NASA/CR—2015-218842

National Air Space (NAS) Data Exchange Environment Through 2060

Aloke Roy
Honeywell, Columbia, Maryland

August 2015

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI Program provides access to the NASA Technical Report Server—Registered (NTRS Reg) and NASA Technical Report Server—Public (NTRS) thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counter-part of peer-reviewed formal professional papers, but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., "quick-release" reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at http://www.sti.nasa.gov

- E-mail your question to help@sti.nasa.gov

- Fax your question to the NASA STI Information Desk at 757-864-6500

- Telephone the NASA STI Information Desk at 757-864-9658

- Write to:
  NASA STI Program
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

NASA/CR—2015-218842

National Air Space (NAS) Data Exchange Environment Through 2060

Aloke Roy
Honeywell, Columbia, Maryland

Prepared under Contract NNA12AB80C

National Aeronautics and
Space Administration

Glenn Research Center
Cleveland, Ohio 44135

August 2015

Level of Review: This material has been technically reviewed by NASA technical management.

Available from

NASA STI Program
Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
703-605-6000

This report is available in electronic form at http://www.sti.nasa.gov/ and http://ntrs.nasa.gov/

National Air Space (NAS) Data Exchange Environment Through 2060

Aloke Roy
Honeywell
Columbia, Maryland 41046

DOCUMENT REVISION LOG

Revision	Description	Date
01	Initial release	4 August 2014

Table of Contents

List of Figures

List of Tables

Best Alternatives Assessment Report

EXECUTIVE SUMMARY

NASA's NextGen Concepts and Technology Development (CTD) Project focuses on capabilities to improve safety, capacity and efficiency of the National Air Space (NAS). In order to achieve those objectives, NASA sought industry-Government partnerships to research and identify solutions for traffic flow management, dynamic airspace configuration, separation assurance, super density operations, airport surface operations and similar forward-looking air-traffic modernization (ATM) concepts. Data exchanges over NAS being the key enabler for most of these ATM concepts, the Sub-Topic area 3 of the CTD project sought to identify technology candidates that can satisfy air-to-air and air/ground communications needs of the NAS in the year 2060 timeframe. Honeywell, under a two-year contract with NASA, is working on this communications technology research initiative. This report summarizes Honeywell's research conducted during the second year of the study task.

In the first year of the performance period, Honeywell conducted a systematic survey of the public domain literature to identify current, emerging and embryonic communication technologies, which included a wide range, starting with the existing, narrow bandwidth, low data rate, ACARS to the very futuristic optical and X-ray communications. Characterization of those technologies was done in an Excel-based workbook using a common set of key attributes and characteristics, which were derived from performance requirements defined in aviation standards. Subsequently, a Quality Function Deployment (QFD) analysis tool was used to map critical needs of key ATM applications to the capabilities of the candidate technologies to prioritize the technology candidates that can meet air-to-air and air/ground ATM application needs. A common architectural framework was established to define the data exchange environment and the context of the air-to-air and air/ground networks in that environment. Three architectures were analyzed using future cellular, next generation Ku/Ka band SATCOM and Self-Organizing Orthogonal Frequency Division Multiple Access (SO-OFDMA) technologies. Architecture options included cellular base stations located on High Altitude Platforms (HAP) and Free Space Optical (FSO) communications for cross-connects. Finally, overall system expenditure against benefits were compared for the proposed architectures to choose the right architecture for NAS environment with minimum cost outflows. The first year of study concluded that a hybrid communications architecture consisting of cellular technology for terrestrial, satellite for Oceanic, polar and remote regions and SO-OFDMA for air-to-air networking will be best suited to meet the future communication needs of the NAS.

The second year of study started from the architecture recommendations of the first year deliverables. The research involved two focus areas: operational and security analyses of the terrestrial and HAP-based cellular, satellite and air-to-air architectures. The operational analysis consisted of two steps: a operational view analysis and simulation modeling of the communication technologies.

The operational view analysis started with the ATM operational concepts and their communication services enablers. The required information flows for those services were estimated by aircraft type, airspace domain and the phase of flight. The information flows were based on the Version 2 of Communications Operating Concept and Requirements for the Future Radio System (COCR) jointly developed by FAA and EUROCONTROL. The data traffic estimated in the COCR was escalated by 2.5% per year to derive the data communication demand for most of the services and aircraft classes. The 2.5% per year escalation factor was recommended in the COCR. Aircraft distribution and movement over National Air Space (NAS) was based on actual aircraft flight data reported by FAA for January 23, 2014. The aircraft data was escalated by a factor of 0.5% per year, which was used by FAA in a recent report to estimate air traffic in the year 2033. To estimate UAS distribution over NAS, it was assumed that UAS operation will be concentrated around major urban areas. Top two hundred and fifty urban areas in the NAS were selected

based on their population density and the UAS platforms were distributed to those areas based on their population ranking. Aircraft movement was simulated at five minute interval over a 24-hour period using a visual tool that permitted computation and display of aircraft concentration at national and regional levels.

For the simulation, a set of priority-based queuing models were developed to estimate the throughput, latency, and dropped packets by information service flows for the communication technologies identified in the first year of this study. The queuing models were combined with the visual simulation tool to evaluate the performance of the three network architectures: cellular, satellite and SO-OFDMA air-to-air.

The operational analysis concluded that the cellular architectures could support up to 400 aircraft in a cell without any significant degradation of the desired services. On the other hand, satellite architecture experienced significant loss of passenger data traffic even with five aircraft per spot beam and had loss of SWIM services when the number of aircraft exceeded fifty per spot beam. In addition, satellite networks had much higher latency compared to cellular networks due to higher propagation delays. The SO-OFDMA air-to-air network using VHF media could support basic surveillance, air traffic and airline operational services but did not have adequate capacity to support SWIM or passenger data.

For the security analysis, a security perimeter was defined between the regulated aeronautical network and the unregulated public network. All classes of devices on the perimeter that would be exposed to the public domain were identified at the first step of the analysis. Subsequently, high-level threat vectors for these classes of devices were identified. The safety objectives and the hazard severity categories for datalink services from the COCR were analyzed in the second step and mapped against the threat vectors to develop a hazard score for each of the threats identified in the first step. In the third step of the security analysis, vulnerability of the three recommended architectures were assessed against the probability of attaining certain hazard score for a given datalink service. If the assessed safety hazard probability of a threat was below the required safety objective for the datalink service, then that particular threat was classified to have no impact on the communication architecture to offer the datalink service. Conversely, if the hazard probability of a threat was higher than the safety objective, that threat was deemed have security impact on the recommended architecture. At the final step of the security analysis, some high level mitigation strategies were recommended for the threats having security impact on the proposed architectures. In summary, RF jamming and man-in-the-middle attacks are major concerns for cellular architectures whereas jamming of the feeder links from a UAS would have serious impact on satellite communications. Lack of link and media access control security in the SO-OFDMA air-to-air network makes it very vulnerable to many security threats. The dynamic nature of the broadcast mode SO-ODFMA makes it difficult to implement cost-effective security measures for this architecture.

This study concludes that all three technology elements, cellular, satellite and SO-OFDMA air-to-air would have a role in the future communications supporting air traffic management beyond NextGen. To mitigate some of the security risks associated with a technology architecture and to provide added capacity, flexibility, reliability and quality of service for future ATM, a hybrid communication architecture utilizing cellular, satellite and air-to-air networking is recommended. In addition, technology elements to seamlessly and simultaneously utilize all available air/ground connectivity options should be employed.

History of technology evolution over the last fifty years is indicative of the challenges to predict the communication technologies and ATM environment fifty years in the future. This Honeywell study captures a high-level view of the future based on current knowledge. It is possible that some game changing technology such as the personal computers, the Internet and the cell phones will materialize within the near future. Therefore, it is strongly recommended that this study be updated at a periodic interval to include future research and developments.

Free Space Optics (FSO), one of the technologies identified in this study, has the potential to become a game changer for future ATM communications. One of the key challenges for applying FSO to aeronautical communications is the acquisition and tracking of aircraft moving at very high relative speeds. Although this study included a preliminary assessment of the FSO technology, it is recommended that a future study should develop technical approach and system design for aircraft acquisition and tracking to support FSO communications.

Similar to FSO, operation of UAS in the NAS is in the infancy today. However, UASs may have a far-reaching impact on future ATM. Therefore, it is recommended that a detailed study be initiated as soon as possible to assess the impact of low-altitude UAS on future NAS communications. That study should also address harmonization strategies for UAS command and control links with traditional ATC communications as well as general integration of UAS information for situational awareness of the pilots and controllers.

In addition to the studies recommended above, Honeywell suggests the following items for future work:

- Develop high fidelity simulation models of the proposed architectures to perform tradeoff analyses and operational scenario-based simulations. By integrating these simulation models with other pre-existing NASA models, higher fidelity system models can be developed to aid future system design.
- Security analysis presented in this paper provides a high level assessment of the security threats, risks and their potential mitigation approaches. A future study should specifically expand this analysis to fully address the security vulnerabilities of the proposed architectures and develop mitigation approaches.
- RF spectrum is a very limited resource and its demand is increasing exponentially with time. Therefore, a future study should analyze the availability of effective spectrum for aeronautical communications and develop a technical approach for reuse and dynamic, on demand, allocation of spectrum.
- The aviation network of the future needs to be very dynamic with multiple air/ground connectivity options supporting simultaneous traffic flows with varied quality of service requirements and ad-hoc, self-configuring air-to-air networks. To maintain robust data flows and to assure low latency and jitter, future aeronautical networks must support sophisticated routing algorithms that can converge very quickly and impose very little system overhead. It is essential to research and design this routing algorithm soon such that it would be ready for standardization within the next ten years. This research should include management of multiple links for seamless inter-technology handovers and leverage currently evolving IP mobility standards.
- Similar to the routing challenges, aircraft architecture may also need to be investigated to facilitate such a dynamic network operation while ensuring security of the flight critical services and safety of flight.

This page left intentionally blank.

Best Alternatives Assessment Report

1. INTRODUCTION

1.1. PURPOSE

The purpose of this document is to provide the results of the Best Alternatives Assessment in Task 6 (Best Alternatives Assessment and Recommendation) of the Next Generation (NextGen) Concepts and Technology Development Project (CTD1), Sub-topic 3, under NASA contract NNA12AB80C. This document is Deliverable 9, to report the details of the Best Alternatives Assessment. Task 6 is part of Phase 2 of the CTD1 project to conduct further analyses and simulation modeling on the best technology alternatives and recommend the best technology for air-to-air and air/ground data communications over the National Air Space (NAS) through the year 2060.

1.2. SCOPE

The scope of this document is to report on the results of the Best Alternatives Assessment of Task 6. The Best Alternatives Assessment further assesses the best communication technology alternatives in operational and security assessments. The operational assessment includes an operational view analysis and simulation modeling analysis. In the simulation modeling analysis, data traffic corresponding to the predicted air traffic environment is simulated and assessed against the best technology alternatives and architecture options using these technology alternatives.

The best communication technology alternatives assessed in Task 6 of Phase 2 and as documented in this report include Cellular, Ku/Ka band SATCOM and Self-Organized Orthogonal Frequency Division Multiple Access (SO-OFDMA) communication technologies. In addition, Free Space Optical (FSO) was found to be a good supplemental technology for the alternatives in an aeronautical telecommunications network. Previous Task 2 in Phase 1 of the NASA CTD1 project identified, characterized and assessed an initial set of candidate communication technologies. The Task 2 assessment resulted in a down-selected list of leading candidates. Task 3 in Phase 1 conducted an architectural analysis of the leading technologies. The task developed communication architectures based on the selected technologies and using platforms such as ground towers, High Altitude Platforms (HAP), and Low Earth Orbit (LEO) and Geosynchronous Earth Orbit (GEO) satellites to achieve an aeronautical network for the future NAS environment. Task 4 of Phase 1 conducted a cost analysis of the leading technologies and architectures to identify the combination of the network architectures to achieve safety critical communication in a cost effective manner without compromising Required Communication Performances (RCPs). The results of the Phase 1 tasks are the three best technology alternatives and architectures, including FSO as a supplemental technology, which are further analyzed and assessed in Task 6 of Phase 2.

