESIS CONTRIBUTIONS	2
B.	THESIS ORGANIZATION	3
II.	BACKGROUND AND RELATED WORK.....	5
A.	MININET.....	5
1.	Overview of Mininet	5
2.	Operations of Mininet.....	6
3.	Limitations of Mininet.....	6
B.	DDS.....	7
1.	Overview of DDS.....	7
2.	Operations of DDS	10
3.	Overview of DDS Security.....	11
4.	Vulnerabilities of DDS.....	12
5.	Performance of DDS	14
C.	RTI PERFTEST.....	15
1.	Throughput Test	15
2.	Latency Test	16
3.	Options for DDS Security.....	16
III.	PROPOSED NETWORK ARCHITECTURE AND SIMULATION	
	SETUP.....	19
A.	PROPOSED NETWORK ARCHITECTURE AND SCENARIO	
	SETUP.....	19
B.	OVERVIEW OF APPROACH TO SIMULATION RUNS.....	21
C.	SELECTION OF MININET PARAMETERS.....	26
D.	SELECTION OF RTI PERFTEST PARAMETERS.....	28
1.	QoS Profiles	28
2.	Execution Time.....	28
3.	Transmission Mode.....	28
4.	Transport Mode	28
5.	Batching	28
6.	Send Queue Size	29
7.	Publishing Rate and Delay Method.....	29
8.	Security	29
E.	SIMULATION HARDWARE AND SOFTWARE	
	SPECIFICATIONS.....	29

IV.	SIMULATION RESULTS AND ANALYSIS	31
A.	IDEAL CONFIGURATION	33
1.	Throughput Test Results (RELIABLE).....	33
2.	Latency Test Results (RELIABLE).....	34
3.	Throughput Test Results (BEST EFFORT at PubRate 100 Hz)	35
4.	Latency Test Results (BEST EFFORT at PubRate 100 Hz)	36
B.	JITTER CONFIGURATION	37
1.	Throughput Test Results (RELIABLE).....	37
2.	Latency Test Results (RELIABLE).....	40
3.	Throughput Test Results (BEST EFFORT at PubRate 100 Hz)	41
4.	Latency Test Results (BEST Effort at PubRate 100 Hz).....	43
C.	MULTI-FLOW CONFIGURATIONS	43
1.	Throughput Test Results	44
2.	Latency Test Results	45
D.	SUMMARY OF RESULTS ANALYSIS	47
V.	CONCLUSIONS	49
A.	SUMMARY	49
B.	RECOMMENDATIONS FOR FUTURE WORK.....	50
APPENDIX.	DETAILED SIMULATION RESULTS.....	53
A.	IDEAL CONFIGURATION	53
1.	Throughput Test Results (RELIABLE).....	53
2.	Latency Test Results (RELIABLE).....	56
3.	Throughput Test Results (BEST EFFORT at PubRate 100 Hz)	59
4.	Latency Test Results (BEST EFFORT at PubRate 100 Hz)	62
B.	JITTER CONFIGURATION	65
1.	Throughput Test Results (RELIABLE).....	65
2.	Latency Test Results (RELIABLE).....	69
3.	Throughput Test Results (BEST EFFORT at PubRate 100 Hz)	72
4.	Latency Test Results (BEST EFFORT at PubRate 100 Hz)	75
C.	MULTI-FLOW CONFIGURATION 1.....	78
1.	Throughput Test Results	78
2.	Latency Test Results	79

D.	MULTI-FLOW CONFIGURATION 2	79
1.	Throughput Test Results	79
2.	Latency Test Results	80
LIST OF REFERENCES		83
INITIAL DISTRIBUTION LIST		87

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	DDS as a Middleware Protocol. Source: [4].....	2
Figure 2.	Example of Virtual Network Created by Mininet. Source: [5].....	6
Figure 3.	Comparison between Message-Centric and Data-Centric DDS Approach. Source: [10].....	8
Figure 4.	Implementation of DDS RTPS Protocol. Source: [14].....	9
Figure 5.	Overview of RTI Perftest Throughput Test. Source: [20].	16
Figure 6.	Cryptographic Transformation of RTPS Message. Source: [21].	17
Figure 7.	Proposed Network Architecture.....	20
Figure 8.	Mininet Implementation of our Proposed Network Architecture	21
Figure 9.	Permutations of Simulations for the Ideal and Jitter Configurations.....	31

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Simulations of Point-to-Point Links Performed for Ideal and Jitter Configurations.....	22
Table 2.	Comparison of Average (Avg) Throughput and Data Sample Losses against PubRate for H1 to H3 Link in the Ideal Configuration	24
Table 3.	Simulation Parameters for the Multi-Flow Configurations	25
Table 4.	Mininet Parameters for the Simulation Configurations	27
Table 5.	Throughput Test Results—Comparison of Avg # of DSsps Diff and OH for the Point-to-Point Links in the Ideal Configuration (RELIABLE).....	34
Table 6.	Latency Test Results—Comparison of OH for the Point-to-Point Links in the Ideal Configuration (RELIABLE)	35
Table 7.	Throughput Test Results—Comparison of Avg # of DSsps Diff and OH for the Point-to-Point Links in the Ideal Configuration (BEST EFFORT)	36
Table 8.	Latency Test Results—Comparison of OH for the Point-to-Point Links in the Ideal Configuration (BEST EFFORT).....	37
Table 9.	Throughput Test Results—Comparison of Avg # of DSsps Diff and OH for the Point-to-Point Links in the Jitter Configuration (RELIABLE).....	39
Table 10.	Latency Test Results—Comparison of OH for the Point-to-Point Links in the Jitter Configuration (RELIABLE)	40
Table 11.	Throughput Test Results—Comparison of Avg # of DSsps Diff, OH and Loss for the Point-to-Point Links in the Jitter Configuration (BEST EFFORT)	42
Table 12.	Latency Test Results—Comparison of OH for the Point-to-Point Links in the Jitter Configuration (BEST EFFORT).....	43
Table 13.	Throughput Test Results—Comparison of Avg # of DSsps and Loss between Multi-Flow Configuration 1 and 2.....	45
Table 14.	Latency Test Results—Comparison of Avg Latency between Multi-Flow Configuration 1 and 2	46

Table 15.	Throughput Test Results—Comparison With and Without Security for H1 to H2 Link for Ideal Configuration (RELIABLE)	53
Table 16.	Throughput Test Results—Comparison With and Without Security for H1 to H5 Link for Ideal Configuration (RELIABLE)	54
Table 17.	Throughput Test Results—Comparison With and Without Security for H1 to H3 Link for Ideal Configuration (RELIABLE)	55
Table 18.	Throughput Test Results—Comparison With and Without Security for H2 to H5 Link for Ideal Configuration (RELIABLE)	55
Table 19.	Throughput Test Results—Comparison With and Without Security for H4 to H5 Link for Ideal Configuration (RELIABLE)	56
Table 20.	Latency Test Results—Comparison With and Without Security for H1 to H2 Link for Ideal Configuration (RELIABLE)	57
Table 21.	Latency Test Results—Comparison With and Without Security for H1 to H5 Link for Ideal Configuration (RELIABLE)	57
Table 22.	Latency Test Results—Comparison With and Without Security for H1 to H3 Link for Ideal Configuration (RELIABLE)	58
Table 23.	Latency Test Results—Comparison With and Without Security for H2 to H5 Link for Ideal Configuration (RELIABLE)	58
Table 24.	Latency Test Results—Comparison With and Without Security for H4 to H5 Link for Ideal Configuration (RELIABLE)	59
Table 25.	Throughput Test Results—Comparison With and Without Security for H1 to H2 Link for Ideal Configuration (BEST EFFORT)	59
Table 26.	Throughput Test Results—Comparison With and Without Security for H1 to H5 Link for Ideal Configuration (BEST EFFORT)	60
Table 27.	Throughput Test Results—Comparison With and Without Security for H1 to H3 Link for Ideal Configuration (BEST EFFORT)	61
Table 28.	Throughput Test Results—Comparison With and Without Security for H2 to H5 Link for Ideal Configuration (BEST EFFORT)	61
Table 29.	Throughput Test Results—Comparison With and Without Security for H4 to H5 Link for Ideal Configuration (BEST EFFORT)	62
Table 30.	Latency Test Results—Comparison With and Without Security for H1 to H2 Link for Ideal Configuration (BEST EFFORT)	63

Table 31.	Latency Test Results—Comparison With and Without Security for H1 to H5 Link for Ideal Configuration (BEST EFFORT).....	63
Table 32.	Latency Test Results—Comparison With and Without Security for H1 to H3 Link for Ideal Configuration (BEST EFFORT).....	64
Table 33.	Latency Test Results—Comparison With and Without Security for H2 to H5 Link for Ideal Configuration (BEST EFFORT).....	64
Table 34.	Latency Test Results—Comparison With and Without Security for H4 to H5 Link for Ideal Configuration (BEST EFFORT).....	65
Table 35.	Throughput Test Results—Comparison With and Without Security for H1 to H2 Link for Jitter Configuration (RELIABLE)	66
Table 36.	Throughput Test Results—Comparison With and Without Security for H1 to H5 Link for Jitter Configuration (RELIABLE)	66
Table 37.	Throughput Test Results—Comparison With and Without Security for H1 to H3 Link for Jitter Configuration (RELIABLE)	67
Table 38.	Throughput Test Results—Comparison With and Without Security for H2 to H5 Link for Jitter Configuration (RELIABLE)	68
Table 39.	Throughput Test Results—Comparison With and Without Security for H4 to H5 Link for Jitter Configuration (RELIABLE)	68
Table 40.	Latency Test Results—Comparison With and Without Security for H1 to H2 Link for Jitter Configuration (RELIABLE)	69
Table 41.	Latency Test Results—Comparison With and Without Security for H1 to H5 Link for Jitter Configuration (RELIABLE)	70
Table 42.	Latency Test Results—Comparison With and Without Security for H1 to H3 Link for Jitter Configuration (RELIABLE)	70
Table 43.	Latency Test Results—Comparison With and Without Security for H2 to H5 Link for Jitter Configuration (RELIABLE)	71
Table 44.	Latency Test Results—Comparison With and Without Security for H4 to H5 Link for Jitter Configuration (RELIABLE)	71
Table 45.	Throughput Test Results—Comparison With and Without Security for H1 to H2 Link for Jitter Configuration (BEST EFFORT)	72
Table 46.	Throughput Test Results—Comparison With and Without Security for H1 to H5 Link for Jitter Configuration (BEST EFFORT)	72

Table 47.	Throughput Test Results—Comparison With and Without Security for H1 to H3 Link for Jitter Configuration (BEST EFFORT)	73
Table 48.	Throughput Test Results—Comparison With and Without Security for H2 to H5 Link for Jitter Configuration (BEST EFFORT)	74
Table 49.	Throughput Test Results—Comparison With and Without Security for H4 to H5 Link for Jitter Configuration (BEST EFFORT)	74
Table 50.	Latency Test Results—Comparison With and Without Security for H1 to H2 Link for Jitter Configuration (BEST EFFORT).....	75
Table 51.	Latency Test Results—Comparison With and Without Security for H1 to H5 Link for Jitter Configuration (BEST EFFORT).....	76
Table 52.	Latency Test Results—Comparison With and Without Security for H1 to H3 Link for Jitter Configuration (BEST EFFORT).....	76
Table 53.	Latency Test Results—Comparison With and Without Security for H2 to H5 Link for Jitter Configuration (BEST EFFORT).....	77
Table 54.	Latency Test Results—Comparison With and Without Security for H4 to H5 Link for Jitter Configuration (BEST EFFORT).....	77
Table 55.	Throughput Test Results for Multi-Flow Configuration 1	78
Table 56.	Latency Test Results for Multi-Flow Configuration 1	79
Table 57.	Throughput Test Results for Multi-Flow Configuration 2	80
Table 58.	Latency Test Results for Multi-Flow Configuration 2	81

LIST OF ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
AP	Access Point
API	Application Programming Interface
Avg	Average
CA	Certificate Authority
CLI	Command Line Interface
CPU	Central Processing Unit
DCPS	Data-Centric Publish Subscribe
DDR4	Double Data Rate 4 th Generation
DDS	Data Distribution Service
DH	Diffie Hellman
Diff	Difference
DR	DataReader
DS	Data Sample
DSsps	Data Samples Sent per Second
DW	DataWriter
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
GCM	Galois Counter Mode
GMAC	Galois Message Authentication Code
H	Host
HQ	Headquarters
IP	Internet Protocol
L	Latency
Min	Minimum
Max	Maximum
MITM	Man-in-the-Middle
OH	Overhead
OS	Operating System
PIM	Platform Independent Module

PKC	Public Key Cryptography
PSM	Platform Specific Module
PMW760	Ship Integration Program Office
Pub	Publisher
PubRate	Publication Rate
QoS	Quality of Service
ROS2	Robot Operating System 2
RSA	Rivest Shamir Adleman
RTI	Real-Time Innovations
RTPS	Real-Time Publish Subscribe
RTT	Round-Trip Time
S	Switch
SATCOM	Satellite Communications
SDN	Software Defined Networking
SEDP	Simple End Point Discovery Protocol
SHMEM	Symmetric Hierarchical Memory
SPDP	Simple Participant Discovery Protocol
Sub	Subscriber
TH	Throughput
UDP	User Datagram Protocol
U.S.	United States
VEth	Virtual Ethernet
WiFi	Wireless Fidelity
VoIP	Voice over Internet Protocol

ACKNOWLEDGMENTS

I would like to express my heartfelt gratitude to Dr. Preetha Thulasiraman, Dr. Brian Bingham, and Mr. Bruce Allen. I was able to bridge the knowledge gap required to successfully complete my thesis because of their invaluable advice and guidance.

I would like to thank the Republic of Singapore Navy for giving me the opportunity to pursue new knowledge and fulfill my aspiration.

Last but not least, I would like to sincerely thank my wife, Teresa, for her constant encouragement and support throughout my stint at Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The use of autonomous or unmanned systems is ubiquitous in the world today. In the civilian and commercial sectors, advances in artificial intelligence have led to increased development and use of unmanned systems, particularly in the industries of information technology, automotive systems, manufacturing, retail, and healthcare [1]. More importantly, unmanned systems have demonstrated huge potential and value as enablers for military operations [2]. To fully exploit the advantages of unmanned systems in the battlespace, improved autonomy and interoperability are key [2]. The eventual goal is for the unmanned systems to interoperate not only with human operators, but also with each other [2]. In addition, with the future leaning towards operating an increasing scale of unmanned systems in the battlespace, command, control and communications systems become significantly important [3]. In particular, the communications and networking protocol must be robust to handle different types of environments, enable interoperability and allow the human operators to control the increasing scale of unmanned systems in the battlespace [2], [3].

The U.S. Navy has recently been studying the integration of communications and networking protocols for unmanned systems. Specifically, the Ship Integration Program Office (PMW760) is interested in the prospect of having a unified, cohesive communications protocol that can be used by all unmanned assets. This communications protocol will contribute to the eventual goal of improved autonomy and interoperability for unmanned systems.

The Data Distribution Service (DDS), a middleware protocol, is a prime candidate for the cohesive communications protocol that PMW760 desires [4]. As illustrated in Figure 1, the middleware is the software layer that resides between the back-end Operating System (OS) and the front-end application layer. It facilitates easy and seamless information exchange across systems and applications. Hence, DDS acts as a bridge and allows different manned and unmanned systems to network and communicate with each other.

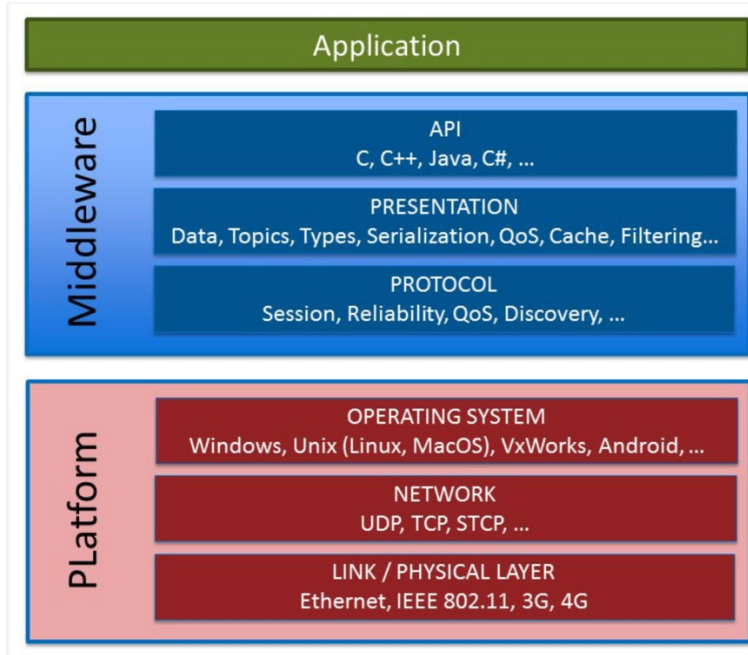


Figure 1. DDS as a Middleware Protocol. Source: [4].

A. THESIS CONTRIBUTIONS

This thesis contributes to funded research by PMW760 to evaluate the performance of DDS as a unified, cohesive unmanned systems communications protocol. The objective of this thesis is to assess the performance of DDS, as the backbone communications protocol, in a network architecture that fits PMW760 Naval use case criteria. Mininet, a network emulator, is used to setup the network parameters and Real-Time Innovations (RTI) Perftest is used to perform the simulations. The contributions of this thesis are as follows:

- Propose a use case architecture that incorporates Satellite Communications (SATCOM) and Wireless Fidelity (WiFi) links to test the ability of DDS to execute cohesive communications between the network nodes within the constraints of the scenario setup.
- Evaluate throughput and latency performance of the individual point-to-point links across various data samples, under ideal and jitter network

configurations, for RELIABLE and BEST EFFORT communications, as well as with and without DDS security.

- Evaluate throughput and latency performance of simultaneous multi-flow communications between the network nodes when jitter and loss are applied to the network configuration.

B. THESIS ORGANIZATION

The rest of this thesis is organized as follows: Chapter II provides an overview of Mininet, the operation of DDS, including the options for DDS security, and how throughput and latency simulation tests are conducted in RTI Perftest. Chapter III describes the proposed network architecture and scenario design that fits the Navy use case. We also discuss the selection of Mininet and DDS parameters for the RTI Perftest simulations. Chapter IV presents and discusses the simulation results. Chapter VI provides thesis conclusions and recommends approaches for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND AND RELATED WORK

In this chapter, we present the background of the software used to conduct our simulations. First, we discuss the operations and limitations of Mininet. Next, we provide an overview of the DDS protocol including its security functions, performance and vulnerabilities. Finally, we present the available test modes and DDS security options for the RTI PerfTest software.

A. MININET

1. Overview of Mininet

Mininet is a scalable network emulator that quickly prototypes network architectures for experimentation on a single computer. Mininet is also a lightweight network emulator that adopts OS-level virtualization and enables research in Software Defined Networking (SDN) and OpenFlow [5]. In SDN, the processor responsible for decision making is centralized in a software-based controller (control plane) and detached from the packet forwarding devices (data plane) [6]. The control and data plane communicates via the OpenFlow protocol which is used to program flow tables in switches or routers [7]. Flow tables dictate the rules and responses that decide how the packets will be managed. Examples include whether packets will be dropped or the next location that they will be forwarded.

Mininet enables virtual networks of different topologies to be setup easily for performance testing and simulations within a sandbox environment. This avoids the costs and inconvenience of having to build and configure real prototypes solely for the purpose of experimentations. Experimentations in Mininet are also realistic because virtual elements created in Mininet are modelled after their respective hardware elements and thus, exhibit similar behavior [8]. Once experimentations are successful, the code can easily be ported over to validate the network using real hardware [5].

2. Operations of Mininet

Mininet utilizes the Python Application Programming Interface (API) to emulate virtual hosts, switches, controllers, and network links by leveraging the features built into the Linux kernel—processes and network namespaces [8]. Network namespaces are Linux containers with independent network interfaces, ports and routing tables. Figure 2 shows that the hosts run in network namespaces as bash (shell) processes which are connected to other elements via their respective virtual Ethernet (Veth) link pairs [5]. These Veth link pairs function as the emulated network links which are controlled by Linux Traffic Control. Packet flows are then directed via the virtual switches using Linux bridge, Open vSwitch or OpenFlow switches which are controlled by default or custom controllers using the Internet Protocol (IP) [5], [8].