1.3. DOCUMENT OVERVIEW

1.3.1. Organization

This document is organized into the following sections:

- Section 1 – Introduction

  Identifies the purpose and scope of the document, summarizes document organization and document conventions, defines terminology and acronyms used throughout the document, and provides references to applicable documents.

- Section 2 – Background

  This section summarizes the activities done in previous tasks of the project. It briefly explains the results of the tasks leading up to the subject of this report, task 6 best alternatives assessment. It also provides summaries of the best technology alternatives and architectures.

- Section 3 – Approach for Best Alternatives Assessment

  This section describes the approach followed for the best technology alternatives assessment. It explains the approach of the operational assessment and security assessment. It identifies the constraints and assumptions of the assessments.

- Section 4 – Operational Assessment

  This section explains the Operational Assessment consisting of Operational View Analysis and a Simulation Modeling Analysis. It evaluates the best alternative technologies based on the operational assessment.

- Section 5 – Security Assessment

  This section describes the security assessment of the best technology alternatives and architectures. It describes the security assessment consisting of threat analysis and risk assessment. It provides the results of the assessment and recommends technical mitigations of the risks. It evaluates the best alternative technologies based on the security assessment.

- Section 6 – Conclusions

  This section provides the summary of the operational and security assessments conducted in Task 6. It summarizes the assessment of the best alternative technologies based on the operational and security assessments. It makes recommendations for future work.

1.3.2. Conventions

The following conventions are used throughout this document:

- Use of the notation [REF-XXX] refers to an applicable reference document, where XXX is the shorthand notation.

1.3.3. Document Relationships

This document reports on the assessment of the best technology alternatives down-selected in previous tasks in Phase 1 of the project. The initial Task 2 in the project identified, characterized and assessed candidate communication technologies. The task generated an initial list of the top technologies from the candidates. Task 3 analyzed architectures using the leading candidate technologies and down-selected the candidates to the best technology alternatives based on

architectural analysis. Task 4 analyzed the cost effectiveness of the technologies and architectures from Task 3.

In the Task 2 analysis, candidate communications technologies were identified, characterized and assessed for meeting the communications requirements of Air Traffic Management (ATM) applications in the year 2060 timeframe. A comparative analysis of the candidate technologies was conducted and summarized, and an initial list of down-selected technologies was generated. The Task 2 document is the *Report on Task 2 of the National Air Space (NAS) Data Exchange Environment Through 2060 project - Identification, Characterization and Mapping of Candidate Technologies* [TASK2RPT].

In Task 3, the architectures were developed using the top candidate communication technologies selected in Task 2 and as reported in the Task 2 report document. The best technologies were down-selected from the list of candidate technologies based on the architectural analysis. The architectures were assessed for air-to-air communication and air/ground communications and the results were summarized in the *Report on Task 3 of the National Air Space (NAS) Data Exchange Environment Through 2060 project – Architecture Analysis* [TASK3RPT]

In Task 4, the architectures analyzed in Task 3 were assessed for cost effectiveness to support air-to-air and air/ground communications. The results were summarized in the *Report on Task 4 of the National Air Space (NAS) Data Exchange Environment Through 2060 project – Cost Analysis* [TASK4RPT]

These documents and other reference documents providing input to the Task 6 analysis are listed in section 1.5.

1.3.4. Word Processing Algorithm

This document was prepared using Microsoft® Office Word 2007.

1.4. TERMINOLOGY

1.4.1. Acronyms

Acronym	Definition
ASDI	Aircraft Situation Display to Industry
AAC	Airline Administrative Communications
ATS	Air Traffic Services
AOC	Aeronautical Operational Control
APC	Airline Passenger Communication
ATR	Avions de Transport Regional (larger commercial air transport aircraft)
AC	Aircraft
AC ↔ BS link	Aircraft-to-ground base station link
AC ↔ HAP link	Aircraft-to-HAP base station link
AC ↔ SAT link	Aircraft-to-satellite link
APT	Airport
ANSPs	Air Navigation Service Providers
ATC	Air Traffic Control
AOA	Autonomous Operations Areas
Arv	arrival
ATM	Air Traffic Management
ATSP	Air Traffic Service Providers
Auth.	authentication
AVS	Advisory Services
BGA	Business and General Aviation
BS	Base station
CTD	Concepts and Technology Development
CSV	comma separated values
CIS	Clearance/ Instruction Services
Dep	departure
DSS	Delegated Separation Services
DL	downlink
DCM	Data Communications Management
DAG-TM	Distributed Air/Ground Traffic Management
EIS	Emergency Information Services
ENR	En-route
FSO	Free Space Optical
FPS	Flight Position/ Intent / Preferences Services
FMS	Flight Management System
FD	flight deck
FAA	Federal Aviation Administration
FSS	Flight Support Services
FIFO	First In, First Out
FSO	Free Space Optical
GDC	Global Data Center
GEO	Geostationary Earth Orbit
GES	Gateway Earth Station
Gbps	Giga-bits per second

Acronym	Definition
GUI	Graphical User Interface
GW	Gateway
HAP	High Altitude Platforms
ICAO	International Civil Aviation Organization
km	kilometer
LEO	Low Earth Orbit
MAC	Media Access Control
MMS	Multimedia Messaging Service
ms	millisecond
MSP	Mobile Service Provider
NETCONN	Network Connection
NETKEEP	Network Keep-alive
NAS	National Air Space
NMS	Network Management System
nm	Nautical mile
NW	network
OEM	Original Equipment Manufacturer
ORP	Oceanic/Remote/Polar
QOS	Quality of Service
RCP	Required Communication Performance
SATCOM	Satellite Communication
SAT ↔ GW link	Satellite-to-ground gateway link
SO-OFDMA	Self-Organized Orthogonal Frequency Division Multiple Access
SMS	Short Message Service
SAT	Satellite
SWIM	System Wide Information Management
TMA	Terminal Maneuvering Area
TBO	Trajectory-Based Operations
TS	Time Sample
TU	Transmission Unit
UTC	Universal Time Coordinated
UAV	Unmanned Aerial Vehicle
UAS	Unmanned Aircraft Systems
UL	uplink
UACS	Unmanned Aircraft Control Station
VPN	Virtual Private Network

1.5. APPLICABLE REFERENCE DOCUMENTS

The following documents, of the exact issue shown with the latest amendments and notes, form a part of this document to the extent specified herein.

1.5.1. Government/Regulatory

Shorthand	Document Number	Document Description
COCR	COCR Version 2.0	Communications Operating Concept and Requirements for the Future Radio System, 2006, version 2.0, EUROCONTROL/FAA
FAA2033		http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=14374

1.5.2. Industry

Shorthand	Document Number	Document Description / Link
ITUR	Report ITU-R M.2171	Characteristics of unmanned aircraft systems and spectrum requirements to support their safe operation in non-segregated airspace, ITU, December 2009
QUEUES		http://iew3.technion.ac.il/serveng2012S/Recitations/Rec13.pdf

1.5.3. Honeywell

Shorthand	Document Number	Document Description / Link
TASK2RPT	NNA12AB80C-D03-01-01	Report on Task 2 of the National Air Space (NAS) Data Exchange Environment Through 2060 project - Identification, Characterization and Mapping of Candidate Technologies, 1 May 2013, revision 01, Honeywell.
TASK3RPT	NNA12AB80C-D04-01-01	Report on Task 3 of the National Air Space (NAS) Data Exchange Environment Through 2060 project – Architecture Analysis, 1 August 2013, revision 01, Honeywell.
TASK4RPT	NNA12AB80C-D05-01-01	Report on Task 4 of the National Air Space (NAS) Data Exchange Environment Through 2060 project – Cost Analysis, 1 September 2013, revision 01, Honeywell.

2. BACKGROUND

This section provides background on the previous Phase 1 tasks and a summary of architectures using the best technology alternatives. The best technology alternatives will be further analyzed and assessed in context of the architectures.

2.1. SUMMARY OF PREVIOUS TASK ANALYSES AND ASSESSMENTS

The primary objective of NASA's Concept and Technology Development (CTD) project is to identify and assess the data exchange environment using air-to-air and air/ground communications to support Air Traffic Management (ATM) applications over National Air Space (NAS) through the year 2060.

In Task 2 of the project, high potential communication technologies to support NextGen air-to-air and air/ground datalinks were identified, characterized and evaluated. Top candidate were down-selected from the original list of 15 technologies from current, emerging and embryonic categories, in a comparative assessment against the requirements of critical ATM applications. See Task 2 report [TASK2RPT].

In Task 3, communication system architectures were developed using the top three candidate technologies, namely Cellular, Ku/Ka band SATCOM and SO-OFDMA, and platforms including HAP, Satellite and terrestrial platforms to achieve the data exchange environment for NAS. An architectural analysis was performed to identify the technical pros and cons of the three architecture options using the technologies. A hybrid architecture consisting of all three architectures was analyzed and shown to be an effective way to meet the communication requirements in the future NAS. FSO was identified as a supplemental technology in the architectures as a high throughput pipe for certain links in the architectures. The results were summarized in Task 3 report [TASK3RPT].

In Task 4, a cost analysis was performed on the architectures of the top three candidate technologies analyzed in Task 3 to identify the most cost effective solution to facilitate the future NAS requirements. The results of the cost analysis found all three technologies to be cost effective for meeting requirements specific to air-to-air and air/ground configurations for future ATM communications.

The three technologies are recommended as the best technology alternatives for further assessment. In Task 6, the best technology alternatives and architectures are assessed in operational and security assessments, which is the subject of this report.

2.2. SUMMARY OF ARCHITECTURE OPTIONS USING THE TECHNOLOGIES

The three architectures and the hybrid architecture that were analyzed in Tasks 3 and 4 are considered for the best alternatives assessment.

Architecture Option 1 is based on the future cellular technology (5G+ cellular) combined with the HAP platform. In this architecture, the terrestrial segment is supported by cellular network, while the airborne segment is supported by a HAP network. The HAP segment includes oceanic

regions and terrain-challenged terrestrial regions where it is difficult or expensive to install and maintain towers. The combination of both the terrestrial cellular network and the HAP based network will be able to support services in all airspaces. FSO link supplements this architecture for backend HAP-to-HAP or HAP-to-Ground communications.

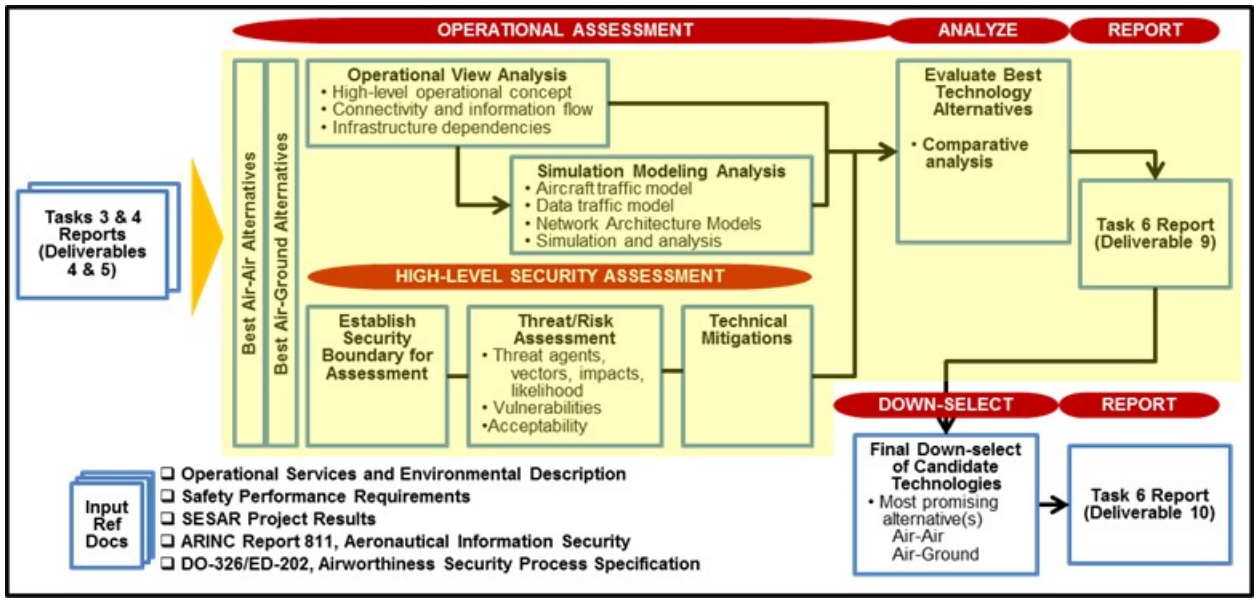
Architecture Option 2 is based on the Ku/Ka band SATCOM technology for providing access to aircraft in both terrestrial and oceanic regions for their communication with ground network. Aircraft makes use of satellite network installed in space for both the air/ground and air-to-air services. The satellite terrestrial network that provides connectivity to the ground network comprises of Gateway Earth Station (GES) and Network Management System (NMS). FSO link is considered as a possible secondary link for inter-satellite and satellite-ground to address some of the challenges and issues inherent in satellite communications.