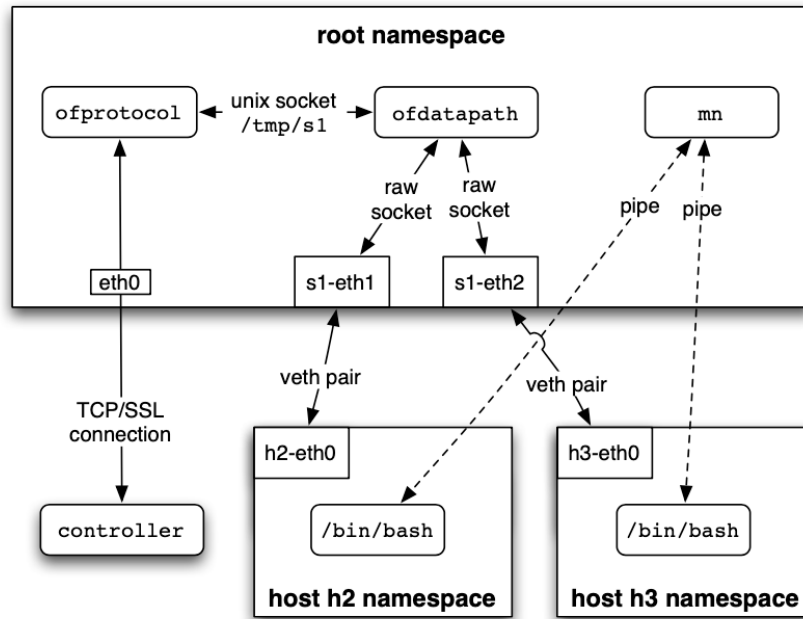


Figure 2. Example of Virtual Network Created by Mininet. Source: [5].

3. Limitations of Mininet

One limitation of Mininet is the issue of resource contention as the resources of a single computer have to be shared across the virtualized elements, affecting results and

leading to degraded network performance [8]. Moreover, this effect is exacerbated with increasing scale of topologies as the number of virtualized elements increases. As part of the study for assessing the limits of Mininet, network performance for three topologies, comprising up to 1500 hosts, were evaluated by varying different network elements for different scenarios in [9]. The study found that bandwidth was not severely impacted when the number of hosts increased from 10 to 1500; results showed a drop in aggregated bandwidth of about 10 Gbps to the median of about 15 Gbps. Achievable bandwidth was also not significantly impacted when the number of switches increased from 2 to 32 while keeping the number of hosts fixed at 100; results showed that achievable bandwidth remained at the median value of about 22–23 Gbps. The study also found that the median Round-Trip Time (RTT) remained at acceptable values of around 1 ms when the number of hosts was increased to 1500. The study concluded that despite the limitations, Mininet remained a robust emulator for network experimentation.

B. DDS

1. Overview of DDS

DDS is a middleware protocol that enables information exchange across systems and applications. However, instead of the conventional message-centric approach, DDS adopts the data-centric approach [10]. There is no longer a requirement for applications to handle the specific message sending protocols because DDS takes over and incorporates them in the middleware layer. In the data-centric approach, the middleware contextualizes the information so that only the system state information and data values are required to be transmitted [10]. Thus, the middleware understands the context of the data that is exchanged and controls what, when and how to share them. The middleware ensures that the right data is delivered to the right place and at the right time [11]. This greatly improves efficiency and as illustrated in Figure 3, the data-centric approach relieves the message handling programming complexity in the application layer, allowing the code to be “transparent” to the applications [10].

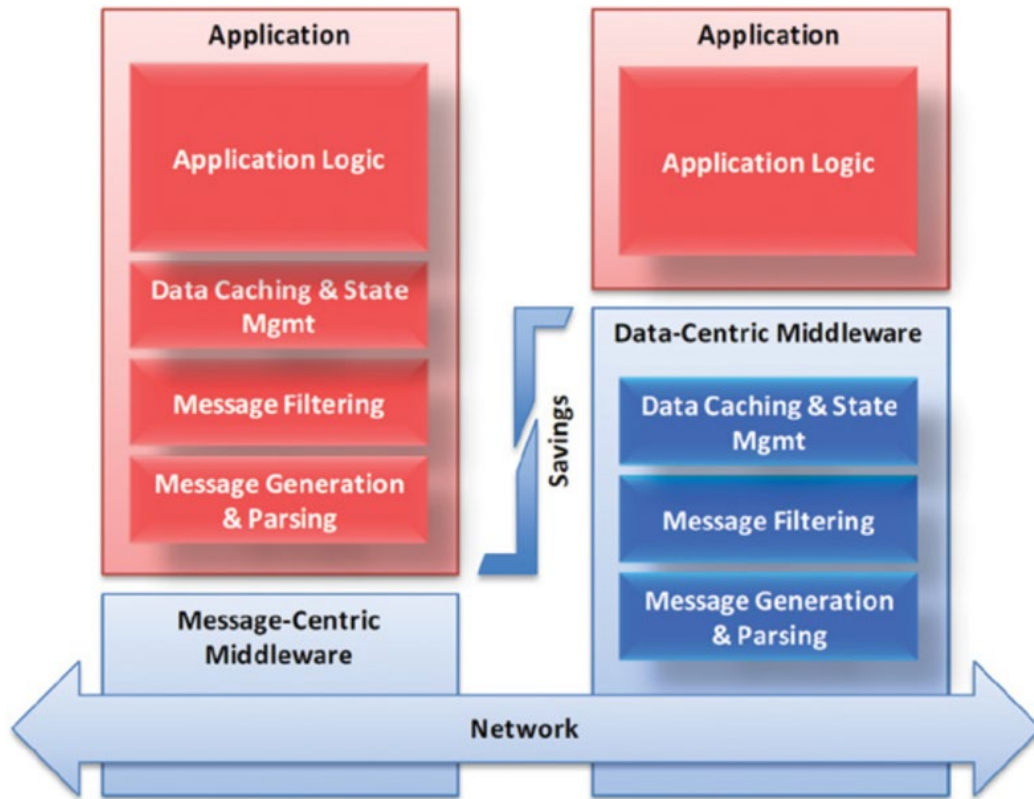


Figure 3. Comparison between Message-Centric and Data-Centric DDS Approach. Source: [10].

DDS adheres to specifications defined by the Data-Centric Publish Subscribe (DCPS) model that is developed by the Object Management Group [12]. In DDS, applications (participants) communicate by publishing or subscribing to topics within distinct and independent domains. Sharing of data across domains is prohibited. Topics are identified by their names and can only represent one type of data. They also have to reside in their respective domains.

The DDS architecture comprises several entities. The sending entities, responsible for transmitting data, comprise the Publisher and its associated DataWriter (DW). Similarly, the receiving entities, responsible for receiving data, comprise the Subscriber and its associated DataReader (DR). The role of DWs and DRs are to write and read data respectively. They also form the end points of the communications links. Publishers and Subscribers communicate peer-to-peer, without any middleman, via the Real-Time Publish

Subscribe (RTPS) protocol [13]. RTPS defines how data are transmitted across the network. Figure 4 illustrates how the RTPS protocol is implemented [14]. Two modules drive the RTPS protocol [13]. The Platform Independent Module (PIM) defines how the end points of the communications links are discovered, the message structure and the data types. The Platform Specific Module (PSM) maps the PIM onto the transport protocols (User Datagram Protocol (UDP) or IP) for transmission across the communications link.

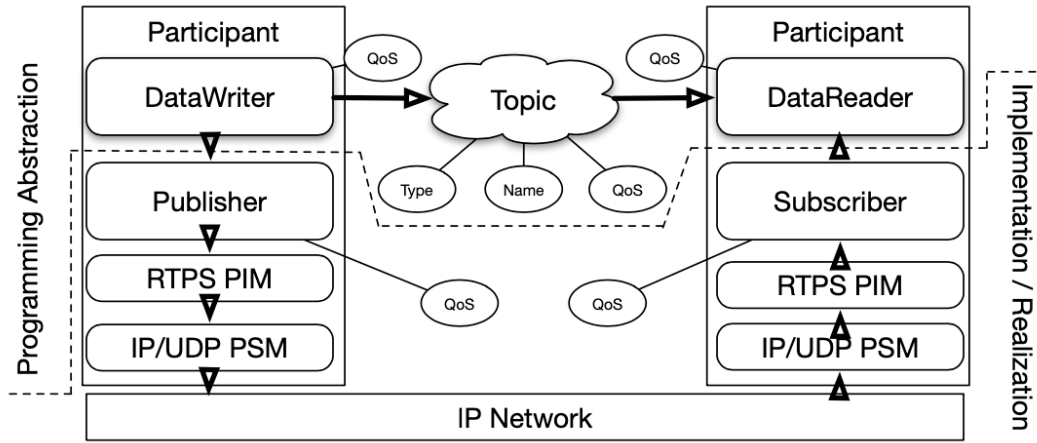


Figure 4. Implementation of DDS RTPS Protocol. Source: [14].

In DDS, Quality of Service (QoS) policies drive the behavior of data flows. There are several QoS policies offered by DDS and the relevant ones discussed in this thesis are as follows:

- Reliability QoS policy defines whether data samples are successfully delivered to the corresponding DRs without any loss of data samples. It can either be set to BEST EFFORT where data samples are not guaranteed to be delivered or RELIABLE where data samples are guaranteed to be delivered to the DRs without any loss.
- Durability QoS Policy determines how and whether old data samples will be stored by the DWs. This provides flexibility in deciding how the old data samples are stored so that they are available for delivery to the DRs

that are late to join the domain. There is a total of four different settings. VOLATILE does not store the old data samples. TRANSIENT LOCAL stores the old data samples only if the DWs are still present in the domain. TRANSIENT stores the old data samples in memory and PERSISTENCE stores the old data samples on the disk such that they are available even after a system reset.

- History QoS policy defines the number of data samples that are stored in the system. KEEP LAST stores the number of data samples specified by the DEPTH parameter and KEEP ALL stores all available data samples.
- Ownership QoS policy governs the DW write access control. It can be set to EXCLUSIVE where only one DW has the rights to write to the topic. If multiple DWs possess the EXCLUSIVE Ownership QoS policy, only the DW that has the highest OWNERSHIP STRENGTH parameter is allowed to write to the topic at any one time. The Ownership QoS policy can also be set to SHARED. This allows multiple DWs to write to the topic at any time.
- Lifespan QoS Policy controls the amount of time that determines when the data samples are no longer valid and will be deleted.

2. Operations of DDS

The operations of DDS comprise four steps. The first two steps involve the discovery of participants and their associated DWs or DRs [15]. In the first step, remote participants discover each other via the Simple Participant Discovery Protocol (SPDP) where participants advertise themselves by periodically sending discovery messages to other participants using BEST EFFORT Reliability QoS policy. In the second step, the discovered participants confirm the discovery of the DWs and DRs via the Simple End Point Discovery Protocol (SEDP) using the RELIABLE Reliability QoS policy. In the third step, Publishers and Subscribers with the same topic name, data type and matching QoS

policies are linked together to establish the communications pathways. Finally, in the last step, data traffic flow through the communications pathways established in step three.

3. Overview of DDS Security

The design of DDS security is to prevent Man-in-the-Middle (MITM) attacks and ensure that only participants with the requisite permissions are allowed to publish, subscribe or access the data [16]. DDS security specifications comprises five security features, namely (1) Authentication, (2) Access Control, (3) Cryptography, (4) Logging, and (5) Data Tagging [16]. These features are implemented via built-in plugins to enable interoperability and can be configured to suit the needs of each participant.

a. Authentication

Authentication forms the start of security checks before participants are allowed to join the secure domains. Identity certificates are signed by a trusted Identity Certificate Authority (CA) such that participant identities are verified and established during the discovery step via the Rivest Shamir Adleman (RSA) Digital Signature Algorithm or Elliptic Curve Digital Signature Algorithm (ECDSA). This process of mutual authentication also facilitates the sharing of secret keys to support Public Key Cryptography (PKC) via Diffie Hellman (DH) or Elliptic Curve Diffie Hellman (ECDH) key exchange protocols.

b. Access Control

Access Control governs participant and domain permission levels via the permissions and governance documents, respectively. These documents are signed by the trusted Permissions CA. The participant permissions document consists of the participant permission levels pertaining to the domains they are allowed to join and the topics they are allowed to publish and subscribe. The domain governance document are the gatekeepers to participants requesting to join the domain and it specifies the kinds and levels of protection. Depending on the security requirements, integrity and/or confidentiality can be protected. Hence, domain governance allows for finer control and flexibility in choosing the kinds of cryptographic protection that are applied to the RTPS Message, SubMessage

(within the RTPS Message), and Serialized Payload (within the SubMessage) [16]. The five kinds of cryptographic protection and their functionalities are as follows [16]:

- *discovery_protection_kind* and *liveliness_protection_kind* protects participants, DWs and DRs during the discovery phase.
- *rtps_protection_kind* protects the entire RTPS Message including the header and the SubMessage (header and elements) within it.
- *metadata_protection_kind* protects the SubMessage header and elements including the Serialized Payload within it.
- *data_protection_kind* protects only the Serialized Payload.

c. *Cryptography*

Cryptography specifies the security algorithms used for encryption and message authentication checks. It supports encryption using 128/256 bits Advanced Encryption Standard (AES) in Galois Counter Mode (GCM), as well as generating Galois Message Authentication Code (GMAC) for message authentication checks.

d. *Logging*

Logging records all security events that occurred to support eventual auditing when the need arises.

e. *Data Tagging*

Data tagging enables the addition of labels to data samples. These labels contain important information that are used by other DDS entities to support the DDS operations.

4. Vulnerabilities of DDS

Vulnerabilities are studied by identifying the potential threats and their line of attacks. Systems are then analyzed to determine whether they are susceptible to the attacks. It was identified in [17] that the main threat to DDS systems was insider attacks caused by participants who were already compromised.

In [17], the study demonstrated and validated five malicious attacks that exploited the vulnerabilities of the DDS systems. These vulnerabilities, on unsecured DDS systems, were studied by investigating the DDS protocols. The five attacks were as follows:

- The first attack manipulates existing data samples and sends modified data samples to Subscribers. It was found that only knowledge of the transmitted data type and Ownership QoS policy was required to carry out the attack.
- The second attack hijacks the data samples from the original Publisher and acts as the malicious Publisher. It exploits the protocol that only the DW with the highest OWNERSHIP STRENGTH parameter will be allowed to send the data samples when Ownership QoS Policy is set to EXCLUSIVE.
- The third attack hijacks the data samples from the original Subscriber such that it will not continue to receive any data samples. For this attack, the Ownership QoS policy for the Publisher needs to be modified such that it differs from the original Subscriber. A malicious Subscriber with the same Ownership QoS policy can then be inserted into the network.
- The fourth attack stops the data samples from being received by a Subscriber. It manipulates the Lifespan QoS policy.
- The fifth attack forces new unknowing participants into joining a malicious domain. This attack exploits the LocatorList environment variable which specifies the IP address used by the DDS entities to initiate SPDP during the discovery phase.

These attacks can be carried out by (1) obtaining the required information via inspection of the RTPS packets using Wireshark and (2) modifying DDS configuration files that control the QoS policies and environment variables. Modification of the DDS configuration files requires the known locations of the files. For applications developed using DDS libraries, the startup process that automatically scans and reads the file with the correct name could be exploited [17]. The authors concluded that while security

enhancements had been progressively implemented in DDS, these new security enhancements may not resolve current security problems. One potential issue that might arise would be putting secure DDS systems in a network together with non-secure legacy DDS systems.

5. Performance of DDS

The performance of DDS is often measured in terms of throughput and latency. The Robot Operating System 2 (ROS2) uses DDS as the middleware layer and a study was conducted to understand how enabling DDS security affects its performance [18]. A test was conducted on a data sample size of 63 KB between two network nodes on a computer. Comparing the results between no security enabled and data samples encrypted with RSA 2048 bits, latency increased from 267 μ s to 1343 μ s and throughput decreased from 35163.7 Mbps to 7177.7 Mbps. This meant that, for this scenario, the overhead required to encrypt data samples with RSA 2048 bits resulted in approximately 403% increase in latency and 80% decrease in throughput. Another test was conducted on data sample sizes ranging from 1 KB to 63 KB between two computers over a wireless network. Similarly, for this test, results for the 4 KB and 63 KB data samples with no security enabled and data samples encrypted with RSA 2048 bits were chosen for comparison. For 4 KB, latency increased from 53349 μ s to 61270 μ s (15% increase) and throughput decreased from 21 Mbps to 17 Mbps (19% decrease). For 63 KB, latency increased from 208883 μ s to 290675 μ s (39% increase) and, interestingly, throughput also increased from 18 Mbps to 24 Mbps (33% increase) after the data samples were encrypted. No further information and assessment were provided by the authors to explain the huge difference between the results of both scenarios, as well as the increase in throughput for the 63 KB data sample in the remote wireless scenario.

Another series of DDS performance tests were conducted by RTI and presented during ROSCon 2018 [19]. The tests were conducted between network nodes on a single computer to show how enabling security impacts the performance of DDS across data samples from 32 B to 1 MB. Tests were also conducted by increasing the number of Subscribers from 1 to 4 in multicast mode. The security settings used were (1) Sign, (2)

Sign and Encrypt, and (3) Sign and Encrypt with Origin Authentication. For the “1 to 1” Publisher-Subscriber tests, across data samples from 32 B to 1 MB, enabling the security settings resulted in increased latency between 1% to 41% and reduced throughput between 0% to 32%. The overhead increased as more features, from (1) to (3), were enabled. The overhead decreased as the size of the data samples increased. For “1 to N” Publisher-Subscriber tests, results were presented for data samples of 32 B, 2 KB, and 128 KB. When N increased from 1 to 4, enabling security resulted in increased latency between 6% to 49% and reduced throughput between 0% to 48%.

C. RTI PERFTEST

RTI PerfTest is a performance testing utility tool developed by RTI to measure minimum and loaded latency, as well as maximum throughput across various scenarios [20]. It provides an easy-to-use Command Line Interface (CLI) and is configurable via several parameters to suit the needs of each scenario. RTI PerfTest also provides support for DDS security and runs in two modes—Throughput Test and Latency Test. Both modes utilize three Topics to obtain the required results. The Announcement Topic is for discovery of DWs and DRs. The Throughput Topic processes throughput results while the Latency Topic processes latency results.

1. Throughput Test

Figure 5 shows an overview of how the Throughput Test works. During the Throughput Test, the Publisher writes data and sends data samples as fast as possible to the Subscriber. In these data samples, an Echo Request sample is sent for every fixed number of data samples determined by the user. The Subscriber then acknowledges the Echo Request sample by sending an Echo Reply sample. The pair of Echo Request-Reply sample measures the RTT and results are output as one-way latency. The Throughput Test floods the network links and internal queues continuously for the duration specified by the user. Hence, it provides the maximum throughput of the network link in Mbps. Although the Throughput Test provides latency results, the flooding of network links and the number of Echo-Request samples sent per fixed number of data samples will affect the latency results. Hence, the Latency Test mode should be used to obtain the minimum latency.

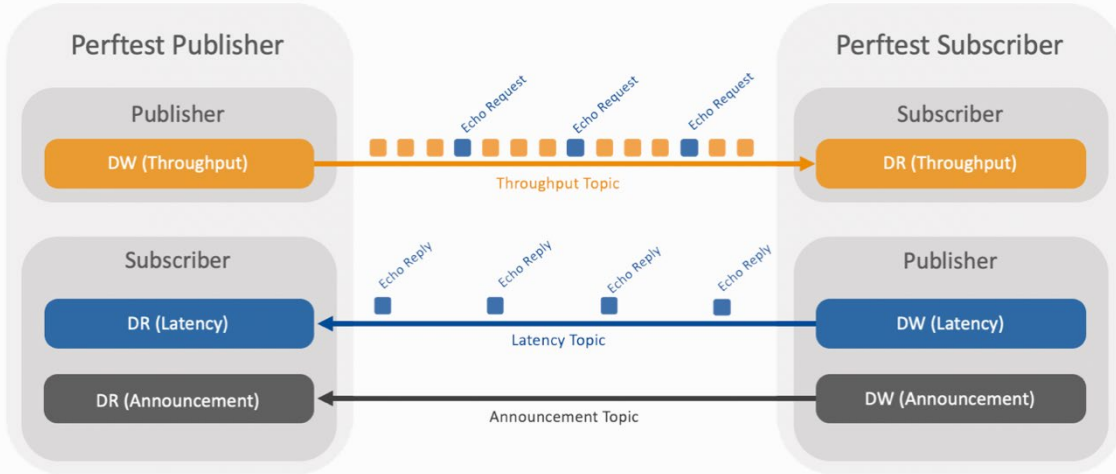


Figure 5. Overview of RTI Perftest Throughput Test. Source: [20].

2. Latency Test

The operation of the Latency Test differs from the Throughput Test. During the Latency Test, the Publisher sends a data sample and waits for each data sample to be sent back by the Subscriber before sending the next data sample. It operates in a “Ping-Pong” fashion such that every data sample measures latency. The Latency Test ensures that the Publisher internal queue remains empty throughout the duration of the test. Hence, it provides the minimum latency of the network link. Although the Latency Test provides throughput results, it will not output the maximum throughput because the network is not operating at its full capacity without the flooding of the network links. Thus, the Throughput Test mode should be used to obtain the maximum throughput.

3. Options for DDS Security

The four default security options supported by RTI Perftest are as follows [18]:

- SecureEncryptDiscovery enables both *discovery_protection_kind* and *liveliness_protection_kind*.
- SecureSign enables *rtps_protection_kind*.
- SecureEncryptSM enables *metadata_protection_kind*.

- SecureEncryptData enables *data_protection_kind*.

Figure 6 shows the RTPS Message elements wrapped with their respective “Prefix” and “Postfix” after all security options are enabled [21]. These can be observed during the RTI Perftest simulations by inspecting the RTPS packets in Wireshark when security options are enabled.

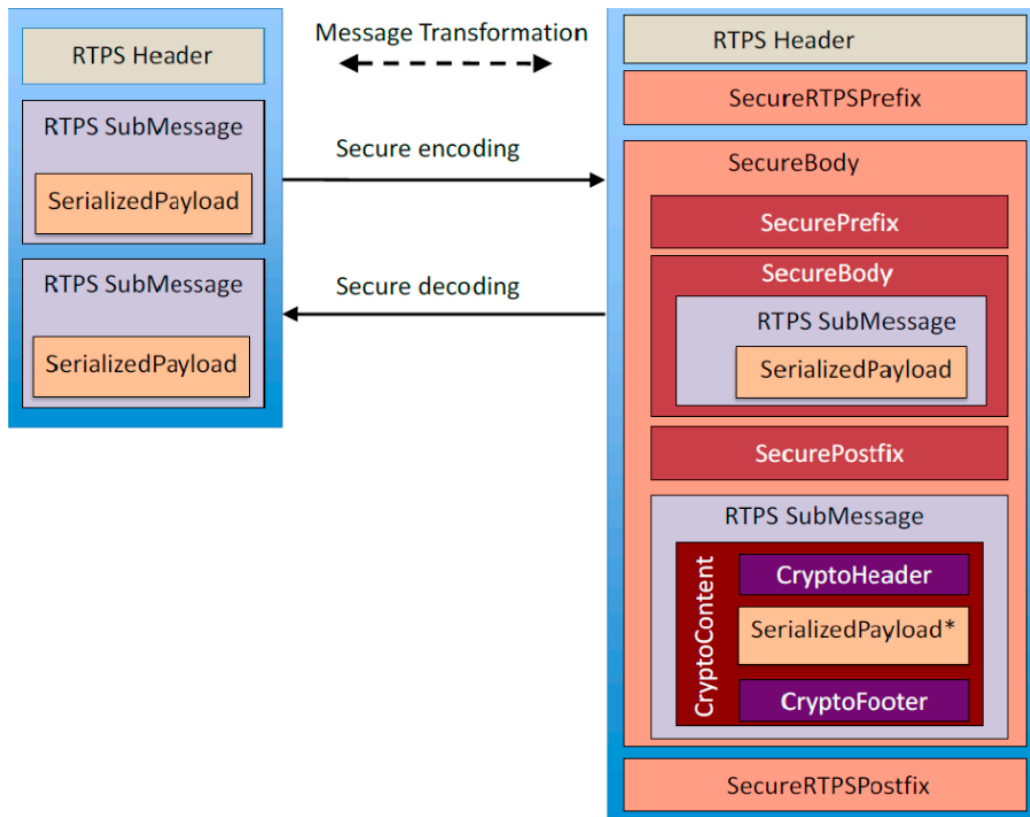


Figure 6. Cryptographic Transformation of RTPS Message. Source: [21].

THIS PAGE INTENTIONALLY LEFT BLANK

III. PROPOSED NETWORK ARCHITECTURE AND SIMULATION SETUP

In this chapter, we detail the proposed use case architecture and scenario design that aligns with the needs of PMW760. We also discuss the methodology to our simulation setup. We start by describing our proposed network architecture and the approach for our simulation runs. We then elaborate on the selection of parameters for the Mininet and RTI Perfest software. We end this chapter by providing the hardware and software specifications for our simulations.

A. PROPOSED NETWORK ARCHITECTURE AND SCENARIO SETUP

Our proposed network architecture is shown in Figure 7. The Mission Commander resides at Headquarters (HQ) and exercises Command and Control over his Task Units, comprising the On-Site Commander, the Support Craft, the Trailer, and the two Drones. The scenario setup is as follows:

- The Mission Commander is located at HQ and connects to the rest of the network via the HQ WiFi. He also controls the Black Drone at the mission site.
- The Support Craft is located at sea and connects to the satellite directly via SATCOM.
- The Trailer is located at the mission site and connects to the satellite to provide WiFi for the Task Units on site.
- The On-Site Commander is located at the mission site and connects to the Trailer WiFi Access Point (AP). He relays the Trailer WiFi signal to enable communications for the Drones. The On-Site Commander also controls the White Drone.
- The Black and White Drones connect to the Drone Communications WiFi AP relayed by the On-Site Commander.

- The Mission Commander, Support Craft and On-Site Commander are able to talk to each other via voice communications.
- The Mission Commander and On-Site Commander receives video data from the Black Drone and White Drone respectively. The Support Craft also shares video data with the Mission Commander and On-Site Commander.

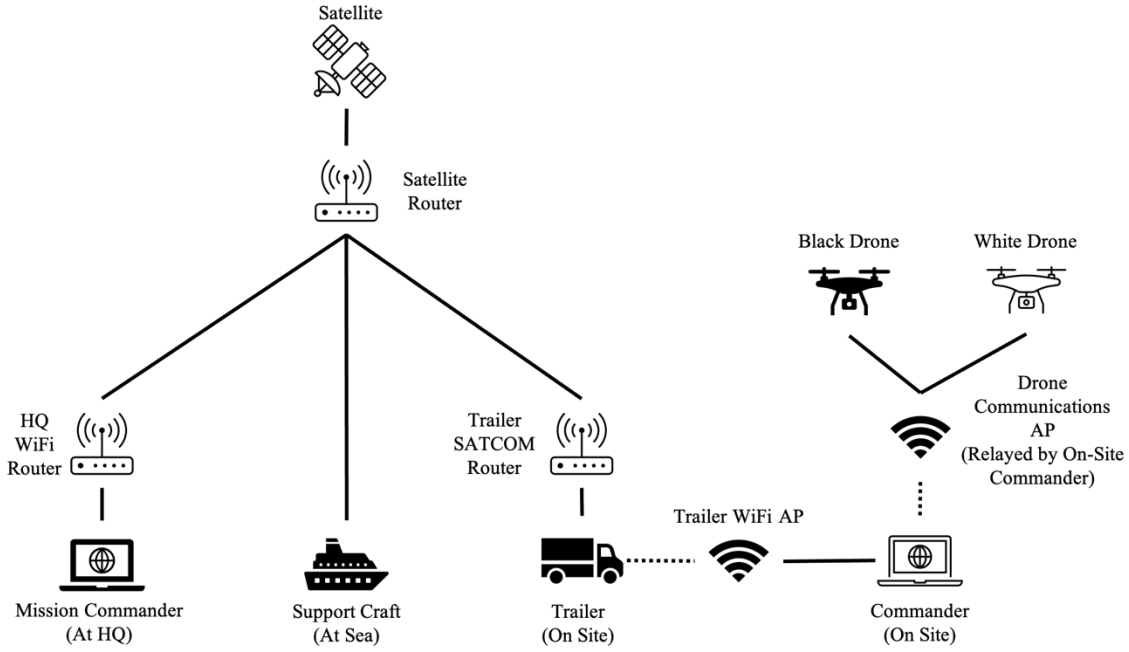


Figure 7. Proposed Network Architecture

Our proposed network architecture is implemented in Mininet with Host (H), Switch (S), and network links as shown in Figure 8. We replaced the routers in Figure 7 with switches so that we are able to evaluate the throughput and latency performance without the need to configure routing tables. The network nodes are connected by the network links which model the flow constraints. The network links setup are as follows:

- The HQ WiFi link connects the Mission Commander (H1) to the rest of the network using the HQ WiFi Switch (S1).

- The SATCOM links connect the Satellite Switch (S2) to S1, the Support Craft (H2), and the Trailer SATCOM Switch (S3).
- The Trailer WiFi link connects S3 to the Trailer WiFi AP modelled by Switch S4.
- The On-Site Commander (H5) relays the Trailer WiFi signal and serves as the Drone Communications AP. Hence, it is directly linked to the Drone Communications AP which is also modelled by S4. In this way, we implement S4 to serve as both the Trailer WiFi AP and Drone Communications AP.
- The Drone WiFi link connects the Black Drone (H3) and White Drone (H4) to the Drone Communications AP.

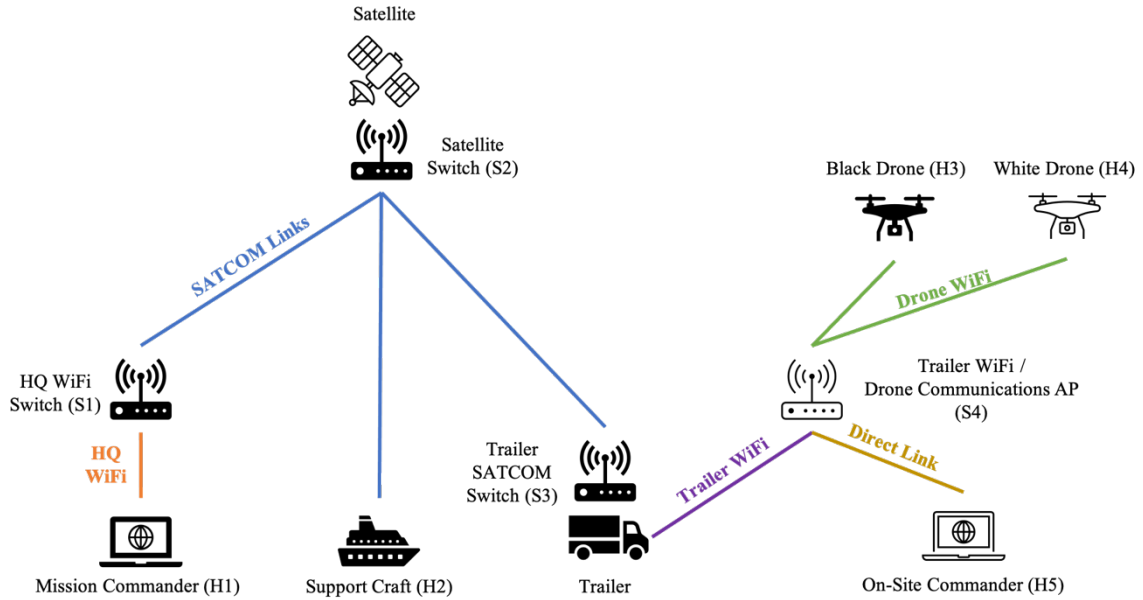


Figure 8. Mininet Implementation of our Proposed Network Architecture

B. OVERVIEW OF APPROACH TO SIMULATION RUNS

The simulation runs are conducted for the Throughput and Latency Test modes. They are classified into three configurations, namely (1) Ideal, (2) Jitter, and (3) Multi-

Flow. The approach is to first obtain the baseline performance for our proposed network architecture. Hence, we start with the Ideal configuration and perform simulations across various sizes of data samples (32 B, 64 B, 128 B, 256 B, 512 B, 1024 B, 2048 B, 4096 B, 8192 B, 16384 B, 32768 B, 63000 B). These simulations are performed for RELIABLE and BEST EFFORT communications, as well as with and without security implemented.

Simulations for the Ideal configuration are performed for the point-to-point links as shown in Table 1. This is to avoid replicating similar results when the Publisher (Pub) and Subscriber (Sub) roles are reversed as the performance will be similar when there are no changes to the flow constraints. The simulations for the point-to-point links are also conducted separately within a single domain so that there will be no contention of the network resources.

Table 1. Simulations of Point-to-Point Links Performed for Ideal and Jitter Configurations

Point-to-Point Network Links	
Pub	Sub
H1	H2
H1	H5
H1	H3
H2	H5
H4	H5

For RELIABLE communications in the Ideal configuration, we do not limit the publication rate (PubRate) so that data samples are sent continuously as fast as possible to obtain the maximum throughput. However, publishing as fast as possible for BEST EFFORT communications results in huge loss of data samples which will not be meaningful for our research work (see Table 2). Thus, we proceed to find the optimum PubRate to be used for BEST EFFORT simulations that meets the requirement of less than 1% loss across all the data samples from 32 B to 63000 B. We employ the Spin delay method (refer to Section D7 in this chapter for further discussion on the Spin delay method) to limit the PubRate to allow the Subscriber to “catch up.” The approach to finding the optimum PubRate is based on the furthest end-to-end link (H1 to H3) in our proposed

network architecture without security implemented. As shown in Table 2, the PubRate of 100 Hz has 0% loss across all the data sample sizes. Hence, we set the baseline PubRate for BEST EFFORT communications to 100 Hz and use it for the BEST EFFORT simulations in the Ideal configuration. We also found that RTI PerfTest computes the throughput results rounded off to one decimal place for small data samples. Thus, the measured results might be less than 0.04 Mbps and are rounded off to show 0.0 Mbps. Furthermore, results for the average data samples sent per second are also rounded off to the nearest whole number. Hence, for data samples with 0% loss, we compute the average throughput expected by multiplying the average data samples sent per second with the corresponding size of the data samples in bits. Table 2 shows that the measured throughput is very close to the expected throughput and the small differences observed are due to rounding off errors when the measured throughput is “computed” by the RTI PerfTest software. For the rest of this thesis, for the throughput results of small data samples that show 0.0 Mbps, we compute the expected throughput and present that instead.

Table 2. Comparison of Average (Avg) Throughput and Data Sample Losses against PubRate for H1 to H3 Link in the Ideal Configuration

BEST EFFORT H1 (Pub) to H3 (Sub) Link										
Data Sample Size (bytes)	Data Sample Size (bits)	PubRate 100 Hz			PubRate 500 Hz			PubRate Not Set		
		Avg Throughput Measured (Mbps)	Avg Throughput Expected (Mbps)	Loss (%)	Avg Throughput Measured (Mbps)	Avg Throughput Expected (Mbps)	Loss (%)	Avg Throughput Measured (Mbps)	Avg Throughput Expected (Mbps)	Loss (%)
32	256	0.0	0.026	0	0.1	0.128	0	12.9	-	41.96
64	512	0.1	0.05	0	0.3	0.26	0	14.3	-	70.17
128	1024	0.1	0.10	0	0.5	0.51	0	22.4	-	74.24
256	2048	0.2	0.20	0	1.0	1.02	0	38.3	-	85.89
512	4096	0.4	0.41	0	2.0	2.05	0	31.1	-	95.72
1024	8192	0.8	0.82	0	4.1	4.10	0	49.1	-	97.24
2048	16384	1.6	1.64	0	8.2	8.19	0	1.0	-	99.97
4096	32768	3.3	3.28	0	16.3	16.38	0	1.7	-	99.97
8192	65536	6.6	6.55	0	32.7	32.77	0	2.3	-	99.95
16384	131072	13.1	13.11	0	4.5	-	92.94	-	-	-
32768	262144	26.2	26.21	0	-	-	-	-	-	-
63000	504000	50.6	50.40	0	-	-	-	1.4	-	99.99

For the Jitter configuration, we adopt the same approach as the Ideal configuration and repeat what was performed. We also adopt the baseline PubRate for BEST EFFORT simulations in the Jitter configuration. This provides a fair comparison for the analysis of the simulation results.

For the Multi-Flow configurations, we perform simulations based on the scenarios to evaluate how multi-flow data (traffic data running in parallel within the network nodes) contend for the network resources and impact performance. Simulations are performed simultaneously so that multiple Hosts are publishing and subscribing across different domains at the same time. The simulation parameters for the Multi-Flow configurations are detailed in Table 3. We run simulations for two Multi-Flow configurations. The Multi-Flow configuration 1 fixes the PubRate at 100 Hz for all simulations as this is the optimal PubRate used in the Jitter configuration. We then compare the results against Multi-Flow configuration 2 where the PubRate is varied for the different data transmission scenarios.

Table 3. Simulation Parameters for the Multi-Flow Configurations

Pub	Sub	Size of Data Samples (Bytes)	PubRate (Hz)	Reliability QoS Policy	Security Implemented
<i>Voice over Internet Protocol (VoIP)</i>					
H1	H2	240	100 / 50	BEST EFFORT	Yes
H1	H5	240	100 / 50	BEST EFFORT	Yes
H2	H1	240	100 / 50	BEST EFFORT	Yes
H2	H5	240	100 / 50	BEST EFFORT	Yes
H5	H1	240	100 / 50	BEST EFFORT	Yes
<i>Video Communications</i>					
H3	H1	1500	100 / 50	BEST EFFORT	Yes
H4	H5	1500	100 / 50	BEST EFFORT	Yes
H2	H1	1500	100 / 50	BEST EFFORT	Yes
<i>Drone Telemetry</i>					
H3	H1	60	100 / 30	RELIABLE	Yes
H4	H5	60	100 / 30	RELIABLE	Yes
<i>Drone Control</i>					
H1	H3	40	100 / 30	RELIABLE	Yes
H5	H4	40	100 / 30	RELIABLE	Yes

C. SELECTION OF MININET PARAMETERS

We implement the network links in Mininet with their respective flow constraints as shown in Table 4. We first look at three parameters which are the same across the simulation configurations—Maximum (Max) Queue Size, Bandwidth and Delay. These parameters must be designed within reasonable specifications or else we might not obtain any results. In the worst case, we might obtain inaccurate results. We found that forcefully transmitting data samples beyond the allocated bandwidth will lead to the Subscriber receiving zero data samples. Inspection of the traffic data in Wireshark reveals that the data samples, as well as synchronization messages in RELIABLE communications, are fragmented and transmitted in batches. This resulted in the total loss of the data samples.

For the SATCOM links, we set the parameters based on a Geostationary satellite with a buffer size (or Max Queue Size) of 100000 cells, link bandwidth of 155.52 Mbps and latency of 275 ms (earth station to earth station) [22]. Hence, the delay of each individual SATCOM link is set to 137.5 ms. For the HQ WiFi link, we set the bandwidth to 500 Mbps, the delay to 5 ms, and the buffer size to 8500 cells. This delay is based on the latency between the earth station switch and end systems presented in [22]. The buffer size of 8500 cells is based on an experimental study conducted on the sizing of the router buffer [23]. For the Trailer WiFi link, we adopt the parameters from the HQ WiFi link but change the bandwidth to 54 Mbps. This bandwidth follows the bandwidth specification of a commercially available satellite communications trailer [24]. For the Drone WiFi link, we use largely the same parameters as the Trailer WiFi link except for the delay which we change to 10 ms [25].