Architecture Option 3 is based on broadband SO-OFDMA technology that uses VHF spectrum allocated for aeronautical purposes. SO-OFDMA is expected to provide air-to-air communication without any service cost for aircraft in all airspaces. Air-to-ground communication over terrestrial regions can be accomplished by having at least one SO-OFDMA node per cell installed on the ground. In oceanic regions, where it is not possible to have ground infrastructure, the packets are routed to the nearest ground SO-OFDMA node through a network of aircraft flying in the region. Hence the combination of both airborne and ground segment will be able to provide air/ground communication needed for an aircraft. FSO is a possible supplemental technology as a secondary air/ground link. In addition, FSO may be combined with SO-OFDMA as a point-to-point system for air-to-air relaying of data traffic in support high air traffic corridors. FSO provides a possible high throughput pipe between aircraft for message relaying.

Hybrid Architecture is a hybrid of all three architectures including HAPs, satellite and terrestrial networks. SO-OFDMA is the most suitable architecture for air-to-air service, while the combination of satellites and HAPs provide a solution for air/ground communications. Cellular network covers the terrestrial regions similar to the HAP-Cellular architecture. Most of the oceanic regions are covered by GEO systems and the high traffic oceanic and terrain challenged terrestrial regions are covered by HAPs. FSO may serve as a supplementary link or may be aimed as a primary technology for air/ground traffic. In terrestrial regions for altitudes below 10,000 ft, where FSO availability may become an issue, cellular technology may be used to provide a supplementary link. FSO may also provide a high throughput pipe between aircraft.

3. APPROACH FOR BEST ALTERNATIVES ASSESSMENT

Figure 3-1 illustrates the approach for the best alternatives assessment activities of Task 6. The high-level activities are highlighted in the figure and include operational assessment, security assessment, comparative analysis and report on the assessments and comparative analysis as reported in this Deliverable 9 document.



Note: The figure highlights the activities conducted as reported in this document, Deliverable 9.

Figure 3-1 Approach for Best Alternatives Assessment

3.1. OPERATIONAL ASSESSMENT

The operational assessment consists of an operational view analysis and simulation modeling analysis. The operational view analysis begins with a high level concept of operations of ATM operational services and the communication services that enable the operational services in the 2060 timeframe. It identifies the information flows of the communication services in the air-to-air and air/ground networks and analyzes the volume of data traffic in the information flows based on aircraft type, airspace domain and phase of flight. The data traffic results are input to the simulation modeling analysis.

The simulation modeling analysis begins by modeling the data flows in the architectures that utilize the best alternative technologies. The models evaluate the performance of the technologies in meeting latency and data throughput requirements of the communication service types. The requirements for data throughput were established by the data traffic results from the operation view analysis. The architecture models then provide the basic modeling concepts and parameters for an aircraft and data traffic simulation and visualization covering the NAS in the 2060 timeframe. The simulation generates latency and data throughput performance results, which are compared to the results of the architecture and data flow models to help validate the models. Performance is measured in terms of latency, data packet loss, achievable throughput and

scalability. The simulation is configurable to change parameters and conduct sensitivity analyses. The best alternative technologies are evaluated based on the results of the operational assessment.

3.2. SECURITY ASSESSMENT

The security perimeter boundary is first established and described to set the context of the security assessment. The contexts of the assessment are the access network architectures that utilize the best communication technology alternatives. The security assessment then conducts a threat analysis and risk assessment within the security perimeters. Security assessment outside of the perimeters is outside the scope of the assessment. The threat analysis identifies and defines threat agents and the threat vectors used by the agents to attack the access networks. It determines the impact and likelihood of each threat. The vulnerability assessment considers and evaluates the weaknesses and exploitability of the access networks to threats. The risk assessment determines the risk of each threat based on the impact and likelihood of the threat and the vulnerability of the access network to the threat. The acceptability of each risk is evaluated to determine the need for mitigations of the risks. The security assessment determines technical mitigations of the unacceptable risks. Only technical mitigations are considered as security policy and operational mitigations are outside the scope of the assessment. The best alternative technologies are evaluated based on the results of the security assessment.

4. OPERATIONAL ASSESSMENT

The three technology candidates chosen as best technology alternatives are analyzed and assessed in an operational assessment. The operational assessment is conducted as an operational view analysis and simulation modeling analysis.

4.1. OPERATIONAL VIEW ANALYSIS

The operational view analysis provides a high-level concept of ATM operations in the 2060 timeframe to understand the required information flows of the communication services that enable the ATM operations. The operational view analysis identifies and characterizes the information flows based on type of aircraft traffic that utilize the communication services, airspace domain and phase of flight. It provides estimates of data traffic loads in the flows, which are then used in the simulation modeling.

4.1.1. Overview of the ATM Concept of Operations in 2060

The Next Generation Air Transportation System (NextGen) aims to make air travel more convenient while ensuring flight operations to be safe, secure and efficient. Advancements in the technologies enable more efficient operations and thus aid in transformation to NextGen. The role of future ATM environment is envisaged as a paradigm shift from controlling aircraft movement to managing air-space. The paradigm shift is seen to be manifested in the following aspects:

- Use of less voice to use of mostly data communications
- Shift to trajectory-based management
- More cooperative management between aircraft and between aircraft and air traffic controllers
- Sharing of more information across NAS information sources.

Communication services to enable the operational services are envisaged as undergoing a paradigm shift as well, to sharing of common broadband IP-based aeronautical communications networks by different types of communications traffic. The traffic congestion problems will be solved by advancements in the technology, new applications, accuracy, and automation of systems.

The ATM paradigm shifts from less voice to more data communications. Data link is expected to play an important role for transmission of routine exchanges. The data link will change the workload distribution of air traffic controller and aircrew. However, it is expected that data communications will not normally be used for transmission of urgent, safety critical messages in tactical traffic situations. Real time voice channels will remain primary mean of communications for certain communications (non-routine, failure recovery and emergency).

The ATM Concept of Operations for 2060 will have a paradigm shift from a tactical control by air traffic controllers to strategic management by controllers and more autonomous operations handled by aircrew and automation. In en-route airspace, trajectory-based operations (TBO) will be used. Strategic and trajectory-based management enabled by data links will be the standard mode of operation in the future system. The data link exchange of trajectories between the flight deck and the ground-side automation might involve down linking the active aircraft trajectory from the Flight Management System (FMS) to the ground automation or uplinking a trajectory clearance

from the controller workstation to the flight deck. The concept of dynamic management of airspace will permit suitably equipped aircraft to select the most advantageous route to its destination. A structured routing system will continue to exist in managed airspace, in particular around major traffic centers with Air Traffic Control (ATC) in charge of managing the routes taken by aircraft. At the same time, total flexibility will exist in areas with autonomous aircraft operations in so called Autonomous Operations Areas (AOA) segregated from the managed airspace.

Higher level of cooperation between the flight crew and ATC for air traffic management is envisaged to achieve capacity and efficiency benefits. Cooperative air traffic management shall provide airspace users with increased flexibility in managing their operations through improved information exchange between the aircraft and ATC. Airborne devices will provide aircrew with enhanced situational awareness and allow a more co-operative ATM between controllers and aircrew. Flight crews of properly equipped aircraft can share flight path changes automatically as 4D trajectories for traffic flow constraints with the area controller or operate at higher levels of autonomy. Routine tasks like handoffs and transfer of communication can be conducted by the automation. Tasks like aircraft-to-aircraft spacing may be delegated to the flight crews by the controller. ATM operations are envisioned to rely on end-to-end strategic traffic flow management, data link communication and information sharing to facilitate fuel efficient flight profiles coordinated between ground automation and airborne flight management systems while minimizing adverse weather effects. Distribution of Air/Ground traffic management between flight crew, air traffic service providers (ATSP) and aeronautical operational control (AOC) personnel shall increase system capacity, while meeting air traffic management (ATM) requirements. The distributed air traffic management may solve a series of key ATM problems (or inefficiencies) in the gate-to-gate operations of the current NAS by utilizing distributed decision-making between the user (flight crew and/or AOC) and the ATSP.

The System Wide Information Management (SWIM) framework shall provide efficient air-ground mechanism for the data management, exchange, and sharing of information available from the various NAS information systems among flight crews, air traffic controllers, airline dispatchers, the military, government agencies, and other users of the NAS. The aircraft data that may be provided by SWIM includes, but is not limited to, video surveillance, aircraft sensor information, and Pilot Reports. SWIM based services will help create a shared common situational awareness among the flight crew, AOC personnel, air traffic controllers, and worldwide Air Navigation Service Providers (ANSPs) throughout the entire flight.

The future network in the 2060 timeframe is envisaged to be a collection of interconnected IP-based networks. Multiple access networks will use different wireless link technologies with significantly different characteristics (ground based, satellite-based, aircraft-to-aircraft). ATM traffic will share common IP-based access networks with other types of data traffic and compete for resources such as data bandwidth. Usage by end users will be seamless across the different access networks during flight phases.

A brief summary of operational concepts envisaged in the 2060 timeframe accommodating significantly increased traffic levels with broader aircraft performance envelopes and with more operators in the same airspace is provided in Table 4-1.

Table 4-1 ATM Operational Concepts Envisaged in the Year 2060

Operation	Description
Collaborative Traffic Management	Co-operation between controllers and flight crews in decision making using the availability of advanced technologies, tools and procedures to improve aircraft movements, reduce spacing and separation requirements, while improving arrival and departure sequencing.
Net-Centric Operations	Network enabled secured information access in real time to improve operational decision making. Timely access to information increases situational awareness while providing consistency of information among decision makers.
Weather Operations	Weather data incorporated in Decision Support Systems (DSS), bypassing the need for manual interpretation, to improve forecast accuracy and minimize the effects of weather on operations. Standardized set of weather sensors/algorithms on board to provide wind, temperature, water vapor, turbulence, and icing data to other users via network
Layered security	A multi-layered security system to mitigate threats. A security system consisting of layers of defense (including techniques, tools, sensors, processes) to help reduce the overall risk of a threat.
Trajectory-Based Operations	Exchange of 4D trajectories between controllers and aircraft to dynamically adjust a flight path in space (longitude, latitude, altitude) more accurately allowing the decrease in separation and increase in airspace capacity

4.1.2. System Context for the Operational View Analysis

The operational view analysis considers communication services as enablers for ATM. Communication services are provided via air/ground communications between aircraft and ground systems, air-to-air communications between two aircraft and ground/ground communications. Ground/ground communications for example include communications between two ATC centers. Both data and voice links will be used for air/ground and air-to-air communications. Data link will be the primary means of communications for most services except some real-time scenarios. Voice links will be used as primary means for non-routine, failure recovery and emergency communications.

This analysis considers data link communication services in air-to-air and air/ground scenarios, as highlighted in the notional communication systems architecture shown in Figure 4-1. Ground-ground network and onboard aircraft networks are not included in the analysis. The analysis considers communicators services used by different aircraft types across the various airspace domains during the phases of flight of an aircraft.