Table 4. Mininet Parameters for the Simulation Configurations

Network Link	Max Queue Size (Number of Cells)	Bandwidth (Mbps)	Delay (ms)	Jitter (ms)	Loss (%)
<i>Ideal Configuration</i>					
SATCOM Link	100000	155.52	137.5	0	0
HQ WiFi Link	8500	500	5	0	0
Trailer WiFi Link	8500	54	5	0	0
Drone WiFi Link	8500	54	10	0	0
<i>Jitter Configuration</i>					
SATCOM Link	100000	155.52	137.5	5	0
HQ WiFi Link	8500	500	5	1	0
Trailer WiFi Link	8500	54	5	1	0
Drone WiFi Link	8500	54	10	1	0
<i>Multi-Flow Configurations</i>					
SATCOM Link	100000	155.52	137.5	5	0.5
HQ WiFi Link	8500	500	5	1	0.1
Trailer WiFi Link	8500	54	5	1	0.1
Drone WiFi Link	8500	54	10	1	0.1

The last two parameters, Jitter and Loss, are different across the simulation configurations. As the Ideal configuration is to obtain the baseline performance, no jitter or loss are applied to this configuration. For the Jitter configuration, we apply a jitter timing of 5 ms to the SATCOM link. This is based on a mean jitter timing of about 10 ms (end-to-end transmission) measured during a satellite video transmission [26]. For the WiFi links, the jitter timing is set to 1 ms [27]. No loss is applied to the Jitter configuration because in the Throughput Test mode, the data samples are sent as fast as possible, and the network links are overloaded. Hence, we do not want to impose additional load on the network links by intentionally simulating random losses. For the Multi-Flow configurations, we use the same jitter timings as the Jitter configuration. However, as we are limiting the publishing rate, we apply a loss of 0.5% for the SATCOM link and 0.1% for the WiFi links. These add up to a maximum loss of 1.3% across the end points of our proposed architecture and is largely in line with the QoS requirements for audio and video transmissions [28].

D. SELECTION OF RTI PERFTEST PARAMETERS

We mainly adopt the default settings and QoS profiles provided by RTI Perftest.

1. QoS Profiles

The default QoS profiles for the Announcement, Throughput and Latency Topics are used. For all QoS profiles, History QoS policy is set to KEEP ALL. Durability QoS policy is set to VOLATILE for the Throughput and Latency profiles and TRANSIENT LOCAL for the Announcement profile. Reliability QoS policy are applied in accordance with Table 3.

2. Execution Time

For every data sample size, we set the execution time for the simulation to 100 s so that we are able to obtain statistically more reliable results. However, for RELIABLE communications, we experience simulation times that exceed 100 s in order to achieve a loss of 0%.

3. Transmission Mode

All simulations are transmitted, one-to-one, in unicast mode.

4. Transport Mode

Transport is set to UDPv4 (UDP that uses IP version 4) to ensure that a fixed transport protocol is used throughout the simulations. The default Transport mode is a combination of UDPv4 and Symmetric Hierarchical Memory (SHMEM). We found that this default mode causes inconsistent network link latencies that may sometimes be much smaller than expected, leading to inconsistent results across the simulations.

5. Batching

Batching is disabled for all the simulations. Nonetheless, we found that setting a batch size will increase the throughput for smaller data samples, as long as the buffer sizes meet the batch size requirements. As the data samples will be accumulated or “batched”

together before transmission, the throughput for smaller data samples will match the throughput for the selected batch size if batching is enabled.

6. Send Queue Size

The default Send Queue Size of 50 cells is used for all the simulations as we found that this value is fairly optimal for our proposed architecture. We also verified that a smaller Send Queue Size decreased throughput but did not improve the latency which remained close to the latency obtained when the default Send Queue Size was used. On the flip side, a larger Send Queue Size increased throughput at the expense of a higher latency.

7. Publishing Rate and Delay Method

For the Ideal and Jitter configurations, we use the PubRate of 100 Hz with the Spin delay method. For the Multi-Flow configurations, we apply the PubRate in accordance with Table 3 and also adopt the Spin delay method. Although the Spin delay method requires more Central Processing Unit (CPU) resources, it adopts an active wait approach and provides a higher resolution than the Sleep delay method. This means that the Publisher, using the Spin delay method, will be able to respond faster and recommence transmissions after waiting in between the sending of data samples.

8. Security

For simulations with security implemented, we use all available default security options—SecureSign, SecureEncryptDiscovery, SecureEncryptData and SecureEncryptSM.

E. SIMULATION HARDWARE AND SOFTWARE SPECIFICATIONS

The specifications of the hardware and software used to perform the simulations are as follows:

- Processor: Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz (Turbo Boost up to 4.60GHz) with 6 Cores
- Memory: 32GB Double Data Rate 4th Generation (DDR4) @ 2666MHz
- OS: Ubuntu 18.04.3

- Mininet: Version 2.2.2
- DDS Software: RTI Connex DDS 6.0.1
- Simulation Utility Software: RTI PerfTest 3.1

IV. SIMULATION RESULTS AND ANALYSIS

In this chapter, we present and discuss the simulation results and analysis for the different network configurations. As illustrated in Figure 9, for the Ideal and Jitter configurations, there are a number of permutations for the simulations. Furthermore, each of the Throughput and Latency Tests shown in Figure 9 are conducted for the five point-to-point links. The Multi-Flow configurations also comprise an additional four sets of results. Given the number of simulations and sets of results that were obtained, we do not present the detailed individual results in this chapter. Instead, we present a subset of the results and the remaining in the Appendix. For the remainder of this chapter, we analyze the results in depth for the Ideal and Jitter configurations—RELIABLE followed by BEST EFFORT communications. We then discuss the results for the Multi-Flow configurations before concluding the chapter with a summary of the results analysis.

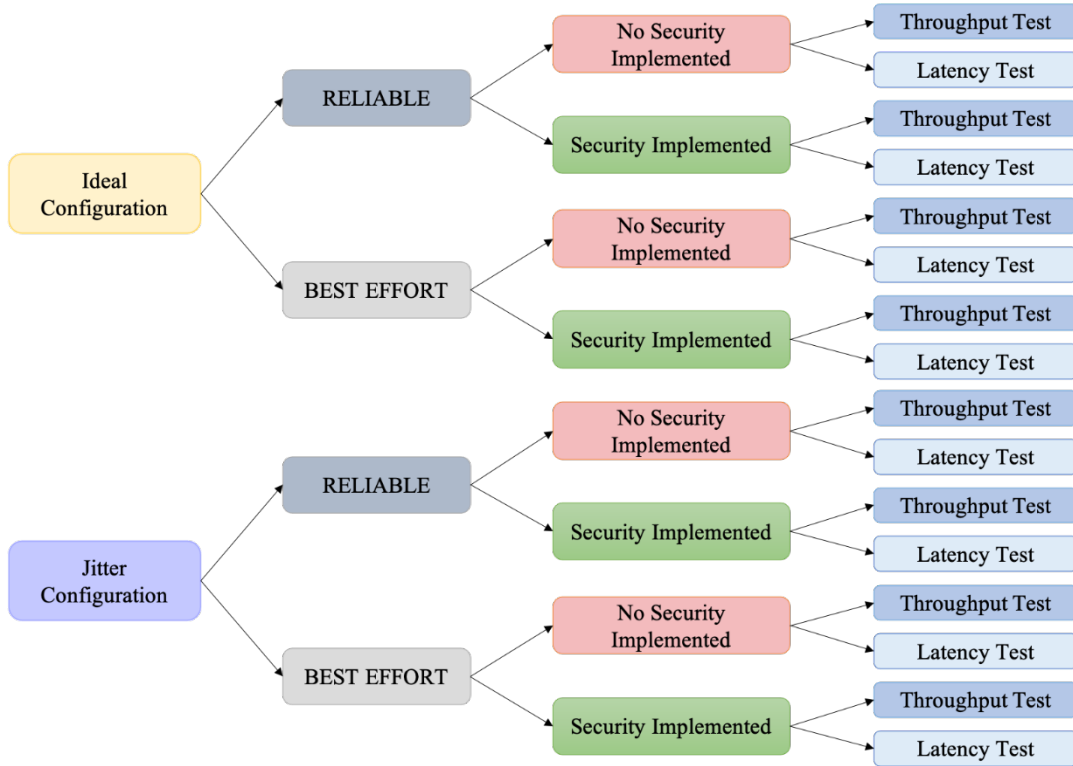


Figure 9. Permutations of Simulations for the Ideal and Jitter Configurations

For the Throughput and Latency Tests conducted in the Ideal and Jitter configurations, we reference the throughput (TH) and latency (L) results with no security implemented and calculate the overhead (OH) of implementing security. As shown in Equation 1 and 2, OH_{TH} and OH_L represents the OH for the Throughput and Latency Tests respectively (refer to the Appendix for the Throughput and Latency Tests results in the Ideal and Jitter configurations to compute the corresponding OH). A positive OH means that the OH is incurred as a result of implementing security—lower throughput and higher latency. A negative OH means that the OH is not incurred and results are better when security is implemented—higher throughput and lower latency.

$$OH_{TH} = (TH_{No_Security_Implemented} - TH_{Security_Implemented}) / TH_{No_Security_Implemented} \times 100\%. \quad (1)$$

$$OH_L = (L_{No_Security_Implemented} - L_{Security_Implemented}) / L_{No_Security_Implemented} \times 100\%. \quad (2)$$

For the Throughput Tests in the Ideal and Jitter configurations, we also tabulate the difference (Diff) in the average number (#) of data samples sent per second (DSsps), with and without security implemented. This Avg # of DSsps Diff term is represented as $DSsps_Diff_{X_Config}$ in Equation 3. The subscript, X_Config , represents the Ideal or Jitter configuration and the values of the Avg # of DSsps in the respective configurations (refer to the Appendix) are used in Equation 3 to compute the corresponding $DSsps_Diff$. A positive $DSsps_Diff$ means that there are less DS sent when security is implemented and vice versa.

$$DSsps_Diff_{X_Config} = DSsps_{X_Config_No_Security_Implemented} - DSsps_{X_Config_Security_Implemented}. \quad (3)$$

For the Multi-Flow configurations, we compare the Throughput and Latency Test results between the Multi-Flow configuration 1 and 2. The Latency Test results in all the network configurations, regardless of whether they are RELIABLE or BEST EFFORT communications, are one-way latency with 0% losses.

For this chapter, we analyze the results by reclassifying the five point-to-point links into “long links” and “short links.” Long links are links that incorporate SATCOM and have a longer RTT. The first four links (H1 to H2, H1 to H5, H1 to H3 and H2 to H5) fall

into this category. The longest end-to-end link is the H1 to H3 link. Short links are links that do not incorporate SATCOM and have a much shorter RTT. Only the H4 to H5 link falls into this category. Please refer to Figure 8 in Chapter III for reference to these links.

A. IDEAL CONFIGURATION

The Ideal configuration, without jitter and loss, forms the baseline performance for our proposed network architecture.

1. Throughput Test Results (RELIABLE)

For RELIABLE communications in the Ideal configuration, it is shown in Table 5 that the difference in the Avg # of DSsps is negligible on the long links but more pronounced on the short link. Most of the DS sizes across the long links have an average difference of 0 DSsps but this increased significantly on the short link. Similarly, the OH is more significant on the short link than the long links. The OH is between 0% and 1.39% on the long links, with the highest OH recorded at 1.39% on the H1 to H3 link. On the short link, the OH is between 0% and 5.27%. We assess that the OH for the short link is more significant than the long link because the OH in implementing security remains the same for both the long and short links. However, the resources required to transmit the data over the short link is much less than the long links. Along the long links, we also observe that the OH is only present in the larger DS of 16384 B and 63000 B. We presume this to be the effect of fragmentation during the transmission of larger DS over the long links. The higher OH for the larger DS are not present on the short link.

Table 5. Throughput Test Results—Comparison of Avg # of DSsps Diff and OH for the Point-to-Point Links in the Ideal Configuration (RELIABLE)

Data Sample Size (Bytes)	H1 (Pub) to H2 (Sub) Link		H1 (Pub) to H5 (Sub) Link		H1 (Pub) to H3 (Sub) Link		H2 (Pub) to H5 (Sub) Link		H4 (Pub) to H5 (Sub) Link	
	Avg # of DSsps Diff	OH (%)	Avg # of DSsps Diff	OH (%)	Avg # of DSsps Diff	OH (%)	Avg # of DSsps Diff	OH (%)	Avg # of DSsps Diff	OH (%)
32	0	0.00	0	0.00	0	0.00	0	0.00	27	0.00
64	0	0.00	0	0.00	0	0.00	0	0.00	25	0.00
128	0	0.00	0	0.00	0	0.00	0	0.00	23	4.00
256	0	0.00	0	0.00	0	0.00	0	0.00	27	0.00
512	0	0.00	0	0.00	0	0.00	0	0.00	33	2.04
1024	0	0.00	0	0.00	0	0.00	0	0.00	29	1.05
2048	0	0.00	0	0.00	0	0.00	0	0.00	11	0.55
4096	0	0.00	0	0.00	0	0.00	0	0.00	83	5.27
8192	0	0.00	1	0.00	0	0.00	0	0.00	27	3.49
16384	0	0.00	1	0.88	0	0.00	1	0.00	10	2.51
32768	0	0.43	0	0.45	1	1.39	1	0.45	4	2.12
63000	0	0.23	0	0.73	1	0.25	0	0.48	2	1.92

2. Latency Test Results (RELIABLE)

For the long links in the Ideal configuration, it is shown in Table 6 that the OH of 0.14% or less is negligible across the DS sizes for RELIABLE communications. On the short link, the OH is visibly higher compared to the long links but is still considered relatively low at 1.64% or less. We assess that the higher OH for the short link is more significant than the long link because the encryption time remains the same for both the long and short links. However, the RTT for the short link is much smaller than the long links. We also observe in Table 6 that the OH increased with the size of DS across all the links.

Table 6. Latency Test Results—Comparison of OH for the Point-to-Point Links in the Ideal Configuration (RELIABLE)

Data Sample Size (Bytes)	H1 (Pub) to H2 (Sub) Link	H1 (Pub) to H5 (Sub) Link	H1 (Pub) to H3 (Sub) Link	H2 (Pub) to H5 (Sub) Link	H4 (Pub) to H5 (Sub) Link
	OH (%)	OH (%)	OH (%)	OH (%)	OH (%)
32	0.02	0.02	0.02	0.02	0.42
64	0.02	0.02	0.01	0.02	0.40
128	0.02	0.02	0.02	0.02	0.39
256	0.02	0.02	0.01	0.01	0.47
512	0.02	0.01	0.02	0.02	0.45
1024	0.02	0.01	0.03	0.02	0.46
2048	0.02	0.01	0.02	0.02	0.49
4096	0.02	0.02	0.03	0.01	0.56
8192	0.03	0.03	0.03	0.03	0.62
16384	0.05	0.05	0.05	0.05	0.85
32768	0.07	0.07	0.06	0.07	1.17
63000	0.13	0.14	0.13	0.10	1.64

3. Throughput Test Results (BEST EFFORT at PubRate 100 Hz)

In Chapter III, we showed that BEST EFFORT communications, for a PubRate of 100 Hz, in the Ideal configuration do not result in any losses on the H1 to H3 link. We further verify that there are no losses across the rest of the links. The results in Table 7 show that the Avg # of DSsps Diff across all the links is negligible. However, more DS sizes have a difference of 1 DSsps compared to RELIABLE communications where the difference for most of the DS sizes is 0 DSsps. The OH between 0% and 1.52% is also largely similar across all the long and short links. This is because we limit the PubRate to 100 Hz in order to achieve 0% loss across all the DS sizes. Similar to the results for RELIABLE communications, choosing a higher PubRate will result in a larger OH on the short link.

Table 7. Throughput Test Results—Comparison of Avg # of DSsps Diff and OH for the Point-to-Point Links in the Ideal Configuration (BEST EFFORT)

Data Sample Size (Bytes)	H1 (Pub) to H2 (Sub) Link		H1 (Pub) to H5 (Sub) Link		H1 (Pub) to H3 (Sub) Link		H2 (Pub) to H5 (Sub) Link		H4 (Pub) to H5 (Sub) Link	
	Avg # of DSsps Diff	OH (%)	Avg # of DSsps Diff	OH (%)	Avg # of DSsps Diff	OH (%)	Avg # of DSsps Diff	OH (%)	Avg # of DSsps Diff	OH (%)
32	0	0.00	0	0.00	0	0.00	1	1.00	0	0.00
64	1	0.00	1	0.00	1	0.00	1	0.00	1	0.00
128	0	0.00	1	0.00	0	0.00	1	0.00	1	0.00
256	1	0.00	1	0.00	0	0.00	1	0.00	1	0.00
512	0	0.00	0	0.00	1	0.00	1	0.00	1	0.00
1024	1	0.00	0	0.00	0	0.00	1	0.00	1	0.00
2048	0	0.00	0	0.00	1	0.00	0	0.00	1	0.00
4096	1	0.00	0	0.00	1	0.00	1	0.00	1	0.00
8192	1	1.52	1	0.00	1	1.52	1	1.52	1	1.52
16384	1	0.00	1	0.00	1	0.00	1	0.00	1	0.00
32768	1	0.38	1	0.76	1	0.00	1	0.38	1	0.38
63000	1	0.59	1	0.20	1	0.40	1	0.20	0	0.00

4. Latency Test Results (BEST EFFORT at PubRate 100 Hz)

The latency results for BEST EFFORT communications are similar to RELIABLE communications in the Ideal configuration. Table 8 shows a negligible OH of 0.09% or less across all the DS sizes on the long links. On the short links, the OH of 1.69% or less is close to the OH of 1.64% for RELIABLE communications. Similarly, we observe that the OH generally increased with the size of the DS across all the links.

Table 8. Latency Test Results—Comparison of OH for the Point-to-Point Links in the Ideal Configuration (BEST EFFORT)

Data Sample Size (Bytes)	H1 (Pub) to H2 (Sub) Link	H1 (Pub) to H5 (Sub) Link	H1 (Pub) to H3 (Sub) Link	H2 (Pub) to H5 (Sub) Link	H4 (Pub) to H5 (Sub) Link
	OH (%)	OH (%)	OH (%)	OH (%)	OH (%)
32	0.02	0.02	0.01	0.02	0.23
64	0.03	0.02	0.02	0.02	0.32
128	0.02	0.01	0.01	0.02	0.43
256	0.02	0.01	0.02	0.02	0.55
512	0.02	0.02	0.02	0.02	0.63
1024	0.02	0.01	0.02	0.02	0.48
2048	0.02	0.02	0.02	0.01	0.55
4096	0.02	0.02	0.02	0.03	0.61
8192	0.03	0.03	0.02	0.03	0.65
16384	0.03	0.03	0.03	0.05	0.92
32768	0.06	0.05	0.05	0.06	1.22
63000	0.09	0.09	0.08	0.09	1.69

B. JITTER CONFIGURATION

In the Jitter configuration, we introduce jitter, without loss, to our proposed network architecture detailed in Table 4 in Chapter III.

1. Throughput Test Results (RELIABLE)

For the long links, it is shown in Table 9 that introducing jitter for RELIABLE communications results in a variable OH between -8.33% and 11.11%. We do not think that the negative OH is a true representation of the OH incurred because it is not practical to achieve better performance results when security is implemented. We assess that the negative OH is an artifact of adding jitter, coupled with the long RTT on the long links, leading to the DS arriving at the Subscriber with a much larger variation or standard deviation compared to the Ideal configuration. First, our results for RELIABLE communications in the Ideal configuration show that the OH on the long links is small and hardly noticeable; the OH is only recorded for the large DS of 32768 B and 63000 B at 1.39% or less. Second, in terms of absolute numbers, the Avg # of DSsps Diff is within ± 5 DSsps which does not deviate drastically from the Ideal configuration result of 1 DSsps.

Third, the variation only manifests in the DS greater than or equal to 2048 B which is consistent with the effect of jitter and transmission of larger fragmented DS over the long links. Hence, we conclude that the OH in the Jitter configuration is “hidden” inside the jitter timings, coupled with the long RTT, on the long links.

It is shown in Table 9 that, unlike the long links, the OH is not “hidden” and is generally positive for the DS greater than or equal to 512 B. There are two DS sizes (16384 B and 32768 B) that show a large negative OH of -429.69% and -87.93% (highlighted in yellow in Table 9). We assess that these are outlier points and the OH should be positive on the short link. This large negative OH warrants a deeper investigation for future work. With the exception of the two outlier points, the OH of 4.26% or less is close to the Ideal configuration result of 5.27% or less. Hence, the effect of jitter and variability are hardly noticeable on the short link.