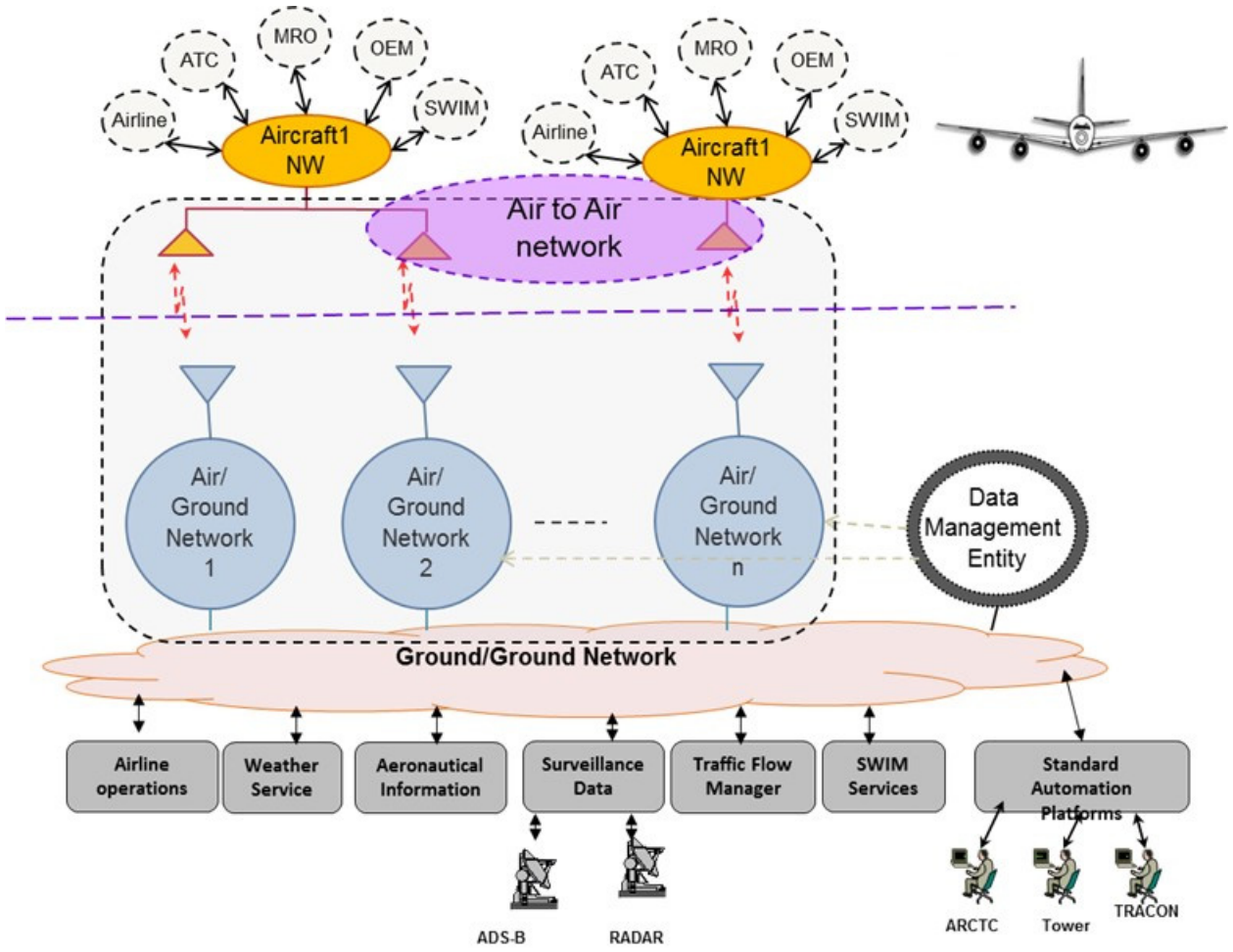


Figure 4-1 System Context for Operational Scenarios

4.1.2.1. TYPES OF COMMUNICATION SERVICES

The different types of communication services that will be supported by the 2060 network include Air Traffic Services (ATS) communications, AOC communications, Airline Administrative Communications (AAC), Aeronautical Passenger Communications (APC) and SWIM communications. Only data links shall exist for SWIM information exchange whereas both data and voice links will be available for other services (ATS, AOC, AAC, and APC). ATS communication services will always have priority over all other services, and AOC communication services will always have priority over AAC and APC services. Communication management shall have mechanisms to prioritize the different service types and also shall be able to prioritize different message types within each service type. For a given service (ATS, AOC, AAC or APC), the system shall provide higher priority for voice services over data services. Also communication management shall prioritize the different services depending on the phase of the flight (e.g. temporary shutdown of APC in TMA/Airport if bandwidth unavailable).

ATS communications are communications related to air traffic services including air traffic control, aeronautical and meteorological information, position reporting and services related to safety and regularity of flight. These communications involve one or more air traffic service

administrations. AOC communications are communications required for the exercise of authority over the initiation, continuation, diversion and termination of flight for safety, regularity and efficiency reasons. AAC is communications are used by airlines related to the business aspects of operating their flights and transport services. These communications are used for a variety of purposes, such as flight and ground transportation, bookings, deployment of crew and aircraft or any other logistical purposes that maintain or enhance the efficiency of operation over-all flight. APC communications are related to the non-safety voice and data services to passengers and crew members for personal communications. SWIM communications are related to the simultaneous sharing of information available from various NAS information systems among flight crews, air traffic controllers, airline dispatchers, military, government agencies, and other users of the NAS.

4.1.2.1.1. Safety Related Services (ATS and AOC)

Air Traffic Services include ATS Voice Services and ATS Data Services. The major ATS Data Services are Data Communications Management Services (DCM), Clearance/ Instruction Services (CIS), Flight Information Services (FIS), Advisory Services (AVS), Emergency Information Services (EIS), Delegated Separation Services (DSS), Common Trajectory Coordination Services, Flight Position/ Intent / Preferences Services (FPS). Aeronautical Operational Control (AOC) services include AOC Voice Services and AOC Data Services.

A class of network management services identified to support operational ATS and AOC services are Network Connection (NETCONN) and Network Keep-alive (NETKEEP).

4.1.2.1.2. Non- safety Related Services (AAC and APC)

The potential AAC services include Passenger Manifest, Aircraft Catering, Baggage Handling, and In-flight Assistance. The APC services identified are Web browsing, E-mail services, Short Message Service (SMS) and Multimedia Messaging Service (MMS), Virtual Private Networks (VPNs), Internet access, video conference services, voice services (telephony), fax services, audio and video streaming, live radio and live television.

4.1.2.1.3. SWIM Enabled Services

Services under the SWIM framework, as illustrated in

Figure 4-2, include Trajectory Information Exchange, Weather Information, Automated Flight Conditions Reports, Airport Diversion Planning, Surface Management with Trajectory Based Operations, and En-route Strategic Planning.

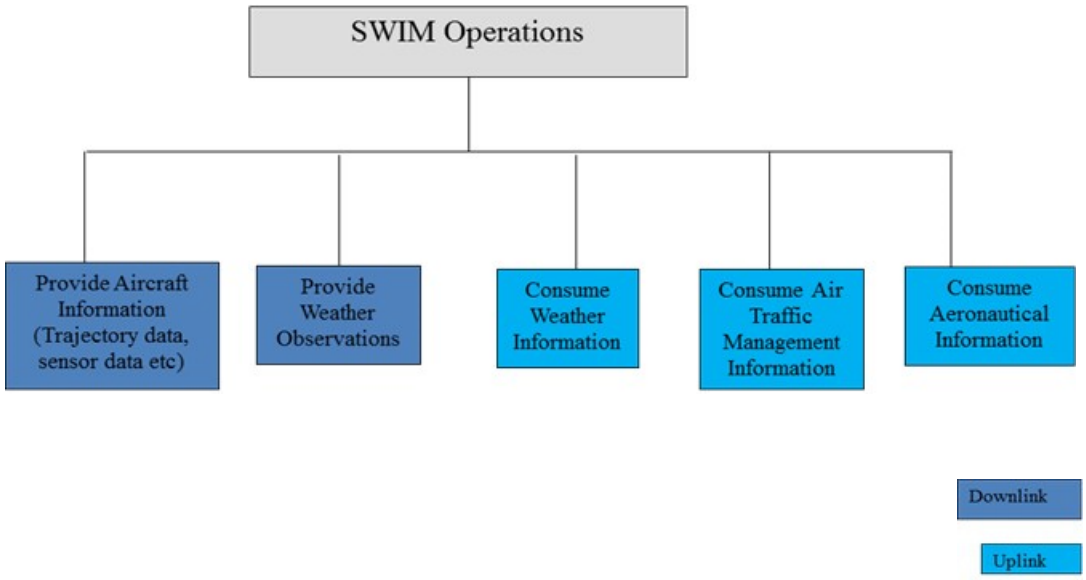


Figure 4-2 SWIM Operations

4.1.2.2. AIRSPACE DOMAINS AND FLIGHT PHASES

The operational scenarios for aeronautical communications are defined in relation to aircraft position in airspace domains and aircraft phase of flight. The airspace domains are Airport (APT), Terminal Maneuvering Area (TMA), En-route (ENR), Oceanic/Remote/Polar (ORP), and a new domain known as an Autonomous Operations Area (AOA) where the aircraft would be delegated self separation. The different phases of flight are identified below along with the domains in which the phases occur:

- Pre-Departure Phase in the APT Domain
- Departure Taxi in the APT Domain
- Departure in the TMA Domain
- Operations in the ENR, ORP and AOA Domains
- Arrival in the TMA Domain
- Arrival in the APT Domain
- Arrival Taxi in the APT Domain

For the various operational scenarios and different flight phases under each airspace domain, a wide range communication services are required and are discussed in the following sections.

4.1.2.3. SERVICES IN AIRSPACE DOMAINS

Figure 4-3 shows the various types of services that are available in different airspace domains. ATS, AOC and AAC services shall be available in all domains. APC services shall be available for passenger communications in ENR, ORP and AOA regions. However APC services may be available in APT and TMA based on remaining bandwidth availability after considering ATS, AOC and AAC usage. SWIM data exchange is expected in APT, TMA, ENR and ORP airspaces.

It is assumed that in AOA regions where AC operation is autonomous, there may be no SWIM data exchange.

Flight Phase / Service	APT	TMA	ENR	ORP	AOA
ATS	✓	✓	✓	✓	✓
AOC	✓	✓	✓	✓	✓
AAC	✓	✓	✓	✓	✓
APC	✓?	✓?	✓	✓	✓
SWIM	✓	✓	✓	✓	NA

✓ Available

✓? Available based on link availability, in low density regions

NA Not available

Figure 4-3 Services per Airspace Domain

4.1.2.4. INTEGRATION OF SERVICES AND TECHNOLOGIES

The future system shall be capable of allocating any available link that is suitable to a required service by taking into account the regulatory constraints, data bandwidth availability, etc., for the mapping of services onto the different links. Assuming relaxation in Civil Aviation Authority (CAA) rules, links deployed for APC communications could be certified for use as backup for ATS and AOC communications. ATS message sizes and volume are relatively small compared to typical APC data traffic. AOC and AAC volume may be similar and may be larger than ATS messages, but it is anticipated that APC traffic data will have much higher volume. SWIM traffic data can also have higher volume compared to ATS, AOC and AAC but maybe less than APC. The point is that APC could use the capacity that is not used for other communications, provided that this does not jeopardize safety related issues. Hence the same link can be used for different purposes, depending on the policy, priorities, airspace domain and the flight phase.

Moreover the system shall enable an aircraft to be simultaneously connected to and seamlessly roam between multiple independent access networks. This allows for make-before-break handover strategies ensuring the continuity and availability requirements of ATM applications.

4.1.2.5. AICRAFT TYPES

The future system shall support mixed aircraft population with varying capabilities and operating envelopes. Through 2060 there will be integration of new airspace users into the system. Microjets (typically 6 to 12 passengers), GA aircraft, military aircrafts (flying under civil rules) and Unmanned Aircraft Systems (UAS) may share the same airspace along with the commercial air lines, resulting in substantial increase of air traffic. The effect of new airspace users on NAS capacity depends on several factors including aircraft use in the airspace, the trip length and altitude, the implementation of new air traffic control technologies and equipment, and the performance capabilities and the rate of integration of the equipment.

4.1.3. Data Traffic Estimates

The following subsections provide the data traffic estimates based on the information flows identified and described above in section 4.1.2.

4.1.3.1. COMMERCIAL LARGE AIRCRAFT

Table 4-2 provides data from the Communications Operating Concept and Requirements for the Future Radio System (COCR) document [REF- COCR] on the estimated Phase 2 traffic for a single aircraft. Traffic estimates are provided for uplink (UL) and downlink (DL) traffic in each service volume (SV) – APT (departures and arrivals), TMA (departures and arrivals), ENR, ORP and AOA. To arrive at ATC and AOC traffic for a single aircraft during 2060 timeframe, the Phase 2 COCR traffic is extrapolated at an annual growth rate of 2.5% over 30 years and is provided in Table 4-3. The estimated data traffic requirement for the AAC service is expected to be similar to that of AOC. The estimated data traffic requirement for APC service per passenger is 2 Mbps DL and 1Mbps UL, based on consideration of applications like fax, voice, internet, video, etc., today. With an assumption of up to 150 passengers per large aircraft and with 20% of the passengers simultaneously using communication service, the total APC data requirement is 60 Mbps DL and 30 Mbps UL. The SWIM data requirements are expected to be around 1 Mbps each for DL and UL, for exchange of aircraft sensors data, graphical weather information, etc.

Table 4-2 Phase 2 Traffic Estimates (kbps) – Single Aircraft, 2030 Timeframe

PHASE 2 – 2030 Data Traffic in kbps		APT SV		TMA SV		ENR SV	ORP SV	AOA
		Dep	Arv	Dep	Arv			
Separate ATS	**UL**	20	3	20	20	20	15	20
	DL	30	10	30	30	30	20	30
	UL&DL	30	10	30	30	30	20	30
Separate AOC	**UL**	40	0.3	0.3	2	40	20	20
	DL	1	1	1	1	1	0.4	0.4
	UL&DL	40	1	1	2	40	20	20
Combined ATS&AOC	**UL**	40	3	20	20	40	20	30
	DL	30	10	30	30	30	20	30
	UL&DL	40	10	30	30	40	20	40

Table 4-3 Traffic Estimates (kbps) – Single Commercial Large Aircraft, 2060 Timeframe

Estimated traffic - 2060 (Data Traffic in kbps)		APT SV		TMA SV		ENR SV	ORP SV	AOA
		Dep	Arv	Dep	Arv			
ATS	UL	45	10	45	45	45	35	45
	DL	65	25	65	65	65	45	65
	UL&DL	65	25	65	65	65	45	65
AOC	UL	85	5	5	5	85	45	45
	DL	5	5	5	5	5	5	5
	UL&DL	85	5	5	5	85	45	45
AAC	UL	85	5	5	5	85	45	45
	DL	5	5	5	5	5	5	5
	UL&DL	85	5	5	5	85	45	45
APC	UL	1,000	1,000	1,000	1,000	1,000	1,000	1,000
	DL	5,000	5,000	5,000	5,000	5,000	5,000	5,000
	UL&DL	5,000	5,000	5,000	5,000	5,000	5,000	5,000
SWIM	UL	1,000	1,000	1,000	1,000	1,000	1,000	0
	DL	1,000	1,000	1,000	1,000	1,000	1,000	0
	UL&DL	2,000	2,000	2,000	2,000	2,000	2,000	0

4.1.3.2. MICROJETS

Microjets are an emerging population of commercial aircraft for small distances, flying with reduced flight plan. They are expected to represent up to 40% of daily traffic (REF-COCR) and will impact the aeronautical landscape. They have the same needs (for ATS/AOC/AAC/SWIM communications) as large commercial aircraft with less demanding in terms of APC communications. The estimated data traffic requirement for APC service per passenger is 2 Mbps DL and 1Mbps UL, based on the applications like fax, voice, internet, video. With an assumption of 12 passengers per microjet worst case and with 50% of the passengers simultaneously using communications, the total APC data requirement is 12 Mbps DL and 6 Mbps UL. Table 4-4, which is derived from Table 4-3, provides the estimated 2060 traffic for a single microjet.

Table 4-4 Traffic Estimates (kbps) – Single Microjet, 2060 Timeframe

Estimated traffic - 2060 (Data Traffic in kbps)		APT SV		TMA SV		ENR SV	ORP SV	AOA
		Dep	Arv	Dep	Arv			
ATS	UL	45	10	45	45	45	35	45
	DL	65	25	65	65	65	45	65
	UL&DL	65	25	65	65	65	45	65
AOC	UL	85	5	5	5	85	45	45
	DL	5	5	5	5	5	5	5
	UL&DL	85	5	5	5	85	45	45
AAC	UL	85	5	5	5	85	45	45
	DL	5	5	5	5	5	5	5
	UL&DL	85	5	5	5	85	45	45
APC	UL	6,000	6,000	6,000	6,000	6,000	6,000	6,000
	DL	12,000	12,000	12,000	12,000	12,000	12,000	12,000
SWIM	UL	1,000	1,000	1,000	1,000	1,000	1,000	0
	DL	1,000	1,000	1,000	1,000	1,000	1,000	0
Total	UL	7,500	7,500	7,500	7,500	7,500	7,500	6,500
	DL	13,500	13,500	13,500	13,500	13,500	13,500	12,500

4.1.3.3. BUSINESS AND GENERAL AVIATION AIRCRAFT

Business and General Aviation (BGA) aircraft are considered as non-commercial aircraft and include training flights, business jets, rescue flights and government-operated aircraft. BGA presents a higher increase in aircraft traffic than the rest of the aircraft types and is expected to grow about 0.5% per year in number from 220,670 aircraft in 2012 to 280,359 aircraft in 2060 [REF- FAA2033]. ATS communications for BGA are supposed to be the same as for any other aircraft. There will be less need for AOC as these are not commercial airlines with needs to optimize the fleet and flight schedules. Therefore, 50% of AOC traffic of large aircraft is assumed for BGA. On the other hand, there is a high demand for APC services. The estimated APC traffic requirement per passenger is 5 Mbps DL and 2 Mbps UL considering applications like telephony, VPN, video conferencing, etc., with high capacity needs during the entire flight. With an assumption of up to 10 passengers per BGA flight on average and with 90% of the passengers simultaneously using communications, the estimated data traffic requirement for APC service is 45 Mbps DL and 18 Mbps UL. Table 4-5 provides the estimated 2060 traffic for a single BGA aircraft derived using the data traffic requirements for large aircraft (see Table 4-3) to arrive at the traffic requirement for ATS, AOC, AAC, APC and SWIM, services.

Table 4-5 Traffic Estimates (kbps) – Single BGA Aircraft, 2060 Timeframe

Estimated traffic - 2060 (Data Traffic in kbps)		APT SV		TMA SV		ENR SV	ORP SV	AOA
		Dep	Arv	Dep	Arv			
ATS	UL	45	10	45	45	45	35	45
	DL	65	25	65	65	65	45	65
	UL&DL	65	25	65	65	65	45	65
AOC	UL	45	5	5	5	45	25	25
	DL	5	5	5	5	5	5	5
	UL&DL	45	5	5	5	45	25	25
AAC	UL	45	5	5	5	45	25	25
	DL	5	5	5	5	5	5	5
	UL&DL	45	5	5	5	45	25	25
APC	UL	18,000	18,000	18,000	18,000	18,000	18,000	18,000
	DL	45,000	45,000	45,000	45,000	45,000	45,000	45,000
SWIM	UL	1,000	1,000	1,000	1,000	1,000	1,000	0
	DL	1,000	1,000	1,000	1,000	1,000	1,000	0
Total	UL	20,000	20,000	20,000	20,000	20,000	20,000	19,000
	DL	46,500	46,500	46,500	46,500	46,500	46,500	4,5500

4.1.3.4. UNMANNED AIRCRAFT SYSTEMS

The Unmanned Aircraft System (UAS) are emerging as a new aircraft type, with a UAS flights expected to outnumber passenger flights in the year 2060 timeframe. Currently most UAS operations around the world are for military purposes. It is anticipated that new standards, regulations and procedures will be formulated to govern the safe integration of civil-use UAS into civilian air space for civil applications ranging from surveillance, scientific data gathering or delivery of services (crop dusting, parcel delivery, etc).

The safe operation of UAS relies on different communications, which represents a critical step in enabling UAS operations in non-segregated airspaces. The required radio communications for safe operation of UAS as illustrated in Figure 4-4 are:

- Radio communications for UAS command and control between the Unmanned Aircraft Control Station (UACS) and the UAS (tele-commands from UACS to the UAS, and telemetry, such as flight status, from the UAS to the UACS).
- Radio communications for air traffic services (voice and data) relay between ATC and the UACS via the UAS.

- Radio communications in support of "sense and avoid", between the UACS and the UAS for ensuring separation from nearby aircraft, terrain and obstacles (e.g. weather data video streams from UAS to UACS).
- Radio communications in support for navigation aids (ADS-B, etc).

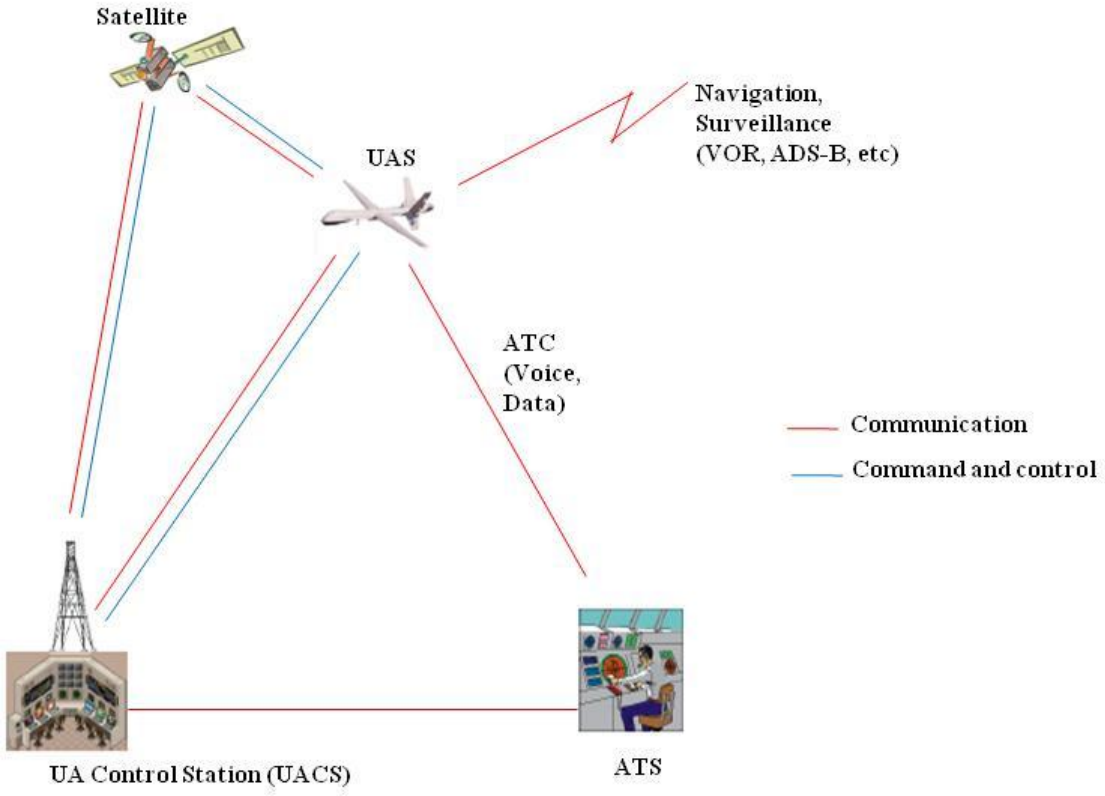


Figure 4-4 UAS Services

The main challenge is integration of Control and Non-Payload Communication (CNPC) and ATS communications to ensure safe and efficient operation of UAS in the civilian air space with no impact on ATS communication, system delays, capacity, safety, and security of passenger-carrying aircraft. For UAS systems, the estimated non-payload CNPC communications throughput for 2030 timeframe is provided in the task-2 report [REF-TASK2RPT], and is provided in Table 4-6. To determine the traffic requirements for the 2060 timeframe, the ATC, Sense and Avoid, Command/control traffic requirements are derived using Table 4-6 considering 2.5% growth every year. The AAC and SWIM traffic requirements for UAS are considered to be similar to that of the commercial aircraft. However the AAC and SWIM communications are expected to be exchanged through a ground link between UAS control station and ATC controller. Hence, over-the-air traffic is zero for these services. The use of UAS in commercial applications is expected to expand in a number of areas. Some of the expected civil and commercial applications of UAS include aerial video surveillance, commercial photography, news/sporting event coverage, infrastructure monitoring, including power facilities, shipping ports, pipelines, etc. The estimated APC traffic requirement for these services is up to 5 Mbps DL. The various data traffic estimates for the 2060 timeframe are provided in Table 4-7.