Table 9. Throughput Test Results—Comparison of Avg # of DSsps Diff and OH for the Point-to-Point Links in the Jitter Configuration (RELIABLE)

Data Sample Size (Bytes)	H1 (Pub) to H2 (Sub) Link		H1 (Pub) to H5 (Sub) Link		H1 (Pub) to H3 (Sub) Link		H2 (Pub) to H5 (Sub) Link		H4 (Pub) to H5 (Sub) Link	
	Avg # of DSsps Diff	OH (%)	Avg # of DSsps Diff	OH (%)	Avg # of DSsps Diff	OH (%)	Avg # of DSsps Diff	OH (%)	Avg # of DSsps Diff	OH (%)
32	0	0.00	0	0.00	0	0.00	0	0.00	15	0.00
64	0	0.00	0	0.00	0	0.00	0	0.00	14	0.00
128	0	0.00	0	0.00	0	0.00	0	0.00	14	0.00
256	0	0.00	0	0.00	0	0.00	0	0.00	16	0.00
512	0	0.00	0	0.00	0	0.00	0	0.00	24	1.06
1024	0	0.00	0	0.00	0	0.00	0	0.00	11	0.56
2048	-2	0.00	-4	0.00	2	0.00	5	9.09	16	0.92
4096	1	0.00	1	0.00	-1	0.00	1	0.00	48	4.26
8192	1	0.00	-1	0.00	2	3.70	2	6.90	13	2.48
16384	1	8.33	-1	-4.00	-1	-4.35	2	11.11	-209	-429.69
32768	-1	-6.67	-1	-6.90	-1	-7.14	0	-4.17	-58	-87.93
63000	0	-8.33	0	-8.33	-1	-2.94	0	0.00	2	3.94

2. Latency Test Results (RELIABLE)

Similar to the Latency Test results for RELIABLE communications in the Ideal configuration, Table 10 shows that the OH recorded is between -0.1% and 0.32% and the impact of adding jitter is negligible on the long links. As mentioned in the previous section, we do not think that the negative OH is a true representation of the OH incurred. We assess that this is an artifact of adding jitter, coupled with the long RTT on the long links, leading to a larger standard deviation in the latency timings compared to the Ideal configuration. The latency timings recorded also have lower minimum and higher maximum latencies compared to the Ideal configuration (refer to the detailed Latency Test results in the Appendix). Latency results for the short link are also similar to the Ideal configuration. The OH numbers recorded are all positive and are slightly higher at 1.74% or less (compared to 1.64% or less in the Ideal configuration). We also observe that the OH generally increased with the larger DS.

Table 10. Latency Test Results—Comparison of OH for the Point-to-Point Links in the Jitter Configuration (RELIABLE)

Data Sample Size (Bytes)	H1 (Pub) to H2 (Sub) Link	H1 (Pub) to H5 (Sub) Link	H1 (Pub) to H3 (Sub) Link	H2 (Pub) to H5 (Sub) Link	H4 (Pub) to H5 (Sub) Link
	OH (%)	OH (%)	OH (%)	OH (%)	OH (%)
32	-0.03	-0.04	0.05	0.02	0.40
64	0.19	0.06	0.13	0.21	0.54
128	0.05	0.09	0.10	0.10	0.55
256	-0.04	-0.07	-0.08	0.06	0.51
512	0.21	0.00	-0.10	0.03	0.55
1024	0.32	0.21	-0.02	0.18	0.49
2048	0.10	-0.02	0.12	0.06	0.51
4096	-0.08	0.03	-0.01	0.06	0.65
8192	-0.02	0.04	0.00	0.20	0.73
16384	0.01	0.08	0.04	-0.01	1.21
32768	0.02	0.09	0.00	0.08	1.61
63000	0.13	0.13	0.17	0.09	1.74

3. Throughput Test Results (BEST EFFORT at PubRate 100 Hz)

At a PubRate of 100 Hz, the Throughput Test for BEST EFFORT communications in the Jitter configuration results in DS losses. Hence, we add the “Loss” field to Table 11 to enable a more holistic analysis. It is shown in Table 11 that the Avg # of DSsps Diff is almost all 0 DSsps across the links. The OH is also generally all 0%. For the few DS sizes that incur OH, the OH stays between -1.06% and 3.03%. Similar to RELIABLE communications, we assess that the negative OH is not a true representation of the OH incurred. Compared to RELIABLE communications, the effect of jitter and variability for BEST EFFORT communications are also less significant when the PubRate is throttled.

With regard to the losses on the long links, it is shown in Table 11 that they are all within 4.91% and decreased as the DS size increased. No losses are recorded for the DS of 16384 B and 63000 B. This observation differs from the earlier observations for the Ideal configuration where the losses increased as the DS size increased (refer to Table 2 in Chapter III). We assess that this observation, regarding losses on the long links, should also be similar to the Ideal configuration. We should expect to see an increase in the losses of larger DS due to the effect of fragmentation during the transmission of larger DS. This observation is also not present on the short link where all the losses are negligible; almost all are 0% except the result of 0.2% for the DS of 63000 B. Further investigation will have to be conducted for future work to examine the relationship between jitter, PubRate, and losses on both the long and short links.

Table 11. Throughput Test Results—Comparison of Avg # of DSsps Diff, OH and Loss for the Point-to-Point Links in the Jitter Configuration (BEST EFFORT)

Data Sample Size (Bytes)	H1 (Pub) to H2 (Sub) Link			H1 (Pub) to H5 (Sub) Link			H1 (Pub) to H3 (Sub) Link			H2 (Pub) to H5 (Sub) Link			H4 (Pub) to H5 (Sub) Link		
	Avg # of DSsps Diff	OH (%)	Loss (%)	Avg # of DSsps Diff	OH (%)	Loss (%)	Avg # of DSsps Diff	OH (%)	Loss (%)	Avg # of DSsps Diff	OH (%)	Loss (%)	Avg # of DSsps Diff	OH (%)	Loss (%)
32	1	1.04	4.20	0	0.00	4.64	0	0.00	4.91	0	0.00	4.38	0	0.00	0.00
64	0	0.00	4.43	0	0.00	4.65	-1	-1.06	4.61	0	0.00	4.32	0	0.00	0.00
128	0	0.00	4.43	1	0.00	4.84	0	0.00	4.59	0	0.00	4.52	0	0.00	0.00
256	0	0.00	4.76	0	0.00	4.42	-1	0.00	4.76	0	0.00	4.11	0	0.00	0.00
512	0	0.00	4.13	0	0.00	4.32	0	0.00	4.73	0	0.00	4.55	0	0.00	0.00
1024	0	0.00	4.39	0	0.00	4.74	0	0.00	4.62	0	0.00	4.55	0	0.00	0.00
2048	0	0.00	1.60	0	0.00	1.69	0	0.00	1.99	0	0.00	1.66	0	0.00	0.00
4096	0	0.00	0.77	0	3.03	0.77	0	0.00	0.94	0	3.03	0.66	0	0.00	0.00
8192	0	0.00	0.04	0	0.00	0.02	0	0.00	0.10	0	0.00	0.11	0	0.00	0.00
16384	0	0.00	0.00	0	0.00	0.01	0	0.00	0.01	0	0.00	0.00	0	0.00	0.00
32768	0	0.00	0.00	0	0.00	0.00	0	0.00	0.00	0	0.00	0.00	-1	0.00	0.00
63000	0	-0.20	0.00	0	0.00	0.00	0	0.00	0.00	0	0.00	0.00	0	0.20	0.00

4. Latency Test Results (BEST Effort at PubRate 100 Hz)

For the Jitter configuration, the Latency Test results for BEST EFFORT communications are similar to the results for RELIABLE communications. As shown in Table 12, the OH on the long links is between -0.22% and 0.34%. This is slightly higher than the results for RELIABLE communications (between -0.1% and 0.32%) but is still negligible. Once again, we assess that the negative OH is not a true representation of the OH incurred. On the short link, the OH is all positive at 1.79% or less. This is also slightly higher than the results for RELIABLE communications (1.74% or less). In addition, we observe that the OH generally increased with the larger DS.

Table 12. Latency Test Results—Comparison of OH for the Point-to-Point Links in the Jitter Configuration (BEST EFFORT)

Data Sample Size (Bytes)	H1 (Pub) to H2 (Sub) Link	H1 (Pub) to H5 (Sub) Link	H1 (Pub) to H3 (Sub) Link	H2 (Pub) to H5 (Sub) Link	H4 (Pub) to H5 (Sub) Link
	OH (%)	OH (%)	OH (%)	OH (%)	OH (%)
32	0.07	0.03	-0.02	0.34	0.18
64	0.03	0.02	0.05	0.02	0.28
128	-0.22	0.12	-0.04	-0.06	0.24
256	0.03	0.28	0.00	0.01	0.41
512	0.03	-0.15	0.07	0.03	0.52
1024	0.11	0.00	-0.10	-0.11	0.50
2048	0.06	0.09	-0.07	-0.05	0.66
4096	-0.06	0.07	0.06	-0.05	0.74
8192	0.15	0.06	0.14	-0.08	0.73
16384	0.13	0.07	0.02	0.00	1.15
32768	0.03	0.06	0.14	0.06	1.47
63000	0.11	0.05	0.14	0.13	1.79

C. MULTI-FLOW CONFIGURATIONS

In the Multi-Flow configurations, we introduce jitter and loss to our proposed network architecture detailed in Table 4 in Chapter III and perform the simulations concurrently. All simulations in the Multi-Flow configurations also have security implemented. The PubRate for the Multi-Flow configuration 1 is fixed at 100 Hz. For the

Multi-Flow configuration 2, the PubRate of 50 Hz is used for secure VoIP and video communications while 30 Hz is used for secure drone control and telemetry.

1. Throughput Test Results

For the Multi-Flow configurations, we use the respective PubRate as reference and compute the Avg # of DSsps Diff between the actual PubRate and the reference PubRate. The Avg # of DSsps Diff is represented as $DSsps_Diff_{Multi-Flow_Config_Y}$ as shown in Equation 4. The subscript, Multi-Flow_Config_Y, represents the Multi-Flow configuration 1 or 2 and values of the Avg # of DSsps in the respective Multi-Flow configurations (refer to the Appendix) are used in Equation 4 to compute the corresponding DSsps_Diff. This allows us to have a sense of how well the DDS system copes with the demands of maintaining a constant PubRate in a loaded network scenario.

$$DSsps_Diff_{Multi-Flow_Config_Y} = DSsps_{Multi-Flow_Config_Y} - PubRate_{Multi-Flow_Config_Y} \quad (4)$$

For the Multi-Flow configuration 1, it is shown in Table 13 that there is an average drop of 8 DSsps or less for BEST EFFORT communications on both the long and short links. For RELIABLE communications, DDS maintains an average drop of 5 DSsps or less on the short link. However, there is a huge drop of 41 DSsps or less on the H1 to H3 link (the longest end-to-end link). With regard to the losses for BEST EFFORT communications in the Multi-Flow configuration 1, Table 13 shows that there are high losses between 3.64% and 8.57% on the long links, but negligible loss of 0.15% on the short link.

For the Multi-Flow configuration 2, Table 13 shows that the Avg # of DSsps Diff is 5 DSsps or less for BEST EFFORT communications which is slightly lower than the result in the Multi-Flow configuration 1 (8 DSsps or less). For RELIABLE communications, DDS maintains an average drop of 3 DSsps or less on the short link and 8 DSsps or less on the H1 to H3 link. These are lower than the results in the Multi-Flow configuration 1 (5 DSsps or less on the short link and 41 DSsps or less on the H1 to H3 link). With regard to the losses for BEST EFFORT communications in the Multi-Flow configuration 2, it is shown in Table 13 that the loss between 0.86% and 2.49% on the long

links are fairly acceptable. On the short link, the loss of 0.31% is negligible. Hence, we conclude that if the PubRate is properly throttled, we are able to achieve lower losses, as well as more consistent throughput performance than the Multi-Flow configuration 1.

Table 13. Throughput Test Results—Comparison of Avg # of DSsps and Loss between Multi-Flow Configuration 1 and 2

Pub	Sub	Data Sample Size (Bytes)	Reliability QoS Policy	Multi-Flow Configuration 1		Multi-Flow Configuration 2	
				Avg # of DSsps Diff	Loss (%)	Avg # of DSsps Diff	Loss (%)
Secure VoIP							
H1	H2	240	BEST EFFORT	-5	5.72	-3	0.86
H1	H5	240	BEST EFFORT	4	8.57	-1	1.31
H2	H1	240	BEST EFFORT	-5	5.70	-3	1.39
H2	H5	240	BEST EFFORT	-5	5.85	11	1.19
H5	H1	240	BEST EFFORT	-5	6.41	-2	1.20
Secure Video Communications							
H3	H1	1500	BEST EFFORT	-3	4.82	-5	2.49
H4	H5	1500	BEST EFFORT	-2	0.15	-2	0.31
H2	H1	1500	BEST EFFORT	-8	3.64	-4	2.07
Secure Drone Telemetry							
H3	H1	60	RELIABLE	-40	0.00	-7	0.00
H4	H5	60	RELIABLE	-5	0.00	-3	0.00
Secure Drone Control							
H1	H3	40	RELIABLE	-41	0.00	-8	0.00
H5	H4	40	RELIABLE	-1	0.00	-3	0.00

2. Latency Test Results

For the Latency Test in the Multi-Flow configurations, we found that there are no DS received at the Subscriber end for BEST EFFORT communications when both BEST EFFORT and RELIABLE simulations are performed concurrently. However, the DS are received at the Subscriber end for RELIABLE communications. We assess that this could be due to competing demands when the simulations are running concurrently, and the DDS system makes no effort to ensure that the DS are received for BEST EFFORT

communications. Thus, instead of following the BEST EFFORT Reliability QoS policy detailed in Table 3 in Chapter III, we change them to RELIABLE as shown in Table 14.

Referencing the average latency results for the Multi-Flow configuration 1, we compute the Avg Latency Difference (L_Diff) as shown in Equation 5 (refer to the Appendix for the Latency Test results in the Multi-Flow configurations to compute the L_Diff).

$$L_Diff = (L_{Multi-Flow_Config_1} - L_{Multi-Flow_Config_2}) / L_{Multi-Flow_Config_1} \times 100\% . \quad (5)$$

It is shown in Table 14 that the difference between the Multi-Flow configuration 1 and 2 varies between -3.16% and 4.5%. Hence, there is only a low impact, variability of $\pm 4.5\%$, on latency when the PubRate is throttled.

Table 14. Latency Test Results—Comparison of Avg Latency between Multi-Flow Configuration 1 and 2

Pub	Sub	Data Sample Size (Bytes)	Reliability QoS Policy	Multi-Flow Configuration 1	Multi-Flow Configuration 2	Avg Latency Difference (%)
				Avg Latency (ms)	Avg Latency (ms)	
Secure VoIP						
H1	H2	240	RELIABLE	288.38	286.98	0.49
H1	H5	240	RELIABLE	288.37	294.08	-1.98
H2	H1	240	RELIABLE	285.10	284.09	0.35
H2	H5	240	RELIABLE	297.21	283.84	4.50
H5	H1	240	RELIABLE	289.04	298.18	-3.16
Secure Video Communications						
H3	H1	1500	RELIABLE	309.02	317.38	-2.70
H4	H5	1500	RELIABLE	10.46	10.48	-0.18
H2	H1	1500	RELIABLE	291.37	295.37	-1.38
Secure Drone Telemetry						
H3	H1	60	RELIABLE	307.09	309.28	-0.71
H4	H5	60	RELIABLE	10.11	10.09	0.12
Secure Drone Control						
H1	H3	40	RELIABLE	299.66	304.67	-1.67
H5	H4	40	RELIABLE	10.11	10.08	0.36

D. SUMMARY OF RESULTS ANALYSIS

To summarize our results, the Ideal and Jitter configurations are evaluated for the five point-to-point links which we have reclassified as long or short links depending on their RTT. The simulations for these configurations are also performed across the various DS sizes for RELIABLE and BEST EFFORT communications, as well as with and without DDS security implemented. For the Multi-Flow configurations, we perform simulations based on the scenarios to evaluate how multi-flow data contend for the network resources and impact performance.

The Ideal configuration forms the baseline performance for the proposed network architecture. Our results show that, for RELIABLE communications, the throughput OH is more significant on the short link (5.27% or less) than the long links (1.39% or less). For BEST EFFORT communications, the throughput OH of 1.52% or less remains largely similar across all the long and short links because we limit the PubRate to 100 Hz to achieve a 0% loss across all the DS sizes. The latency OH, for both RELIABLE and BEST EFFORT communications, is more significant on the short link (within 1.7% or less) than the long links (within 0.15% or less). It also generally increased when the size of the DS increased.

In the Jitter configuration, our results show that the DS arrive at the Subscriber with a much larger standard deviation compared to the Ideal configuration and this leads to both positive and negative OH. We assess that the negative OH is not a true representation of the OH incurred and the OH is “hidden” inside the jitter timings, coupled with the long RTT, on the long links. For RELIABLE communications, the throughput OH on the long links remains within a variability of $\pm 11.15\%$. On the short link, with the exception of the two outlier points, we assess that the throughput OH should all be positive. The effect of jitter and variability are less significant on the short link; the OH of 4.26% or less is close to the results of 5.27% or less in the Ideal configuration. For BEST EFFORT communications, the throughput OH on the long and short links is largely negligible (within $\pm 0.2\%$), with the exception of a few points for the long links which exhibit a slightly higher variability (within $\pm 3.05\%$). Hence, the effects of jitter and variability are also less significant when the PubRate is throttled. The simulations for BEST EFFORT

communications result in losses of 4.91% or less on the long links and these losses decreased as the DS size increased. For the latency OH for both RELIABLE and BEST EFFORT communications, our results show that it is more significant on the short link (within 1.8%) than the long links (within $\pm 0.35\%$). It also generally increased when the size of the DS increased.

Lastly, we conclude from the results of the Multi-Flow configurations that if the PubRate is properly throttled in a loaded network scenario, we are able to achieve low losses (2.49% or less), as well as more consistent throughput performance. Throttling the PubRate in a loaded network scenario also has a low impact on latency (within $\pm 4.5\%$).

V. CONCLUSIONS

In this chapter, we provide a summary of the highlights and key findings of this thesis and make recommendations for future work.

A. SUMMARY

Unmanned systems have been a key asset for military operations, and to fully exploit their capabilities, improved autonomy and interoperability is of paramount importance. To ensure interoperability and greater autonomy, a cohesive communications protocol that allows unmanned systems to be networked together is required. DDS is a middleware and a prime candidate for the cohesive communications protocol that the PMW760 desires.

We have proposed a network architecture that fits the PMW760 Naval use case criteria. This network architecture incorporates SATCOM and WiFi links to enable us to evaluate the performance of DDS as the backbone communications protocol. We used Mininet to setup the network parameters and RTI PerfTest as the performance testing utility tool.

We have evaluated the throughput and latency performance of DDS in different network configurations—Ideal, Jitter and Multi-Flow. For RELIABLE communications, the simulations were conducted by sending the DS as fast as possible. In the Ideal configuration, we have shown that the throughput OH is small (5.27% or less) on both the long and short links. It is also more prominent on the short link than the long link because the OH in implementing security remains the same for both the long and short links. However, the resources required to transmit the data over the short links is much less than the long links. In the Jitter configuration, we have found that the DS arrive at the Subscriber with a much larger standard deviation compared to the Ideal configuration and this leads to both positive and negative OH. On the long links, we assess that the negative OH is not a true representation of the OH incurred and the throughput OH is “hidden” in the jitter timings, coupled with the long RTT. On the short link, the throughput OH should all be positive and results are similar to the Ideal configuration. For BEST EFFORT

communications in the Ideal and Jitter configurations, the PubRate is throttled and our results have shown that the throughput OH remains relatively similar across all the long and short links. For the latency OH, for RELIABLE and BEST EFFORT communications in the Ideal and Jitter configurations, we have shown that it is relatively low (1.79% or less) on the short link and negligible on the long links. It also generally increased as the size of the DS increased. In the Multi-Flow configurations, we have shown that, in a loaded network scenario, we are able to achieve low losses (2.49% or less), as well as more consistent throughput performance with a low impact on latency (within $\pm 4.5\%$) by choosing a suitable PubRate.