Table 4-6 Worst Case Non-payload Comm. Throughput for UAS, 2030 Timeframe

Worst Case Non-payload Communications Throughput (bits/sec) for the Year 2030									
Command and Control				ATS Relay			Send and Avoid		
Control		NavAids		ATS Voice Relay	ATS Data Relay		Target Tracks	Airborne Weather Radar	Video
UL	DL	UL	DL		UL	DL	DL		
4,606	7,615	669	1,140	4,800	113	173	9,170	27, 771	270,000

Table 4-7 Traffic Estimates (kbps) – Single UAS, 2060 timeframe

Worst Case Non-payload Communications Throughput (kbps) for the Year 2060 (extrapolated 2.5% growth Year-over-Year, YOY)																
Command and Control				ATS Relay			AAC		APC		SWIM		Sense and Avoid			
Control		NavAids		ATS Voice Relay	ATS Data Relay								Target Tracks	Airborne Weather Radar	Video	
UL	DL	UL	DL		UL	DL	UL	DL	UL	DL	UL	DL	DL			
10	15	5	5	10	5	5	0	0	0	5,000	0	0	20	60	570	

4.1.3.5. MILITARY AIRCRAFT

Military aircraft (when flying under civil rules) shall be considered as any other BGA aircraft to exchange data such as radar pictures, flight plan and direct voice communications. However the traffic requirement for military aircraft is not considered in this study because sufficient information is not available at this point of time about military aircraft traffic and their data requirement.

4.1.3.6. DATA FLOW SUMMARY

This section is a summary of the data traffic estimates. The data traffic requirements for safety critical traffic (ATS and AOC services) is approximately 300Kbps and contributes only up to 1% of the overall traffic requirement. High traffic requirement is expected in APC services to cater for various passenger needs. The various traffic requirements for different kinds of aircraft are summarized in the Table 4-8. Per aircraft throughput requirement is up to 100Mbps for large aircraft, 20Mbps for microjets, 70Mbps for BGA and 6Mbps for UAS (irrespective of flight phase and airspace domain).

Table 4-8 Data Traffic Estimates (kbps) – Summary, 2060 timeframe

Estimated Traffic 2060 in kbps		ATS	AOC	AAC	SWIM	APC	Total
Commercial AC (large)	**UL**	45	85	85	1,000	30,000	31,500
	DL	65	5	5	1,000	60,000	61,500
	UL&DL	100	100	100	2,000	90,000	100,000
Microjet	**UL**	45	85	85	1,000	6,000	75,00
	DL	65	5	5	1,000	12,000	13,500
	UL&DL	100	100	100	2,000	18,000	20,000
BGA	**UL**	45	45	45	1,000	20,000	21,500
	DL	65	5	5	1,000	45,000	46,500
	UL&DL	100	100	100	2,000	65,000	70,000
UAS	**UL**	10	10	0	0	0	100
	DL	10	700	0	0	5,000	6,000
	UL&DL	20	700	0	0	5,000	6,000

4.2. SIMULATION MODELING ANALYSIS

A simulation tool is developed to assess the operational performance of the aeronautical network for the future NAS environment through the year 2060. The three network architecture options identified in the Architecture Analysis report [REF-TASK3RPT] are considered for simulation modeling. For each network topology considered, an appropriate model is created, by carrying out network planning based on the estimated air traffic and data traffic requirements. The simulation model reflects the aeronautical environment as realistically as possible. This includes realistic flight patterns for the air traffic, a realistic model of the data traffic that is transmitted over the network, and a realistic representation of the ground network, including base stations for the air/ground links. Since the scenario considered is targeting the 2060 timeframe, a number of assumptions have to be made regarding, for example, the increase in air traffic during the upcoming years, the deployment of future wireless access technologies, the possibility of different kinds of aircraft flying in the same airspace with different flight phases and the amount of data traffic that will be generated in the network.

Security functionalities are not included in the definition of simulation scenarios, since the ability to cope with security threats and attacks cannot be verified by means of simulations. However, the security assessment for different architecture options identified in Architecture Analysis report [REF-TASK3RPT] is conducted under a separate subtask as reported in section 5.

4.2.1. Simulation Concept and Objectives

The overall concept of the simulation model is shown in Figure 4-5. The tool provides the operational performance reports for the identified three network architectures, with data traffic estimates and air traffic estimates input to the model. The operational scenarios provide a basis for estimating the data traffic needed for a single aircraft. These scenarios include all operations related to different kinds of services and for different kinds of aircraft envisaged through 2060. Another input for the tool, the air traffic model, is provided in section 4.2.3.

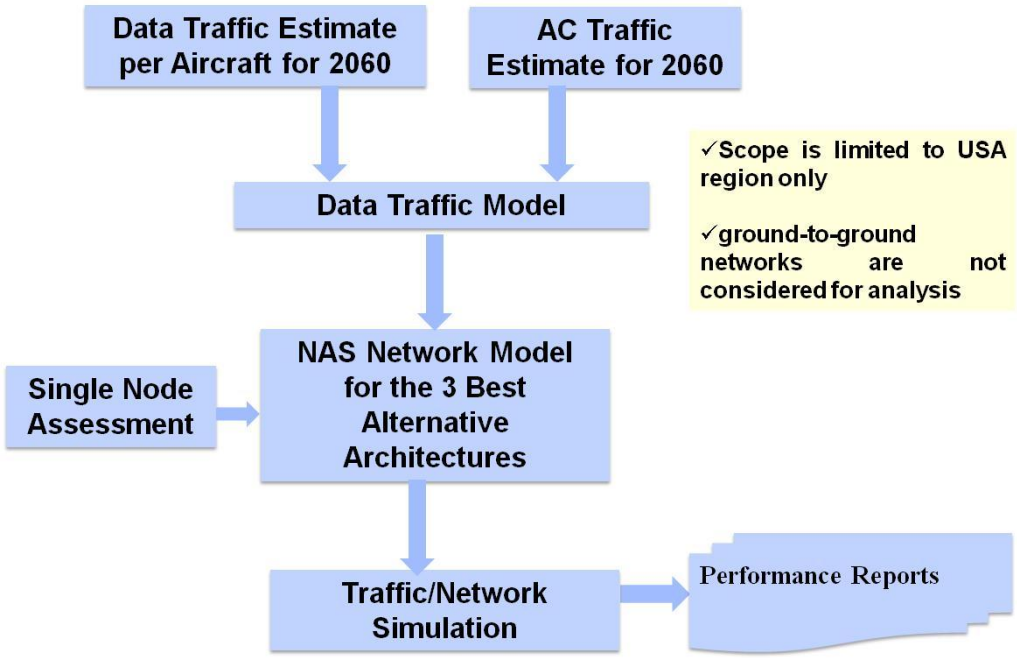


Figure 4-5 Simulation Model

4.2.2. Scope of Simulation

The scope of the simulation work is limited to the following:

- Air traffic across the Continental United States (CONUS) will be simulated.
- The best alternative technologies and architectures that were selected in the Architecture Analysis report [REF-TASK3RPT] are modeled for analysis.
- The simulation is limited to the macro level traffic generation based on the rates as estimated in section 4.1 on operational scenarios. The simulation is not intended to create actual message transfers across the layers of protocols and end applications.
- The ground network and ground systems are considered as a single cloud entity that sinks the downlink data traffic. Constant delays are accounted in the delay model for these entities. Internal network elements are not simulated.

4.2.3. Air Traffic Model

Figure 4-6 shows the steps in calculating aircraft traffic. The air traffic forecasting model requires information about current air traffic across the CONUS. Honeywell Global Data Center (GDC) has the capability to monitor air traffic across the globe in real time. The current air traffic information called Aircraft Situation Display to Industry (ASDI) is provided by the Federal Aviation Administration (FAA) to industry. The data obtained from the GDC database includes the location, altitude, airspeed, destination, estimated time-of-arrival and designated identifier of air carrier. The air traffic considered in the simulation model is based on the air traffic records on 23rd January 2014. Figure 4-7 (a) shows the sample air traffic ASDI table.

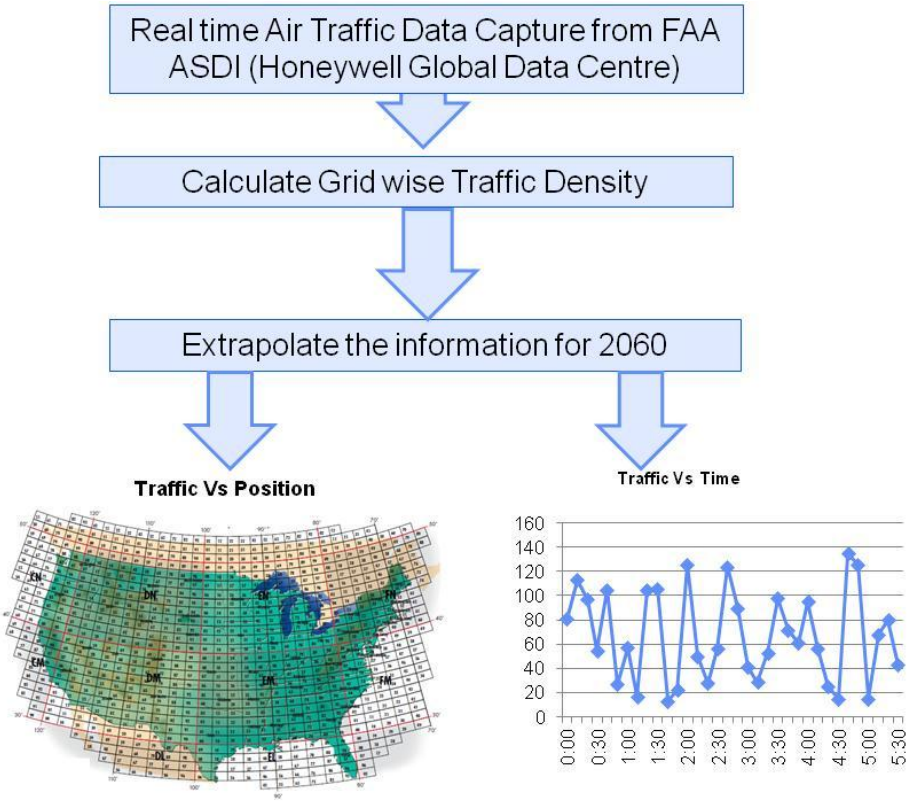


Figure 4-6 Aircraft Traffic Calculation

4.2.3.1. EXTRAPOLATION OF AIR TRAFFIC

The COCR document [REF-COCR] predicts a growth of 2.5% increase in the Peak Instantaneous Aircraft Count for every year. However a more recent report from the FAA [REF-FAA2033] predicts the U.S. mainline air carrier passenger jet fleet will increase at 0.5% for every year over the period 2013-2033. An average growth of 0.5% YOY is applied over the captured air traffic information to arrive at the air traffic estimates in 2060. New rows are added in the current ASDI table assigning arbitrary call signs to the newly added aircraft, as shown in the Figure 4-7 (b). The number of newly added rows is based on the air traffic growth considered and is configurable by the simulation user from the Graphical User Interface (GUI) front end.

recorded_at	seq	callsign	speed	assigned_a	latitude	longitude	sourcetimestamp
1/23/2014 6:00	1	ASA129	400	380	56.8833	-133.3	1/23/2014 5:54
1/23/2014 6:00	2	JZA425	160	8	49.1667	-123.117	1/23/2014 5:54
1/23/2014 6:00	3	WJA496	400	410	50.9667	-119.017	1/23/2014 5:54
1/23/2014 6:00	4	QXE580	340	230	51.8	-117.883	1/23/2014 5:54
1/23/2014 6:00	5	BXH454	190	126	50.0167	-111.183	1/23/2014 5:54
1/23/2014 6:00	6	UAL460	300	115	48.7167	-122.567	1/23/2014 5:54
1/23/2014 6:00	1	GTX653	176	45	30.8942	-97.3897	1/23/2014 5:54
1/23/2014 6:00	2	N616MB	169	74	36.3494	-100.363	1/23/2014 5:54
1/23/2014 6:00	3	EMD29	116	11	32.7889	-97.3558	1/23/2014 5:54
1/23/2014 6:00	4	AAL2497	394	280C	34.5281	-103.921	1/23/2014 5:54
1/23/2014 6:00	5	MRA224	191	110C	31.6414	-99.1217	1/23/2014 5:54
1/23/2014 6:00	7	ACA255	240	42	49.1333	-122.833	1/23/2014 5:54
1/23/2014 6:00	6	DYA1101	240	050T	15.2	146	1/23/2014 5:54
1/23/2014 6:00	1	ASQ5860	200	17	45.5167	-73.6667	1/23/2014 5:54
1/23/2014 6:00	8	CJT572	450	350	48.3667	-112.8	1/23/2014 5:54
1/23/2014 6:00	1	JZA7784	230	82	43.7833	-79.6167	1/23/2014 5:54
1/23/2014 6:00	9	JZA238	220	200	53.7333	-128.117	1/23/2014 5:54
1/23/2014 6:00	2	USC800	165	070C	26.8419	-81.0169	1/23/2014 5:54
1/23/2014 6:00	3	LN990LC	331	159	26.0122	-79.8414	1/23/2014 5:54
1/23/2014 6:00	4	AAL2232	477	370C	29.5394	-78.7975	1/23/2014 5:54
1/23/2014 6:00	5	AWE800	502	390C	21.7864	-69.0075	1/23/2014 5:54
1/23/2014 6:00	6	AAL991	489	330C	20.5317	-73.5761	1/23/2014 5:54
1/23/2014 6:00	1	EGF3477	371	360C	32.6603	-109.934	1/23/2014 5:54
1/23/2014 6:00	2	SQC7971	543	390C	34.7919	-112.086	1/23/2014 5:54
1/23/2014 6:00	3	NKS199	350	339C	31.3419	-103.295	1/23/2014 5:54
1/23/2014 6:00	4	DAL2355	392	340C	35.0719	-106.14	1/23/2014 5:54
1/23/2014 6:00	5	SWA4832	135	11	33.4303	-112.024	1/23/2014 5:54
1/23/2014 6:00	6	NKS339	316	339C	34.1667	-102.59	1/23/2014 5:54
1/23/2014 6:00	7	ASQ4185	394	206	32.0419	-105.682	1/23/2014 5:54

(a)

recorded_at	seq	callsign	speed	assigned_a	latitude	longitude	sourcetimestamp
1/23/2014 6:00	1	ASA129	400	380	56.8833	-133.3	1/23/2014 5:54
1/23/2014 6:00	2	JZA425	160	8	49.1667	-123.117	1/23/2014 5:54
1/23/2014 6:00	3	WJA496	400	410	50.9667	-119.017	1/23/2014 5:54
1/23/2014 6:00	4	QXE580	340	230	51.8	-117.883	1/23/2014 5:54
1/23/2014 6:00	5	BXH454	190	126	50.0167	-111.183	1/23/2014 5:54
1/23/2014 6:00	6	UAL460	300	115	48.7167	-122.567	1/23/2014 5:54
1/23/2014 6:00	1	GTX653	176	45	30.8942	-97.3897	1/23/2014 5:54
1/23/2014 6:00	2	N616MB	169	74	36.3494	-100.363	1/23/2014 5:54
1/23/2014 6:00	3	EMD29	116	11	32.7889	-97.3558	1/23/2014 5:54
1/23/2014 6:00	4	AAL2497	394	280C	34.5281	-103.921	1/23/2014 5:54
1/23/2014 6:00	5	MRA224	191	110C	31.6414	-99.1217	1/23/2014 5:54
1/23/2014 6:00	7	ACA255	240	42	49.1333	-122.833	1/23/2014 5:54
1/23/2014 6:00	6	DYA1101	240	050T	15.2	146	1/23/2014 5:54
1/23/2014 6:00	1	ASQ5860	200	17	45.5167	-73.6667	1/23/2014 5:54
1/23/2014 6:00	8	CJT572	450	350	48.3667	-112.8	1/23/2014 5:54
1/23/2014 6:00	1	JZA7784	230	82	43.7833	-79.6167	1/23/2014 5:54
1/23/2014 6:00	9	JZA238	220	200	53.7333	-128.117	1/23/2014 5:54
1/23/2014 6:00	2	USC800	165	070C	26.8419	-81.0169	1/23/2014 5:54
1/23/2014 6:02	6	UAL460	300	115	48.7167	-122.567	1/23/2014 5:56
1/23/2014 6:00	3	LN990LC	331	159	26.0122	-79.8414	1/23/2014 5:54
1/23/2014 6:00	4	AAL2232	477	370C	29.5394	-78.7975	1/23/2014 5:54
1/23/2014 6:00	5	AWE800	502	390C	21.7864	-69.0075	1/23/2014 5:54
1/23/2014 6:00	6	AAL991	489	330C	20.5317	-73.5761	1/23/2014 5:54
1/23/2014 6:00	1	EGF3477	371	360C	32.6603	-109.934	1/23/2014 5:54
1/23/2014 6:00	2	SQC7971	543	390C	34.7919	-112.086	1/23/2014 5:54
1/23/2014 6:00	3	NKS199	350	339C	31.3419	-103.295	1/23/2014 5:54
1/23/2014 6:00	4	DAL2355	392	340C	35.0719	-106.14	1/23/2014 5:54
1/23/2014 6:00	5	SWA4832	135	11	33.4303	-112.024	1/23/2014 5:54
1/23/2014 6:00	6	NKS339	316	339C	34.1667	-102.59	1/23/2014 5:54
1/23/2014 6:00	7	ASQ4185	394	206	32.0419	-105.682	1/23/2014 5:54

(b)

Figure 4-7 Current Schedule Vs Extrapolated Schedule with Growth

4.2.3.2. UAS TRAFFIC ADDITION IN SIMULATION MODEL

The future use of UAS is expected to become more prominent in all the three major market segments: military, civilian and commercial. However, the current ASDI data does not have UAS traffic information. Hence, UAS traffic is added to the simulation model over the entire CONUS region, based on the human population. The urban areas and major cities in the CONUS (up to 250) are ranked according to population. The most populous city is assigned with a configurable UAS aircraft and the UAS in the remaining cities are derived based on the UAS in the most populous city, as shown in Figure 4-8.

Rank	City	2010 Census	UAVs (based on poupulation
1	*New York*	8,175,133	100
2	Los Angeles	3,792,621	47
3	Chicago	2,695,598	33
4	*Houston*	2,100,263	26
5	*Philadelphia*	1,526,006	19
6	Phoenix	1,445,632	18
7	San Antonio	1,327,407	17
8	San Diego	1,307,402	16
9	Dallas	1,197,816	15
10	San Jose	945,942	12
11	Austin	790,390	10
12	*Jacksonville*	821,784	11
13	***Indianapolis***	820,445	11
14	San Francisco	805,235	10
15	Columbus	787,033	10
16	Fort Worth	741,206	10
17	Charlotte	731,424	9
18	Detroit	713,777	9
19	El Paso	649,121	8
20	Memphis	646,889	8
21	Boston	617,594	8
22	Seattle	608,660	8
23	***Denver***	600,158	8
24	***Washington*** [13]	601,723	8

Figure 4-8 UAS Traffic Estimate

4.2.4. Data Traffic Model

The data traffic estimates are provided in section 4.1 for the different categories of services that will be supported by the network: ATS, AOC, AAC, APC and SWIM. For ATS and AOC services,

the estimate is based on those services that are defined in the COCR. The AAC services estimate is assumed to be equal to that of the AOC estimate. For APC services, the traffic that is generated by a single passenger is characterized statistically. This traffic per passenger is then scaled according to the number of passengers in different kinds of aircraft in order to estimate the total amount of APC traffic that is generated on board an aircraft. Table 4-9 is based on the data traffic estimates arrived in the section 4.1.3.6 and is used to generate the data traffic in the network simulation.

Table 4-9 Data Traffic Estimates (kbps) – 2060 Timeframe

Estimated Traffic 2060 in kbps	ATC	AOC	AAC	SWIM	APC
ATR	100	100	100	2,000	90,000
Microjet	100	100	100	2,000	18,000
BGA	100	100	100	2,000	65,000
UAV	100	700	0	0	5,000

4.2.5. Queuing Model

The data traffic packets from each of the aircraft within the service volume of the access network tower are divided into 5 priority classes as ATC, AOC, AAC, SWIM, and APC. ATC is Class 1 highest priority, AOC is class 2 second highest priority, up to APC as class 5, which is the lowest priority class. Different classes of traffic have different Quality of Service (QOS) requirements. Hence the aircraft network is considered as an M/M/1 system with separate queues for packets with different priority classes, as shown in Figure 4-9.

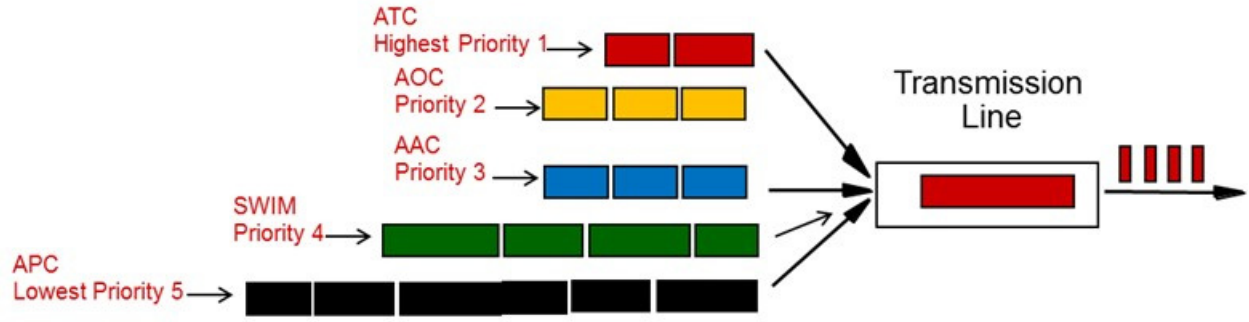


Figure 4-9 Priority Queuing

In this Priority Queue model, the packets of lower priority start transmission only if no higher priority packet is waiting. The service rate of the channel 'μ' is assumed to be the same for different classes. With the arrival rates of different classes given as λ1, . . . λk, the mean results for latency in the queue , system latency and loss probability are derived.

The average queuing delay of the k^{th} class is given by Equation 4-1 [REF- QUEUES].

$$W^k_q = \sum^k_{j=1}(\rho_j/ \mu_j) / ((1- \rho_1 - \rho_2 - \rho_3 - \ldots - \rho_k)* (1- \rho_1 - \rho_2 - \rho_3 - \ldots - \rho_{k-1})) \quad \textbf{Equation 4-1}$$

where $\rho_k = \lambda_k / \mu_k$; is the fraction of time allocated by server to class k.

The system latency for a given packet is defined as the total time period a tagged packet spends in the system, i.e., the number of time slots between the end of the packet's arrival slot and the end of its departure slot. The average system latency of the k^{th} class is given by Equation 4-2.

$$S_k = W^k_q + 1/ \mu_k \quad \textbf{Equation 4-2}$$

Table 4-10 gives the theoretical latency calculations for different traffic classes over a single cell channel.