Lastly, two key insights gleaned from our results are (1) throughput depends on the PubRate and the size of the DS, and (2) there is no significant impact on latency even though latency generally increased with the size of the DS. Hence, for our proposed network architecture with long links (SATCOM) and short links (WiFi), it is important to transmit the DS at the optimal size and PubRate to achieve consistent throughput performance with low losses and OH. Choosing a suitable PubRate also reduces the effect of jitter and variability. We recommend using high PubRate and large DS sizes for the short links so that high throughput with low losses and latency can be leveraged. On the other hand, a calibrated PubRate and small DS sizes will be more effective for the long links to reduce variability and losses and achieve consistent throughput performance; albeit achieving lower throughput compared to the short links. Although there are other middleware technologies (for example ZeroMQ), we assess that DDS, and the RTPS protocol, is a proven technology that complies to standards and satisfies both performance and security requirements for our proposed architecture.

B. RECOMMENDATIONS FOR FUTURE WORK

For future work, we recommend that the following be performed:

- Investigate the points of interest derived from this thesis: For RELIABLE communications in the Jitter configuration, investigate why the two outlier points (the DS of 16384 B and 63000 B) showed a large negative throughput OH on the short link. For BEST EFFORT communications in

the Jitter configuration, investigate why the losses decreased as the DS sizes increased on the long links, and examine the relationship between jitter, PubRate, and losses on both the long and short links.

- Scaling the proposed network architecture: Scalability is important to enable unmanned swarm operations. Hence, increasing the scale of network nodes to evaluate the performance of DDS in the Multi-Flow configurations will be beneficial.
- Setup a testbed comprising real and simulated network nodes: The real network nodes will bring in real constraints from the world to offer a more realistic DDS performance evaluation. Integrating real network traffic into simulated network traffic will also enable us to evaluate the limitations of DDS.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. DETAILED SIMULATION RESULTS

In this chapter, we present the detailed simulation results for all the permutations in the Ideal, Jitter and Multi-Flow configurations. For both the Throughput and Latency Tests in the Ideal and Jitter configurations, we present the results with and without security implemented and compute the OH. In particular, we present the Avg # of DSsps, Avg Throughput, and Loss for the Throughput Tests, and Minimum (Min), Maximum, and Avg one-way latencies for the Latency Tests. For the Multi-Flow configurations, we present the same results, except computing the OH, because all the simulations had security implemented.

A. IDEAL CONFIGURATION

1. Throughput Test Results (RELIABLE)

Tables 15 to 19 shows the Throughput Test results—comparison with and without security for RELIABLE communications in the Ideal configuration for the five point-to-point links.

Table 15. Throughput Test Results—Comparison With and Without Security for H1 to H2 Link for Ideal Configuration (RELIABLE)

Throughput Test Results for H1 (Pub) to H2 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
32	256	89	0.023	0.00	89	0.023	0.00	0.00
64	512	89	0.046	0.00	89	0.046	0.00	0.00
128	1024	89	0.1	0.00	89	0.1	0.00	0.00
256	2048	89	0.2	0.00	89	0.2	0.00	0.00
512	4096	89	0.4	0.00	89	0.4	0.00	0.00
1024	8192	89	0.7	0.00	89	0.7	0.00	0.00
2048	16384	89	1.5	0.00	89	1.5	0.00	0.00
4096	32768	89	2.9	0.00	89	2.9	0.00	0.00
8192	65536	89	5.8	0.00	89	5.8	0.00	0.00

Throughput Test Results for H1 (Pub) to H2 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
16384	131072	88	11.6	0.00	88	11.6	0.00	0.00
32768	262144	87	23	0.00	87	22.9	0.00	0.43
63000	504000	86	43.6	0.00	86	43.5	0.00	0.23

Table 16. Throughput Test Results—Comparison With and Without Security for H1 to H5 Link for Ideal Configuration (RELIABLE)

Throughput Test Results for H1 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
32	256	87	0.022	0.00	87	0.022	0.00	0.00
64	512	87	0.045	0.00	87	0.045	0.00	0.00
128	1024	87	0.1	0.00	87	0.1	0.00	0.00
256	2048	87	0.2	0.00	87	0.2	0.00	0.00
512	4096	87	0.4	0.00	87	0.4	0.00	0.00
1024	8192	87	0.7	0.00	87	0.7	0.00	0.00
2048	16384	87	1.4	0.00	87	1.4	0.00	0.00
4096	32768	87	2.9	0.00	87	2.9	0.00	0.00
8192	65536	87	5.7	0.00	86	5.7	0.00	0.00
16384	131072	86	11.3	0.00	85	11.2	0.00	0.88
32768	262144	84	22.2	0.00	84	22.1	0.00	0.45
63000	504000	81	41.3	0.00	81	41	0.00	0.73

Table 17. Throughput Test Results—Comparison With and Without Security for H1 to H3 Link for Ideal Configuration (RELIABLE)

Throughput Test Results for H1 (Pub) to H3 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSps	Avg Throughput (Mbps)	Loss (%)	
32	256	84	0.022	0.00	84	0.022	0.00	0.00
64	512	84	0.043	0.00	84	0.043	0.00	0.00
128	1024	84	0.1	0.00	84	0.1	0.00	0.00
256	2048	84	0.2	0.00	84	0.2	0.00	0.00
512	4096	84	0.3	0.00	84	0.3	0.00	0.00
1024	8192	84	0.7	0.00	84	0.7	0.00	0.00
2048	16384	84	1.4	0.00	84	1.4	0.00	0.00
4096	32768	84	2.8	0.00	84	2.8	0.00	0.00
8192	65536	84	5.5	0.00	84	5.5	0.00	0.00
16384	131072	83	10.9	0.00	83	10.9	0.00	0.00
32768	262144	82	21.6	0.00	81	21.3	0.00	1.39
63000	504000	79	39.9	0.00	78	39.8	0.00	0.25

Table 18. Throughput Test Results—Comparison With and Without Security for H2 to H5 Link for Ideal Configuration (RELIABLE)

Throughput Test Results for H2 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSps	Avg Throughput (Mbps)	Loss (%)	
32	256	89	0.023	0.00	89	0.023	0.00	0.00
64	512	89	0.046	0.00	89	0.046	0.00	0.00
128	1024	89	0.1	0.00	89	0.1	0.00	0.00
256	2048	89	0.2	0.00	89	0.2	0.00	0.00
512	4096	89	0.4	0.00	89	0.4	0.00	0.00
1024	8192	89	0.7	0.00	89	0.7	0.00	0.00
2048	16384	89	1.5	0.00	89	1.5	0.00	0.00
4096	32768	88	2.9	0.00	88	2.9	0.00	0.00
8192	65536	88	5.8	0.00	88	5.8	0.00	0.00
16384	131072	88	11.5	0.00	87	11.5	0.00	0.00

Throughput Test Results for H2 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
32768	262144	85	22.3	0.00	84	22.2	0.00	0.45
63000	504000	82	41.8	0.00	82	41.6	0.00	0.48

Table 19. Throughput Test Results—Comparison With and Without Security for H4 to H5 Link for Ideal Configuration (RELIABLE)

Throughput Test Results for H4 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
32	256	2412	0.6	0.00	2385	0.6	0.00	0.00
64	512	2411	1.2	0.00	2386	1.2	0.00	0.00
128	1024	2409	2.5	0.00	2386	2.4	0.00	4.00
256	2048	2409	4.9	0.00	2382	4.9	0.00	0.00
512	4096	2386	9.8	0.00	2353	9.6	0.00	2.04
1024	8192	2319	19	0.00	2290	18.8	0.00	1.05
2048	16384	2208	36.2	0.00	2197	36	0.00	0.55
4096	32768	1561	51.2	0.00	1478	48.5	0.00	5.27
8192	65536	786	51.6	0.00	759	49.8	0.00	3.49
16384	131072	394	51.7	0.00	384	50.4	0.00	2.51
32768	262144	197	51.9	0.00	193	50.8	0.00	2.12
63000	504000	103	52	0.00	101	51	0.00	1.92

2. Latency Test Results (RELIABLE)

Tables 20 to 24 shows the Latency Test results—comparison with and without security for RELIABLE communications in the Ideal configuration for the five point-to-point links.

Table 20. Latency Test Results—Comparison With and Without Security for H1 to H2 Link for Ideal Configuration (RELIABLE)

One-Way Latency Test Results for H1 (Pub) to H2 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	280.18	280.45	280.33	280.23	280.92	280.40	0.02
64	280.19	280.43	280.33	280.22	280.58	280.39	0.02
128	280.20	280.74	280.34	280.22	280.52	280.38	0.02
256	280.23	280.49	280.34	280.27	280.51	280.40	0.02
512	280.18	280.46	280.34	280.24	280.50	280.38	0.02
1024	280.17	280.51	280.33	280.27	280.47	280.39	0.02
2048	280.21	280.90	280.38	280.28	280.54	280.43	0.02
4096	280.29	281.26	280.42	280.34	280.57	280.47	0.02
8192	280.53	280.78	280.66	280.61	280.83	280.74	0.03
16384	280.98	281.26	281.15	281.14	281.40	281.28	0.05
32768	281.88	282.24	282.04	282.03	282.45	282.24	0.07
63000	283.41	283.81	283.65	283.62	284.88	284.02	0.13

Table 21. Latency Test Results—Comparison With and Without Security for H1 to H5 Link for Ideal Configuration (RELIABLE)

One-Way Latency Test Results for H1 (Pub) to H5 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	285.16	285.52	285.39	285.27	285.56	285.45	0.02
64	285.17	285.48	285.39	285.23	285.58	285.44	0.02
128	285.20	285.54	285.39	285.24	285.63	285.44	0.02
256	285.21	285.51	285.4	285.26	288.87	285.46	0.02
512	285.17	285.50	285.4	285.25	285.53	285.43	0.01
1024	285.21	285.51	285.39	285.21	285.57	285.43	0.01
2048	285.20	286.27	285.44	285.22	285.62	285.47	0.01
4096	285.43	285.68	285.6	285.52	285.80	285.67	0.02
8192	286.12	286.46	286.29	286.12	286.52	286.38	0.03
16384	287.47	287.82	287.65	287.55	287.93	287.78	0.05
32768	289.94	290.29	290.16	290.02	290.54	290.35	0.07
63000	294.47	294.93	294.67	294.65	295.28	295.08	0.14

Table 22. Latency Test Results—Comparison With and Without Security for H1 to H3 Link for Ideal Configuration (RELIABLE)

One-Way Latency Test Results for H1 (Pub) to H3 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	295.22	295.60	295.42	295.27	295.59	295.47	0.02
64	295.22	295.56	295.42	295.24	295.73	295.46	0.01
128	295.23	295.58	295.41	295.33	295.61	295.48	0.02
256	295.21	296.16	295.43	295.26	295.61	295.47	0.01
512	295.16	295.55	295.41	295.23	295.60	295.48	0.02
1024	295.21	295.66	295.42	295.22	295.61	295.50	0.03
2048	295.24	296.38	295.46	295.19	295.63	295.51	0.02
4096	295.43	295.75	295.62	295.51	295.80	295.70	0.03
8192	296.16	296.55	296.32	296.21	297.03	296.42	0.03
16384	297.46	298.07	297.7	297.62	299.44	297.83	0.05
32768	300.02	300.77	300.19	300.13	300.59	300.38	0.06
63000	304.44	304.95	304.71	304.68	306.31	305.10	0.13

Table 23. Latency Test Results—Comparison With and Without Security for H2 to H5 Link for Ideal Configuration (RELIABLE)

One-Way Latency Test Results for H2 (Pub) to H5 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	280.18	280.43	280.34	280.18	280.52	280.40	0.02
64	280.19	280.51	280.34	280.23	280.48	280.39	0.02
128	280.19	280.49	280.35	280.17	280.53	280.39	0.02
256	280.21	280.46	280.35	280.21	280.54	280.38	0.01
512	280.18	280.51	280.35	280.23	280.54	280.40	0.02
1024	280.18	280.48	280.35	280.15	280.50	280.39	0.02
2048	280.23	280.77	280.39	280.2	280.60	280.44	0.02
4096	280.43	280.64	280.56	280.39	280.74	280.59	0.01
8192	281.10	281.33	281.25	281.16	281.44	281.33	0.03
16384	282.47	282.72	282.61	282.52	282.86	282.74	0.05
32768	284.99	285.24	285.12	285.02	285.51	285.32	0.07
63000	289.50	289.89	289.67	289.45	290.26	289.96	0.10

Table 24. Latency Test Results—Comparison With and Without Security for H4 to H5 Link for Ideal Configuration (RELIABLE)

One-Way Latency Test Results for H4 (Pub) to H5 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	10.03	11.18	10.24	10.06	10.54	10.28	0.42
64	10.03	11.64	10.24	10.06	10.43	10.28	0.40
128	10.04	10.53	10.24	10.05	10.97	10.28	0.39
256	10.03	10.67	10.24	10.04	10.59	10.28	0.47
512	10.03	10.45	10.24	10.06	10.49	10.28	0.45
1024	10.05	10.86	10.24	10.04	11.52	10.29	0.46
2048	10.06	10.50	10.26	10.06	11.88	10.31	0.49
4096	10.27	10.75	10.49	10.28	10.67	10.55	0.56
8192	10.94	11.44	11.17	10.97	13.16	11.24	0.62
16384	12.29	13.11	12.53	12.33	12.85	12.64	0.85
32768	14.80	15.80	15.04	14.84	15.64	15.22	1.17
63000	19.31	20.45	19.60	19.37	20.20	19.92	1.64

3. Throughput Test Results (BEST EFFORT at PubRate 100 Hz)

Tables 25 to 29 shows the Throughput Test results—comparison with and without security for BEST EFFORT communications in the Ideal configuration for the five point-to-point links.

Table 25. Throughput Test Results—Comparison With and Without Security for H1 to H2 Link for Ideal Configuration (BEST EFFORT)

Throughput Test Results for H1 (Pub) to H2 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	
32	256	100	0.026	0.00	100	0.026	0.00	0.00
64	512	100	0.1	0.00	99	0.1	0.00	0.00
128	1024	100	0.1	0.00	100	0.1	0.00	0.00

Throughput Test Results for H1 (Pub) to H2 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	
256	2048	100	0.2	0.00	99	0.2	0.00	0.00
512	4096	100	0.4	0.00	100	0.4	0.00	0.00
1024	8192	100	0.8	0.00	99	0.8	0.00	0.00
2048	16384	99	1.6	0.00	99	1.6	0.00	0.00
4096	32768	100	3.3	0.00	99	3.3	0.00	0.00
8192	65536	100	6.6	0.00	99	6.5	0.00	1.52
16384	131072	100	13.1	0.00	99	13.1	0.00	0.00
32768	262144	100	26.3	0.00	99	26.2	0.00	0.38
63000	504000	100	50.5	0.00	99	50.2	0.00	0.59

Table 26. Throughput Test Results—Comparison With and Without Security for H1 to H5 Link for Ideal Configuration (BEST EFFORT)

Throughput Test Results for H1 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	
32	256	100	0.026	0.00	100	0.026	0.00	0.00
64	512	100	0.1	0.00	99	0.1	0.00	0.00
128	1024	100	0.1	0.00	99	0.1	0.00	0.00
256	2048	100	0.2	0.00	99	0.2	0.00	0.00
512	4096	99	0.4	0.00	99	0.4	0.00	0.00
1024	8192	100	0.8	0.00	100	0.8	0.00	0.00
2048	16384	100	1.6	0.00	100	1.6	0.00	0.00
4096	32768	100	3.3	0.00	100	3.3	0.00	0.00
8192	65536	100	6.6	0.00	99	6.6	0.00	0.00
16384	131072	100	13.1	0.00	99	13.1	0.00	0.00
32768	262144	100	26.3	0.00	99	26.1	0.00	0.76
63000	504000	100	50.4	0.00	99	50.3	0.00	0.20

Table 27. Throughput Test Results—Comparison With and Without Security for H1 to H3 Link for Ideal Configuration (BEST EFFORT)

Throughput Test Results for H1 (Pub) to H3 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	
32	256	100	0.026	0.00	100	0.026	0.00	0.00
64	512	100	0.1	0.00	99	0.1	0.00	0.00
128	1024	100	0.1	0.00	100	0.1	0.00	0.00
256	2048	100	0.2	0.00	100	0.2	0.00	0.00
512	4096	100	0.4	0.00	99	0.4	0.00	0.00
1024	8192	100	0.8	0.00	100	0.8	0.00	0.00
2048	16384	100	1.6	0.00	99	1.6	0.00	0.00
4096	32768	100	3.3	0.00	99	3.3	0.00	0.00
8192	65536	100	6.6	0.00	99	6.5	0.00	1.52
16384	131072	100	13.1	0.00	99	13.1	0.00	0.00
32768	262144	100	26.2	0.00	99	26.2	0.00	0.00
63000	504000	100	50.6	0.00	99	50.4	0.00	0.40

Table 28. Throughput Test Results—Comparison With and Without Security for H2 to H5 Link for Ideal Configuration (BEST EFFORT)

Throughput Test Results for H2 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	
32	256	100	0.026	0.00	99	0.025	0.00	1.00
64	512	100	0.1	0.00	99	0.1	0.00	0.00
128	1024	100	0.1	0.00	99	0.1	0.00	0.00
256	2048	100	0.2	0.00	99	0.2	0.00	0.00
512	4096	100	0.4	0.00	99	0.4	0.00	0.00
1024	8192	100	0.8	0.00	99	0.8	0.00	0.00
2048	16384	100	1.6	0.00	100	1.6	0.00	0.00
4096	32768	100	3.3	0.00	99	3.3	0.00	0.00
8192	65536	100	6.6	0.00	99	6.5	0.00	1.52
16384	131072	100	13.1	0.00	99	13.1	0.00	0.00

Throughput Test Results for H2 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	
32768	262144	100	26.3	0.00	99	26.2	0.00	0.38
63000	504000	100	50.5	0.00	99	50.4	0.00	0.20

Table 29. Throughput Test Results—Comparison With and Without Security for H4 to H5 Link for Ideal Configuration (BEST EFFORT)

Throughput Test Results for H4 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	
32	256	100	0.026	0.00	100	0.026	0.00	0.00
64	512	100	0.1	0.00	99	0.1	0.00	0.00
128	1024	100	0.1	0.00	99	0.1	0.00	0.00
256	2048	100	0.2	0.00	99	0.2	0.00	0.00
512	4096	100	0.4	0.00	99	0.4	0.00	0.00
1024	8192	100	0.8	0.00	99	0.8	0.00	0.00
2048	16384	100	1.6	0.00	99	1.6	0.00	0.00
4096	32768	100	3.3	0.00	99	3.3	0.00	0.00
8192	65536	100	6.6	0.00	99	6.5	0.00	1.52
16384	131072	100	13.1	0.00	99	13.1	0.00	0.00
32768	262144	100	26.3	0.00	99	26.2	0.00	0.38
63000	504000	99	50.4	0.00	99	50.4	0.00	0.00

4. Latency Test Results (BEST EFFORT at PubRate 100 Hz)

Tables 30 to 34 shows the Latency Test results—comparison with and without security for BEST EFFORT communications in the Ideal configuration for the five point-to-point links.

Table 30. Latency Test Results—Comparison With and Without Security for H1 to H2 Link for Ideal Configuration (BEST EFFORT)

One-Way Latency Test Results for H1 (Pub) to H2 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	280.23	280.40	280.32	280.23	280.44	280.38	0.02
64	280.20	280.40	280.32	280.24	280.45	280.39	0.03
128	280.23	280.42	280.33	280.27	280.45	280.39	0.02
256	280.23	280.41	280.33	280.26	280.44	280.38	0.02
512	280.21	280.52	280.32	280.24	280.45	280.37	0.02
1024	280.21	280.40	280.32	280.24	280.47	280.37	0.02
2048	280.25	280.85	280.35	280.26	280.50	280.42	0.02
4096	280.31	280.46	280.39	280.31	280.53	280.46	0.02
8192	280.53	280.70	280.63	280.58	280.84	280.72	0.03
16384	281.00	281.20	281.12	281.05	281.28	281.20	0.03
32768	281.90	283.02	282.02	281.95	282.41	282.18	0.06
63000	283.44	285.37	283.63	283.52	284.23	283.89	0.09

Table 31. Latency Test Results—Comparison With and Without Security for H1 to H5 Link for Ideal Configuration (BEST EFFORT)

One-Way Latency Test Results for H1 (Pub) to H5 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	285.31	285.53	285.4	285.26	286.09	285.45	0.02
64	285.28	285.48	285.4	285.32	285.54	285.45	0.02
128	285.26	285.52	285.39	285.32	285.50	285.43	0.01
256	285.27	285.54	285.4	285.29	285.51	285.44	0.01
512	285.25	285.51	285.4	285.31	285.51	285.44	0.02
1024	285.26	285.49	285.4	285.3	285.51	285.44	0.01
2048	285.22	286.42	285.43	285.41	285.54	285.48	0.02
4096	285.44	285.70	285.58	285.47	285.69	285.63	0.02
8192	286.14	286.44	286.29	286.2	286.45	286.37	0.03
16384	287.49	287.81	287.65	287.58	287.83	287.73	0.03
32768	289.98	291.33	290.14	290.02	290.40	290.28	0.05
63000	294.47	294.86	294.67	294.63	295.21	294.93	0.09

Table 32. Latency Test Results—Comparison With and Without Security for H1 to H3 Link for Ideal Configuration (BEST EFFORT)

One-Way Latency Test Results for H1 (Pub) to H3 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	295.30	295.65	295.43	295.3	295.58	295.46	0.01
64	295.30	296.12	295.44	295.38	295.59	295.49	0.02
128	295.30	297.01	295.45	295.36	295.65	295.49	0.01
256	295.31	295.53	295.44	295.33	295.62	295.49	0.02
512	295.31	295.54	295.44	295.33	295.63	295.49	0.02
1024	295.28	295.52	295.44	295.33	295.64	295.49	0.02
2048	295.28	296.33	295.46	295.36	295.58	295.51	0.02
4096	295.51	295.75	295.63	295.53	295.89	295.69	0.02
8192	296.18	297.55	296.34	296.24	296.55	296.41	0.02
16384	297.53	299.32	297.7	297.54	298.37	297.79	0.03
32768	300.03	300.32	300.17	300.05	300.57	300.33	0.05
63000	304.52	304.91	304.7	304.62	305.27	304.95	0.08

Table 33. Latency Test Results—Comparison With and Without Security for H2 to H5 Link for Ideal Configuration (BEST EFFORT)

One-Way Latency Test Results for H2 (Pub) to H5 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	280.22	280.56	280.33	280.23	280.49	280.39	0.02
64	280.20	280.39	280.32	280.21	280.44	280.36	0.02
128	280.23	280.49	280.32	280.25	280.52	280.38	0.02
256	280.21	280.43	280.32	280.26	280.42	280.36	0.02
512	280.18	280.38	280.33	280.25	280.45	280.37	0.02
1024	280.17	280.39	280.32	280.24	280.50	280.37	0.02
2048	280.22	280.99	280.36	280.22	280.85	280.40	0.01
4096	280.36	280.59	280.51	280.42	281.04	280.59	0.03
8192	281.09	281.40	281.23	281.18	281.39	281.31	0.03
16384	282.47	282.64	282.58	282.52	284.31	282.71	0.05
32768	284.94	285.19	285.08	284.95	285.40	285.24	0.06
63000	289.44	289.77	289.62	289.56	290.22	289.88	0.09

Table 34. Latency Test Results—Comparison With and Without Security for H4 to H5 Link for Ideal Configuration (BEST EFFORT)

One-Way Latency Test Results for H4 (Pub) to H5 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	10.04	10.28	10.14	10.06	10.41	10.16	0.23
64	10.05	10.29	10.16	10.05	10.31	10.19	0.32
128	10.05	10.49	10.21	10.05	10.35	10.25	0.43
256	10.04	10.61	10.22	10.05	10.47	10.28	0.55
512	10.05	10.80	10.21	10.06	10.45	10.27	0.63
1024	10.05	10.51	10.23	10.06	12.16	10.28	0.48
2048	10.05	10.82	10.25	10.06	10.45	10.30	0.55
4096	10.26	11.87	10.47	10.27	11.94	10.53	0.61
8192	10.92	11.34	11.15	10.98	13.02	11.22	0.65
16384	12.31	13.96	12.52	12.33	12.76	12.63	0.92
32768	14.78	15.48	15.01	14.80	15.43	15.20	1.22
63000	19.31	20.14	19.57	19.37	21.63	19.90	1.69

B. JITTER CONFIGURATION

1. Throughput Test Results (RELIABLE)

Tables 35 to 39 shows the Throughput Test results—comparison with and without security for RELIABLE communications in the Jitter configuration for the five point-to-point links.

Table 35. Throughput Test Results—Comparison With and Without Security for H1 to H2 Link for Jitter Configuration (RELIABLE)

Throughput Test Results for H1 (Pub) to H2 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	
32	256	88	0.023	0.00	88	0.023	0.00	0.00
64	512	88	0.045	0.00	88	0.045	0.00	0.00
128	1024	88	0.1	0.00	88	0.1	0.00	0.00
256	2048	88	0.2	0.00	88	0.2	0.00	0.00
512	4096	88	0.4	0.00	88	0.4	0.00	0.00
1024	8192	88	0.7	0.00	88	0.7	0.00	0.00
2048	16384	66	1.1	0.00	68	1.1	0.00	0.00
4096	32768	50	1.6	0.00	49	1.6	0.00	0.00
8192	65536	24	1.6	0.00	23	1.6	0.00	0.00
16384	131072	18	2.4	0.00	17	2.2	0.00	8.33
32768	262144	11	3	0.00	12	3.2	0.00	-6.67
63000	504000	7	3.6	0.00	7	3.9	0.00	-8.33

Table 36. Throughput Test Results—Comparison With and Without Security for H1 to H5 Link for Jitter Configuration (RELIABLE)

Throughput Test Results for H1 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	Avg # of DSsps	Avg Through-put (Mbps)	Loss (%)	
32	256	87	0.022	0.00	87	0.022	0.00	0.00
64	512	87	0.045	0.00	87	0.045	0.00	0.00
128	1024	87	0.1	0.00	87	0.1	0.00	0.00
256	2048	87	0.2	0.00	87	0.2	0.00	0.00
512	4096	87	0.4	0.00	87	0.4	0.00	0.00
1024	8192	87	0.7	0.00	87	0.7	0.00	0.00
2048	16384	58	1	0.00	62	1	0.00	0.00
4096	32768	49	1.6	0.00	48	1.6	0.00	0.00
8192	65536	42	2.8	0.00	43	2.8	0.00	0.00
16384	131072	18	2.5	0.00	19	2.6	0.00	-4.00

Throughput Test Results for H1 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
32768	262144	10	2.9	0.00	11	3.1	0.00	-6.90
63000	504000	7	3.6	0.00	7	3.9	0.00	-8.33

Table 37. Throughput Test Results—Comparison With and Without Security for H1 to H3 Link for Jitter Configuration (RELIABLE)

Throughput Test Results for H1 (Pub) to H3 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
32	256	84	0.022	0.00	84	0.022	0.00	0.00
64	512	84	0.043	0.00	84	0.043	0.00	0.00
128	1024	84	0.1	0.00	84	0.1	0.00	0.00
256	2048	84	0.2	0.00	84	0.2	0.00	0.00
512	4096	84	0.3	0.00	84	0.3	0.00	0.00
1024	8192	84	0.7	0.00	84	0.7	0.00	0.00
2048	16384	56	0.9	0.00	54	0.9	0.00	0.00
4096	32768	47	1.6	0.00	48	1.6	0.00	0.00
8192	65536	41	2.7	0.00	39	2.6	0.00	3.70
16384	131072	17	2.3	0.00	18	2.4	0.00	-4.35
32768	262144	10	2.8	0.00	11	3	0.00	-7.14
63000	504000	6	3.4	0.00	7	3.5	0.00	-2.94

Table 38. Throughput Test Results—Comparison With and Without Security for H2 to H5 Link for Jitter Configuration (RELIABLE)

Throughput Test Results for H2 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
32	256	88	0.023	0.00	88	0.023	0.00	0.00
64	512	88	0.045	0.00	88	0.045	0.00	0.00
128	1024	88	0.1	0.00	88	0.1	0.00	0.00
256	2048	88	0.2	0.00	88	0.2	0.00	0.00
512	4096	88	0.4	0.00	88	0.4	0.00	0.00
1024	8192	88	0.7	0.00	88	0.7	0.00	0.00
2048	16384	65	1.1	0.00	60	1	0.00	9.09
4096	32768	50	1.6	0.00	49	1.6	0.00	0.00
8192	65536	43	2.9	0.00	41	2.7	0.00	6.90
16384	131072	20	2.7	0.00	18	2.4	0.00	11.11
32768	262144	9	2.4	0.00	9	2.5	0.00	-4.17
63000	504000	6	3.2	0.00	6	3.2	0.00	0.00

Table 39. Throughput Test Results—Comparison With and Without Security for H4 to H5 Link for Jitter Configuration (RELIABLE)

Throughput Test Results for H4 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
32	256	2289	0.6	0.00	2274	0.6	0.00	0.00
64	512	2288	1.2	0.00	2274	1.2	0.00	0.00
128	1024	2287	2.3	0.00	2273	2.3	0.00	0.00
256	2048	2289	4.7	0.00	2273	4.7	0.00	0.00
512	4096	2283	9.4	0.00	2259	9.3	0.00	1.06
1024	8192	2163	17.7	0.00	2152	17.6	0.00	0.56
2048	16384	1980	32.5	0.00	1964	32.2	0.00	0.92
4096	32768	1147	37.6	0.00	1099	36	0.00	4.26
8192	65536	553	36.3	0.00	540	35.4	0.00	2.48

Throughput Test Results for H4 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
16384	131072	49	6.4	0.00	258	33.9	0.00	-429.69
32768	262144	66	17.4	0.00	124	32.7	0.00	-87.93
63000	504000	50	25.4	0.00	48	24.4	0.00	3.94

2. Latency Test Results (RELIABLE)

Tables 40 to 44 shows the Latency Test results—comparison with and without security for RELIABLE communications in the Jitter configuration for the five point-to-point links.

Table 40. Latency Test Results—Comparison With and Without Security for H1 to H2 Link for Jitter Configuration (RELIABLE)

One-Way Latency Test Results for H1 (Pub) to H2 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	273.08	288.17	280.58	271.35	288.22	280.50	-0.03
64	271.73	288.13	280.05	272.97	287.86	280.58	0.19
128	272.96	287.99	280.31	273.28	286.73	280.45	0.05
256	272.90	288.56	280.69	274.08	288.39	280.57	-0.04
512	272.12	287.10	279.93	272.43	287.92	280.53	0.21
1024	273.75	287.28	279.76	273.42	288.06	280.66	0.32
2048	275.18	288.33	282.48	275.59	288.69	282.75	0.10
4096	278.12	288.62	284.01	278.85	288.80	283.78	-0.08
8192	280.74	288.89	285.52	281.07	290.04	285.47	-0.02
16384	282.57	289.62	286.85	283.17	290.12	286.87	0.01
32768	285.09	290.10	288.07	285.05	290.64	288.13	0.02
63000	286.03	290.73	288.7	287.02	290.80	289.08	0.13

Table 41. Latency Test Results—Comparison With and Without Security for H1 to H5 Link for Jitter Configuration (RELIABLE)

One-Way Latency Test Results for H1 (Pub) to H5 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	277.48	292.40	285.41	279.53	291.91	285.29	-0.04
64	277.87	293.62	284.97	278.22	292.04	285.15	0.06
128	275.94	292.92	285.29	278.13	292.33	285.56	0.09
256	277.12	292.35	285.46	276.67	291.91	285.25	-0.07
512	276.89	293.85	285.15	279.04	291.30	285.15	0.00
1024	277.88	292.23	284.83	276.9	293.56	285.43	0.21
2048	282.68	294.34	288.13	282.92	293.48	288.07	-0.02
4096	283.16	292.84	288.81	283.18	294.00	288.90	0.03
8192	286.00	295.54	290.58	286.16	295.37	290.69	0.04
16384	288.79	295.90	292.17	289.29	294.98	292.41	0.08
32768	291.38	297.02	293.99	291.4	297.53	294.27	0.09
63000	294.19	301.53	297.17	294.39	302.37	297.55	0.13

Table 42. Latency Test Results—Comparison With and Without Security for H1 to H3 Link for Jitter Configuration (RELIABLE)

One-Way Latency Test Results for H1 (Pub) to H3 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	287.78	302.16	295.33	287.6	303.71	295.46	0.05
64	286.75	302.10	295.17	288.11	302.07	295.55	0.13
128	288.80	303.04	295.47	287.16	303.56	295.77	0.10
256	288.55	302.51	295.52	287.97	301.59	295.29	-0.08
512	286.87	302.80	295.57	287.43	301.86	295.28	-0.10
1024	288.59	302.59	295.29	288	302.08	295.22	-0.02
2048	290.82	304.05	297.73	292.05	304.12	298.09	0.12
4096	292.17	304.11	298.87	293.16	304.65	298.86	-0.01
8192	295.59	304.80	300.8	295.92	304.62	300.80	0.00
16384	298.86	306.00	302.21	298.4	306.23	302.34	0.04
32768	301.62	307.44	304.32	301.27	306.95	304.33	0.00
63000	303.88	310.80	307.25	304.61	313.01	307.79	0.17

Table 43. Latency Test Results—Comparison With and Without Security for H2 to H5 Link for Jitter Configuration (RELIABLE)

One-Way Latency Test Results for H2 (Pub) to H5 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	273.45	286.71	280.58	272.56	287.61	280.63	0.02
64	272.65	286.49	280	271.96	287.94	280.61	0.21
128	272.30	288.68	280.24	272.58	286.50	280.51	0.10
256	273.32	288.75	280.44	272.26	288.10	280.61	0.06
512	272.70	289.15	280.37	273.75	287.88	280.45	0.03
1024	271.46	288.50	280.11	273.73	288.51	280.62	0.18
2048	275.15	288.41	282.75	275.27	289.32	282.91	0.06
4096	277.02	289.15	283.86	279.81	288.79	284.02	0.06
8192	280.83	289.28	285.4	281.5	289.19	285.98	0.20
16384	283.96	290.24	287.13	284.04	290.82	287.12	-0.01
32768	286.10	292.18	288.83	285.91	291.84	289.07	0.08
63000	288.79	297.32	291.89	289.21	295.54	292.15	0.09

Table 44. Latency Test Results—Comparison With and Without Security for H4 to H5 Link for Jitter Configuration (RELIABLE)

One-Way Latency Test Results for H4 (Pub) to H5 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	9.17	11.23	10.23	9.24	11.43	10.28	0.40
64	9.14	11.23	10.24	9.14	11.41	10.29	0.54
128	9.14	11.22	10.23	9.19	12.64	10.29	0.55
256	9.14	11.26	10.24	9.20	11.29	10.29	0.51
512	9.24	11.25	10.24	9.20	11.30	10.29	0.55
1024	9.18	11.24	10.25	9.19	11.32	10.30	0.49
2048	9.42	11.28	10.58	9.43	11.33	10.64	0.51
4096	9.73	11.36	10.75	9.68	11.36	10.82	0.65
8192	10.24	11.52	11.01	10.32	11.65	11.09	0.73
16384	11.21	13.44	11.67	11.27	12.96	11.81	1.21
32768	13.66	16.18	14.04	13.76	16.32	14.27	1.61
63000	18.26	22.69	18.69	18.39	21.27	19.02	1.74

3. Throughput Test Results (BEST EFFORT at PubRate 100 Hz)

Tables 45 to 49 shows the Throughput Test results—comparison with and without security for BEST EFFORT communications in the Jitter configuration for the five point-to-point links.

Table 45. Throughput Test Results—Comparison With and Without Security for H1 to H2 Link for Jitter Configuration (BEST EFFORT)

Throughput Test Results for H1 (Pub) to H2 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
32	256	96	0.025	3.97	95	0.024	4.20	1.04
64	512	95	0.049	4.67	95	0.049	4.43	0.00
128	1024	95	0.1	4.25	95	0.1	4.43	0.00
256	2048	95	0.2	4.51	95	0.2	4.76	0.00
512	4096	95	0.4	4.55	95	0.4	4.13	0.00
1024	8192	95	0.8	4.46	95	0.8	4.39	0.00
2048	16384	98	1.6	1.48	98	1.6	1.60	0.00
4096	32768	98	3.2	0.72	98	3.2	0.77	0.00
8192	65536	99	6.5	0.10	99	6.5	0.04	0.00
16384	131072	99	13.1	0.00	99	13.1	0.00	0.00
32768	262144	99	26.2	0.00	99	26.2	0.00	0.00
63000	504000	99	50.2	0.00	99	50.3	0.00	-0.20

Table 46. Throughput Test Results—Comparison With and Without Security for H1 to H5 Link for Jitter Configuration (BEST EFFORT)

Throughput Test Results for H1 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
32	256	95	0.024	4.43	95	0.024	4.64	0.00
64	512	95	0.049	4.48	95	0.049	4.65	0.00
128	1024	95	0.1	4.39	94	0.1	4.84	0.00

Throughput Test Results for H1 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
256	2048	95	0.2	4.44	95	0.2	4.42	0.00
512	4096	95	0.4	4.62	95	0.4	4.32	0.00
1024	8192	95	0.8	4.64	95	0.8	4.74	0.00
2048	16384	98	1.6	1.83	98	1.6	1.69	0.00
4096	32768	99	3.3	0.67	99	3.2	0.77	3.03
8192	65536	99	6.5	0.11	99	6.5	0.02	0.00
16384	131072	99	13.1	0.00	99	13.1	0.01	0.00
32768	262144	99	26.2	0.00	99	26.2	0.00	0.00
63000	504000	99	50.3	0.00	99	50.3	0.00	0.00

Table 47. Throughput Test Results—Comparison With and Without Security for H1 to H3 Link for Jitter Configuration (BEST EFFORT)

Throughput Test Results for H1 (Pub) to H3 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
32	256	95	0.024	4.62	95	0.024	4.91	0.00
64	512	94	0.048	4.73	95	0.049	4.61	-1.06
128	1024	95	0.1	4.58	95	0.1	4.59	0.00
256	2048	94	0.2	4.99	95	0.2	4.76	0.00
512	4096	95	0.4	4.58	95	0.4	4.73	0.00
1024	8192	95	0.8	4.47	95	0.8	4.62	0.00
2048	16384	97	1.6	1.97	97	1.6	1.99	0.00
4096	32768	99	3.2	0.87	99	3.2	0.94	0.00
8192	65536	99	6.5	0.08	99	6.5	0.10	0.00
16384	131072	99	13.1	0.03	99	13.1	0.01	0.00
32768	262144	99	26.2	0.00	99	26.2	0.00	0.00
63000	504000	99	50.3	0.00	99	50.3	0.00	0.00

Table 48. Throughput Test Results—Comparison With and Without Security for H2 to H5 Link for Jitter Configuration (BEST EFFORT)

Throughput Test Results for H2 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
32	256	95	0.024	4.90	95	0.024	4.38	0.00
64	512	95	0.049	4.38	95	0.049	4.32	0.00
128	1024	95	0.1	4.33	95	0.1	4.52	0.00
256	2048	95	0.2	4.49	95	0.2	4.11	0.00
512	4096	95	0.4	4.51	95	0.4	4.55	0.00
1024	8192	95	0.8	4.28	95	0.8	4.55	0.00
2048	16384	98	1.6	1.73	98	1.6	1.66	0.00
4096	32768	99	3.3	0.61	99	3.2	0.66	3.03
8192	65536	99	6.5	0.10	99	6.5	0.11	0.00
16384	131072	99	13.1	0.00	99	13.1	0.00	0.00
32768	262144	99	26.2	0.00	99	26.2	0.00	0.00
63000	504000	99	50.3	0.00	99	50.3	0.00	0.00

Table 49. Throughput Test Results—Comparison With and Without Security for H4 to H5 Link for Jitter Configuration (BEST EFFORT)

Throughput Test Results for H4 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)	
32	256	100	0.026	0.00	100	0.026	0.00	0.00
64	512	99	0.1	0.00	99	0.1	0.00	0.00
128	1024	99	0.1	0.00	99	0.1	0.00	0.00
256	2048	99	0.2	0.00	99	0.2	0.00	0.00
512	4096	99	0.4	0.00	99	0.4	0.00	0.00
1024	8192	99	0.8	0.00	99	0.8	0.00	0.00
2048	16384	99	1.6	0.00	99	1.6	0.00	0.00
4096	32768	99	3.3	0.00	99	3.3	0.00	0.00
8192	65536	99	6.5	0.00	99	6.5	0.00	0.00
16384	131072	99	13.1	0.00	99	13.1	0.00	0.00

Throughput Test Results for H4 (Pub) to H5 (Sub) Link								
Data Sample Size (Bytes)	Data Sample Size (bits)	No Security Implemented			Security Implemented			OH (%)
		Avg # of DSps	Avg Throughput (Mbps)	Loss (%)	Avg # of DSps	Avg Throughput (Mbps)	Loss (%)	
32768	262144	99	26.2	0.00	100	26.2	0.00	0.00
63000	504000	99	50.4	0.00	99	50.3	0.00	0.20

4. Latency Test Results (BEST EFFORT at PubRate 100 Hz)

Tables 50 to 54 shows the Latency Test results—comparison with and without security for BEST EFFORT communications in the Jitter configuration for the five point-to-point links.

Table 50. Latency Test Results—Comparison With and Without Security for H1 to H2 Link for Jitter Configuration (BEST EFFORT)

One-Way Latency Test Results for H1 (Pub) to H2 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	271.63	287.95	280.33	272.74	288.34	280.54	0.07
64	272.57	286.95	279.94	272.45	287.01	280.03	0.03
128	273.13	287.46	280.53	272.99	287.79	279.91	-0.22
256	271.92	287.17	280.42	273.96	287.94	280.52	0.03
512	273.42	286.76	280.4	273.41	287.31	280.48	0.03
1024	273.37	287.66	280.13	273.22	286.45	280.43	0.11
2048	276.81	289.05	282.82	277.49	288.59	283.00	0.06
4096	278.11	289.23	284.08	276.91	288.84	283.90	-0.06
8192	280.16	289.80	285.45	281.35	289.50	285.87	0.15
16384	282.77	289.92	286.78	283.09	289.87	287.15	0.13
32768	284.50	290.27	287.88	285.38	290.34	287.96	0.03
63000	286.72	290.64	288.61	286.41	291.05	288.92	0.11

Table 51. Latency Test Results—Comparison With and Without Security for H1 to H5 Link for Jitter Configuration (BEST EFFORT)

One-Way Latency Test Results for H1 (Pub) to H5 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	278.09	292.40	285.52	278.06	292.26	285.61	0.03
64	276.13	292.97	285.35	279.17	293.69	285.42	0.02
128	278.27	291.70	284.91	276.39	294.64	285.25	0.12
256	279.43	291.67	284.93	277.79	293.02	285.74	0.28
512	278.68	292.62	285.55	277.1	293.51	285.11	-0.15
1024	278.70	292.62	285.11	277.3	292.50	285.11	0.00
2048	282.70	293.41	287.76	283.08	294.00	288.02	0.09
4096	283.18	293.42	288.95	284.09	294.93	289.14	0.07
8192	286.34	294.36	290.63	286.06	294.80	290.79	0.06
16384	288.64	295.84	292.16	287.96	294.96	292.37	0.07
32768	291.18	296.34	293.92	291.29	296.36	294.10	0.06
63000	293.84	299.21	296.68	293.99	299.15	296.83	0.05

Table 52. Latency Test Results—Comparison With and Without Security for H1 to H3 Link for Jitter Configuration (BEST EFFORT)

One-Way Latency Test Results for H1 (Pub) to H3 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	289.51	302.41	295.5	287.04	302.73	295.44	-0.02
64	287.23	303.66	295.49	289.39	301.84	295.62	0.05
128	289.02	302.24	295.52	288.81	302.57	295.40	-0.04
256	288.28	303.47	295.62	288.58	302.17	295.61	0.00
512	288.82	303.24	295.62	288.74	302.83	295.81	0.07
1024	288.82	303.52	296	288.27	302.54	295.71	-0.10
2048	291.37	303.59	297.83	290.78	302.82	297.62	-0.07
4096	293.43	304.70	299.08	293.93	304.02	299.27	0.06
8192	295.15	304.96	300.42	297.04	305.28	300.83	0.14
16384	298.77	305.40	302.35	298.13	305.48	302.41	0.02
32768	300.98	306.72	304.04	301.79	307.02	304.46	0.14
63000	303.72	309.78	306.72	304.58	310.12	307.15	0.14

Table 53. Latency Test Results—Comparison With and Without Security for H2 to H5 Link for Jitter Configuration (BEST EFFORT)

One-Way Latency Test Results for H2 (Pub) to H5 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	272.27	287.12	279.87	272.93	287.45	280.82	0.34
64	273.69	288.09	280.18	272.19	287.87	280.22	0.02
128	272.51	287.46	280.38	272.51	288.73	280.21	-0.06
256	271.70	286.48	280.26	273.67	287.95	280.30	0.01
512	273.37	288.09	280.48	274.06	288.19	280.56	0.03
1024	273.58	289.11	280.35	272.5	286.67	280.06	-0.11
2048	276.14	288.41	282.89	275.45	288.24	282.74	-0.05
4096	277.51	289.12	283.93	278.19	288.34	283.79	-0.05
8192	281.57	289.21	285.81	280.14	288.90	285.57	-0.08
16384	283.02	290.50	286.97	283.21	289.75	286.96	0.00
32768	285.36	291.10	288.8	286.42	291.48	288.96	0.06
63000	289.20	294.11	291.36	289.46	294.07	291.73	0.13

Table 54. Latency Test Results—Comparison With and Without Security for H4 to H5 Link for Jitter Configuration (BEST EFFORT)

One-Way Latency Test Results for H4 (Pub) to H5 (Sub) Link							
Data Sample Size (Bytes)	No Security Implemented			Security Implemented			OH (%)
	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)	
32	9.16	11.18	10.13	9.21	11.35	10.15	0.18
64	9.15	11.38	10.16	9.14	11.18	10.19	0.28
128	9.18	13.07	10.21	9.13	11.37	10.23	0.24
256	9.19	11.24	10.22	9.13	11.25	10.26	0.41
512	9.16	11.22	10.21	9.25	11.25	10.27	0.52
1024	9.17	11.24	10.22	9.19	11.30	10.28	0.50
2048	9.41	11.25	10.55	9.40	11.31	10.62	0.66
4096	9.54	11.25	10.72	9.54	11.37	10.80	0.74
8192	10.17	12.63	10.97	10.28	11.59	11.05	0.73
16384	11.18	12.16	11.59	11.22	13.72	11.72	1.15
32768	13.63	15.22	13.96	13.72	16.47	14.16	1.47
63000	18.23	20.86	18.57	18.32	19.96	18.90	1.79

C. MULTI-FLOW CONFIGURATION 1

1. Throughput Test Results

Table 55 shows the Throughput Test results for the various scenarios in the Multi-Flow configuration 1.

Table 55. Throughput Test Results for Multi-Flow Configuration 1

Pub	Sub	Data Sample Size (Bytes)	Data Sample Size (bits)	PubRate (Hz)	Reliability QoS Policy	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)
<i>Secure VoIP</i>								
H1	H2	240	1920	100	BEST EFFORT	95	0.2	5.72
H1	H5	240	1920	100	BEST EFFORT	104	0.2	8.57
H2	H1	240	1920	100	BEST EFFORT	95	0.2	5.70
H2	H5	240	1920	100	BEST EFFORT	95	0.2	5.85
H5	H1	240	1920	100	BEST EFFORT	95	0.2	6.41
<i>Secure Video Communications</i>								
H3	H1	1500	12000	100	BEST EFFORT	97	1.2	4.82
H4	H5	1500	12000	100	BEST EFFORT	98	1.2	0.15
H2	H1	1500	12000	100	BEST EFFORT	92	1.1	3.64
<i>Secure Drone Telemetry</i>								
H3	H1	60	480	100	RELIABLE	60	0.029	0.00
H4	H5	60	480	100	RELIABLE	95	0.046	0.00
<i>Secure Drone Control</i>								
H1	H3	40	320	100	RELIABLE	59	0.019	0.00
H5	H4	40	320	100	RELIABLE	99	0.032	0.00

2. Latency Test Results

Table 56 shows the Latency Test results for the various scenarios in the Multi-Flow configuration 1.

Table 56. Latency Test Results for Multi-Flow Configuration 1

Pub	Sub	Data Sample Size (Bytes)	PubRate (Hz)	Reliability QoS Policy	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)
<i>Secure VoIP</i>							
H1	H2	240	100	RELIABLE	272.81	571.51	288.38
H1	H5	240	100	RELIABLE	277.48	573.14	288.37
H2	H1	240	100	RELIABLE	272.13	563.91	285.10
H2	H5	240	100	RELIABLE	273.16	570.14	297.21
H5	H1	240	100	RELIABLE	276.41	578.08	289.04
<i>Secure Video Communications</i>							
H3	H1	1500	100	RELIABLE	291.75	603.43	309.02
H4	H5	1500	100	RELIABLE	9.27	29.59	10.46
H2	H1	1500	100	RELIABLE	276.36	568.66	291.37
<i>Secure Drone Telemetry</i>							
H3	H1	60	100	RELIABLE	288.63	596.60	307.09
H4	H5	60	100	RELIABLE	9.11	25.32	10.11
<i>Secure Drone Control</i>							
H1	H3	40	100	RELIABLE	288.26	598.24	299.66
H5	H4	40	100	RELIABLE	9.10	24.12	10.11

D. MULTI-FLOW CONFIGURATION 2

1. Throughput Test Results

Table 57 shows the Throughput Test results for the various scenarios in the Multi-Flow configuration 2.

Table 57. Throughput Test Results for Multi-Flow Configuration 2

Pub	Sub	Data Sample Size (Bytes)	Data Sample Size (bits)	PubRate (Hz)	Reliability QoS Policy	Avg # of DSsps	Avg Throughput (Mbps)	Loss (%)
<i>Secure VoIP</i>								
H1	H2	240	1920	50	BEST EFFORT	47	0.1	0.86
H1	H5	240	1920	50	BEST EFFORT	49	0.1	1.31
H2	H1	240	1920	50	BEST EFFORT	47	0.1	1.39
H2	H5	240	1920	50	BEST EFFORT	61	0.1	1.19
H5	H1	240	1920	50	BEST EFFORT	48	0.1	1.20
<i>Secure Video Communications</i>								
H3	H1	1500	12000	50	BEST EFFORT	45	0.5	2.49
H4	H5	1500	12000	50	BEST EFFORT	48	0.6	0.31
H2	H1	1500	12000	50	BEST EFFORT	46	0.6	2.07
<i>Secure Drone Telemetry</i>								
H3	H1	60	480	30	RELIABLE	23	0.011	0.00
H4	H5	60	480	30	RELIABLE	27	0.013	0.00
<i>Secure Drone Control</i>								
H1	H3	40	320	30	RELIABLE	22	0.007	0.00
H5	H4	40	320	30	RELIABLE	27	0.009	0.00

2. Latency Test Results

Table 58 shows the Latency Test results for the various scenarios in the Multi-Flow configuration 2.

Table 58. Latency Test Results for Multi-Flow Configuration 2

Pub	Sub	Data Sample Size (Bytes)	PubRate (Hz)	Reliability QoS Policy	Min Latency (ms)	Max Latency (ms)	Avg Latency (ms)
<i>Secure VoIP</i>							
H1	H2	240	50	RELIABLE	273.97	570.20	286.98
H1	H5	240	50	RELIABLE	275.88	576.48	294.08
H2	H1	240	50	RELIABLE	272.73	566.45	284.09
H2	H5	240	50	RELIABLE	272.15	563.44	283.84
H5	H1	240	50	RELIABLE	277.98	575.18	298.18
<i>Secure Video Communications</i>							
H3	H1	1500	50	RELIABLE	291.74	891.72	317.38
H4	H5	1500	50	RELIABLE	9.25	26.74	10.48
H2	H1	1500	50	RELIABLE	278.35	617.90	295.37
<i>Secure Drone Telemetry</i>							
H3	H1	60	30	RELIABLE	288.06	597.47	309.28
H4	H5	60	30	RELIABLE	9.13	22.55	10.09
<i>Secure Drone Control</i>							
H1	H3	40	30	RELIABLE	287.58	595.64	304.67
H5	H4	40	30	RELIABLE	9.08	22.10	10.08

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- [1] M. Mehta, “Top 5 Industry Early Adopters Of Autonomous Systems.” Forbes, May 28, 2018, [Online]. Available: <https://www.forbes.com/sites/oracle/2018/05/28/top-5-industry-early-adopters-of-autonomous-systems/?sh=27b54972b931>.
- [2] Committee on Autonomous Vehicles in Support of Naval Operations, Naval Studies Board, Division on Engineering and Physical Sciences, and National Research Council of the National Academies, *Autonomous Vehicles in Support of Naval Operations*. Washington, DC, USA: National Academies Press, 2005.
- [3] NUWC Division Newport Public Affairs, “Evolving Command, Control and Communications for Unmanned Systems.” NAVSEA, Jan. 08, 2021, [Online]. Available: <https://www.navsea.navy.mil/Media/News/SavedNewsModule/Article/2466552/evolving-command-control-and-communications-for-unmanned-systems/>.
- [4] DDS Foundation, “What is DDS?” Object Management Group, Accessed: Jan. 15, 2021. [Online]. Available: <https://www.dds-foundation.org/what-is-dds-3/>.
- [5] B. Lantz, B. Heller, and N. McKeown, “A network in a laptop: rapid prototyping for software-defined networks,” in *Proceedings of the Ninth ACM SIGCOMM Workshop on Hot Topics in Networks*, 2010, pp. 1–6, [Online]. Available: <http://portal.acm.org/citation.cfm?doid=1868447.1868466>.
- [6] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, “A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks,” *IEEE Commun. Surv. Tutor.*, vol. 16, no. 3, pp. 1617–1634, 2014, doi: 10.1109/SURV.2014.012214.00180.
- [7] N. McKeown *et al.*, “OpenFlow: enabling innovation in campus networks,” in *ACM SIGCOMM Computer Communication Review*, Mar. 2008, vol. 38, pp. 69–74, doi: 10.1145/1355734.1355746.
- [8] Bob Lantz, Nikhil Handigol, Brandon Heller, and Vimal Jeyakumar, “Introduction to Mininet.” GitHub, Sep. 25, 2018, [Online]. Available: <https://github.com/mininet/mininet/wiki/Introduction-to-Mininet>.
- [9] D. Muelas, J. Ramos, and J. E. L. d. Vergara, “Assessing the Limits of Mininet-Based Environments for Network Experimentation,” *IEEE Netw.*, vol. 32, no. 6, pp. 168–176, Nov. 2018, doi: 10.1109/MNET.2018.1700277.
- [10] RTI, “Data-Centric Middleware.” Accessed: Jan. 17, 2021. [Online]. Available: https://www.rti.com/hubfs/docs/RTI_Data_Centric_Middleware.pdf.

- [11] DDS Foundation, “How Does DDS Work?” Object Management Group, Accessed: Jan. 15, 2021. [Online]. Available: <https://www.dds-foundation.org/how-dds-works/>.
- [12] Object Management Group, “Data Distribution Service (DDS) Version 1.4.” Apr. 2015, Accessed: Jan. 15, 2021. [Online]. Available: <https://www.omg.org/spec/DDS/1.4/PDF>.
- [13] Object Management Group, “The Real-time Publish-Subscribe Protocol DDS Interoperability Wire Protocol (DDSI-RTPSTM) Specification Version 2.3.” Apr. 2019, Accessed: Jan. 15, 2021. [Online]. Available: <https://www.omg.org/spec/DDSI-RTPS/2.3/PDF>.
- [14] H.-Y. Choi, A. L. King, and I. Lee, “Making DDS Really Real-Time with Openflow,” in *Proceedings of the 13th International Conference on Embedded Software*, Oct. 2016, pp. 1–10, doi: 10.1145/2968478.2968479.
- [15] K. An, A. Gokhale, D. Schmidt, S. Tambe, P. Pazandak, and G. Pardo-Castellote, “Content-Based Filtering Discovery Protocol (CFDP): Scalable and Efficient OMG DDS Discovery Protocol,” in *Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems - DEBS '14*, 2014, pp. 130–141, doi: 10.1145/2611286.2611300.
- [16] Object Management Group, “DDS Security Version 1.1.” Jul. 2018, Accessed: Jan. 15, 2021. [Online]. Available: <https://www.omg.org/spec/DDS-SECURITY/1.1/PDF>.
- [17] M. J. Michaud, T. Dean, and S. P. Leblanc, “Attacking OMG Data Distribution Service (DDS) Based Real-Time Mission Critical Distributed Systems,” in *2018 13th International Conference on Malicious and Unwanted Software (MALWARE)*, Nantucket, MA, USA, Oct. 2018, pp. 68–77, doi: 10.1109/MALWARE.2018.8659368.
- [18] V. DiLuoffo, W. R. Michalson, and B. Sunar, “Robot Operating System 2: The need for a holistic security approach to robotic architectures,” *Int. J. Adv. Robot. Syst.*, vol. 15, no. 3, p. 172988141877001, May 2018, doi: 10.1177/1729881418770011.
- [19] G. Pardo and R. White, “Leveraging DDS Security in ROS2,” presented at the ROSCon 2018, Accessed: Jan. 15, 2021. [Online]. Available: https://roscon.ros.org/2018/presentations/ROSCon2018_DDS_Security_in_ROS2.pdf.
- [20] Real-Time Innovations Inc, “RTI Perftest Version 3.1.” Dec. 2020, Accessed: Jan. 15, 2021. [Online]. Available: <https://community.rti.com/static/documentation/perftest/current/index.html>.

- [21] V. DiLuoffo, W. R. Michalson, and B. Sunar, “Credential Masquerading and OpenSSL Spy: Exploring ROS 2 using DDS security,” Apr. 2019, Accessed: Jan. 24, 2021. [Online]. Available: <http://arxiv.org/abs/1904.09179>.
- [22] R. Goyal, S. Kota, R. Jain, S. Fahmy, B. Vandalore, and J. Kallaus, “Analysis and Simulation of Delay and Buffer Requirements of Satellite-ATM Networks for TCP/IP Traffic.” Cornell University, Sep. 23, 1998, [Online]. Available: <https://arxiv.org/abs/cs/9809052v1>.
- [23] N. Beheshti, Y. Ganjali, and M. Ghobadi, “Experimental Study of Router Buffer Sizing,” in *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*, Oct. 2008, pp. 197–210, [Online]. Available: <https://doi-org.libproxy.nps.edu/10.1145/1452520.1452545>.
- [24] Ground Control, “Satellite Communications Trailer.” Nov. 23, 2020, Accessed: Jan. 31, 2021. [Online]. Available: <https://www.groundcontrol.com/mobile-satellite-trailer.htm>.
- [25] H. Ullah, N. Gopalakrishnan Nair, A. Moore, C. Nugent, P. Muschamp, and M. Cuevas, “5G Communication: An Overview of Vehicle-to-Everything, Drones, and Healthcare Use-Cases,” *IEEE Access*, vol. 7, pp. 37251–37268, 2019, doi: 10.1109/ACCESS.2019.2905347.
- [26] A. Annese, P. Barsocchi, N. Celandroni, and E. Ferro, “Performance Evaluation of UDP Multimedia Traffic Flows in Satellite - WLAN Integrated Paths.” Institute of Information Science and Technologies, Italian National Research Council, 2005, [Online]. Available: https://openportal.isti.cnr.it/data/2005/160273/2005_160273.pdf.
- [27] J. A. R. P. de Carvalho, H. Veiga, P. Gomes, C. F. F. P. R. Pacheco, N. Marques, and A. D. Reis, “Laboratory performance of wi-fi point-to-point links: A case study,” in *2009 Wireless Telecommunications Symposium*, Prague, May 2009, pp. 1–5, doi: 10.1109/WTS.2009.5068953.
- [28] G. Giambene, “QoS Requirements for Multimedia Services,” in *Resource Management in Satellite Networks: Optimization and Cross-Layer Design*, J. I. Moreno Novella and F. J. Gonzalez Castano, Eds. New York, N.Y: Springer, 2007, pp. 67–94.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California