Table 4-10 Priority Queue Latency Example

Incoming rate		ATC	AOC	AAC	SWIM	APC	Total
λ per ATR AC (Kbps)		100	100	100	2,000	90,000	
λ per BGA AC (Kbps)		100	100	100	2,000	65,000	
λ per MJET AC (Kbps)		100	200	200	2,000	1,8000	
λ per UAV AC (Kbps)		100	700	0	0	5,000	
λ per CARGO AC (Kbps)		100	100	100	2,000	0	
Total λ actual (Kbps)		1,000	1,000	1,000	20,000	900,000	923,000
Available Ch Capacity (Kbps)		1,000,000	999,000	99,8000	997,000	977,000	
Max. Ch Capacity K (packets/sec)		1,250,000	1,248,750	1,247,500	1,246,250	1,221,250	
$\lambda_{packet/sec}$		1,250	1,250	1,250	25,000	1,125,000	1,153,750
$\mu_{packet/sec}$		1,262,626.26	1,262,626.26	1,262,626.26	1,262,626.263	1,262,626.263	1,262,626
ρ		0.00099	0.00099	0.00099	0.0198	0.891	0.91377
W_{Q} (micro sec)		0.000785	0.001573	0.002364	0.018509	8.588294	
$W_{s(micro\ sec)}$		0.792785	0.793573	0.794364	0.810509	9.380294	
W_{s} (micro sec) percentile	90	1.826	1.828	1.829	1.867	21.603	
	95	2.375	2.378	2.380	2.428	28.103	

4.2.5.1. PREEMPTION SCENARIO

Figure 4-10 shows how the different classes of packets are prioritized and sent over the channel. The highest priority packets (darker shade, red in color, no diagonal lines, as shown in Figure 4-10) preempt the lower priority packets (lighter shade, gold, no diagonal lines, and darker shade, green in color, with diagonal lines as shown in the figure) and are transmitted prior to the lower priority packets.

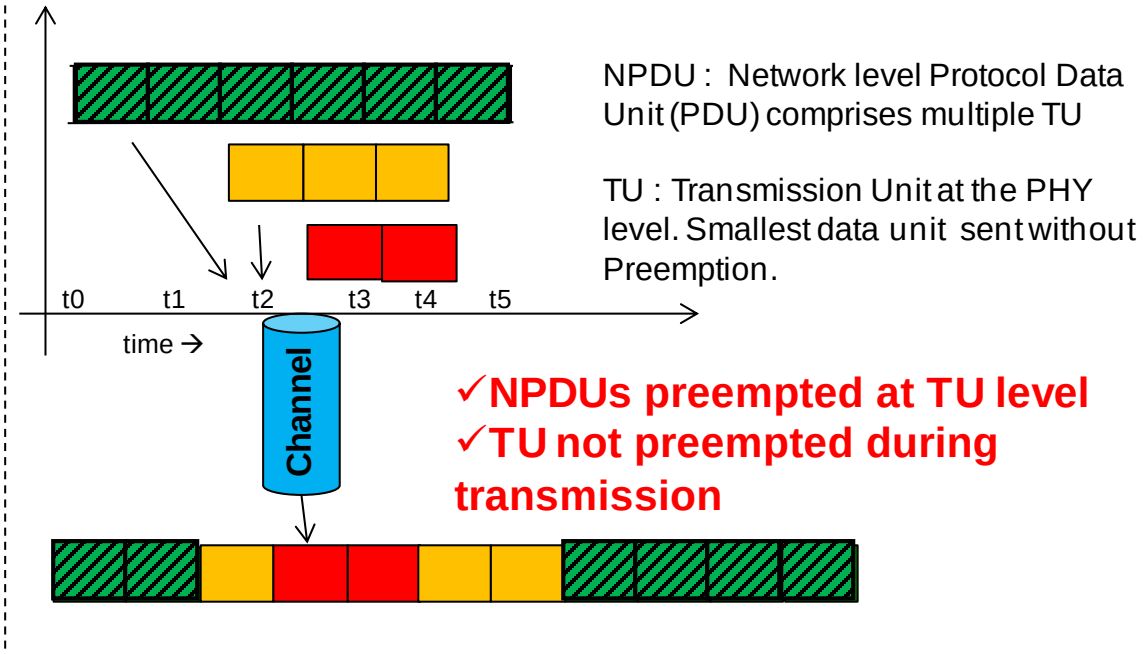


Figure 4-10 Packet Preemption

4.2.6. Network Models

The network modeling and simulation is carried out for the networks and combination of networks that were identified in the NASA CDTI Project Phase 1 reports. Air/-Ground Network models are developed based on the selected technologies and platforms such as Cellular ground towers, HAP and GEO satellites for the operational assessment of future NAS environment. Air-to-Air Network model is developed and load analysis is carried out for the NAS environment considering VHF, FSO and L-band for the air-to-air communication link.

4.2.6.1. GROUND-BASED CELLULAR NETWORK MODEL AND SIMULATION

In the cellular network architecture it is assumed that the ground base stations distributed across the entire CONUS region provide connectivity to the ground network for all the aircraft flying over the CONUS region. The coverage of the CONUS region by cellular towers, each tower represented as covering one hexagonal grid area is shown in the Figure 4-11.

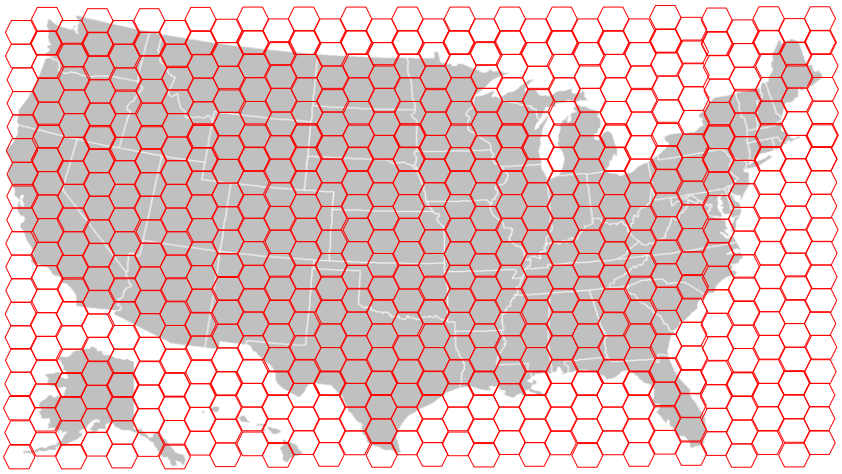


Figure 4-11 Hexagonal Grid Cellular Coverage

4.2.6.1.1. Single Cell Service Volume

Figure 4-12 shows the service volume for a single cell tower with hexagonal grid coverage. The aircraft flying over a particular hexagonal grid is assumed to be serviced by the tower in that grid.

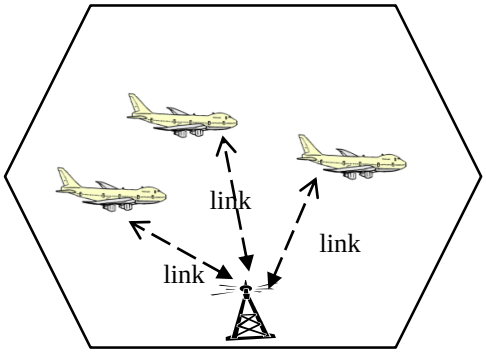


Figure 4-12 Single Cell Service Volume

4.2.6.1.2. Cellular Tower Simulation Model

Figure 4–12 shows the network model considered for communication performance analysis using air/round cellular data links. It is broadly divided into three networks viz. airborne network (NW), commercial (communication service provider) network and aeronautical ground network. The airborne network comprises of the aircraft that are communicating with their respective cellular base station towers for both the cabin and cockpit services through the same data link. For a single cellular ground tower, the airborne network service coverage range is assumed to be approximately 100 Nm. All the aircraft within the service coverage of the tower communicate directly with the tower, which offers a total bandwidth up to 1Gbps.

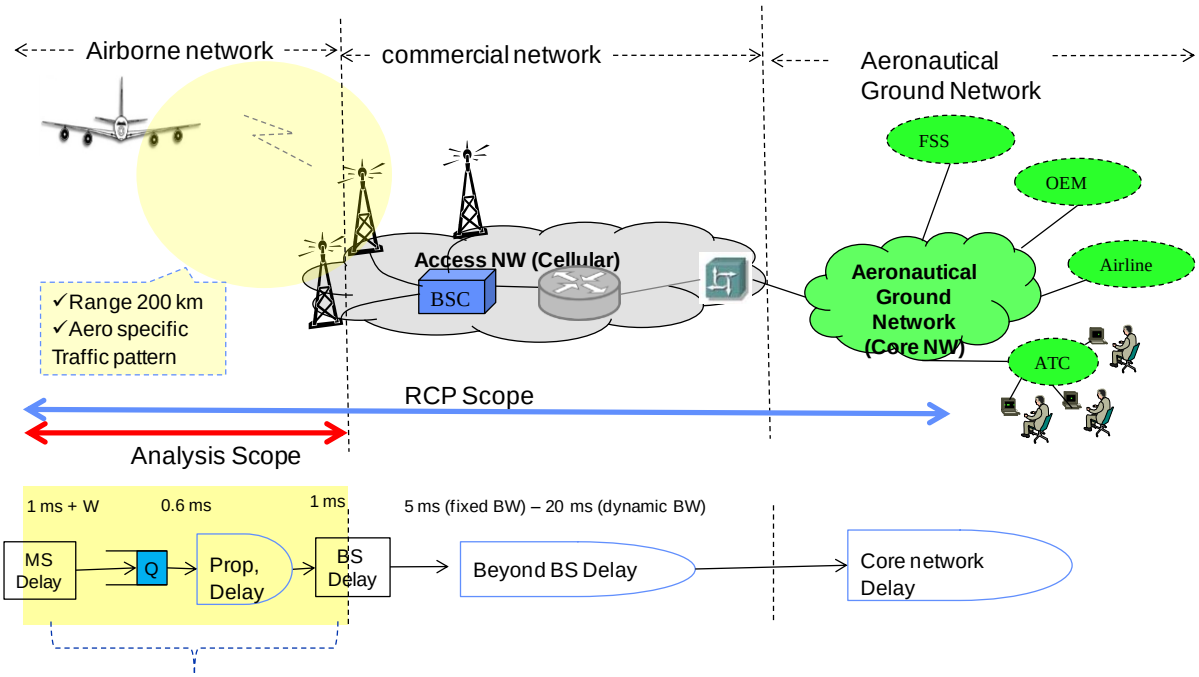


Figure 4-13 Cellular Network Model

The commercial network comprises of different network elements like base station controller, cellular gateways, routers and other network elements, etc., that provide communication between aircraft and the core aeronautical ground network. The commercial network could be a shared network, the infrastructure and the spectrum of which could be shared to offer the different services (aeronautical specific and other mobile communications services). However, the cellular network service provider may lease dedicated spectrum carriers for aeronautical specific services, to satisfy the specifications of Required Communications Performance needed for NextGen ATM applications. The mobility framework within the commercial cellular network is expected to seamlessly support both vertical and horizontal mobility so that end-to-end communications are not interrupted by the network transitions.

The aeronautical ground network in the model represents the interconnection of various service providers such as Flight Support Service (FSS) centers, Original Equipment Manufacturer (OEM) support centers, weather information centers, ATC centers, airline operations centers, etc. ANSP gateways are interconnected in order to share information across ANSP networks. The aeronautical ground network is a common requirement for all of the technology candidates that were considered in the operation view analysis. Hence the entire ground network is treated as a single cloud for the purpose of this analysis and the details are not covered in this report.

4.2.6.1.3. Simulation Assumptions

The following are the assumptions made with respect to the cellular network model simulation.

- Pre-provisioned connections are assumed between the aircraft and the cellular tower.

- Media Access Control (MAC) Layer processing latency at aircraft and service tower is assumed to be 1 ms.
- The signal propagation latency between the aircraft and the tower is up to 0.6 ms, considering the aircraft flying at a maximum distance of 200Km from the service tower.
- The commercial network beyond the base station may introduce latency up to 5 ms in case of fixed leased bandwidth allocation and latency up to 20 ms in case of dynamic bandwidth for the aircraft services. High priority traffic (ATC, AOC, AAC, and SWIM) is assumed to have fixed bandwidth allocation with 5 ms latency and lower priority APC traffic type to have dynamic bandwidth allocations with up to 20 ms latency.
- Cellular link channel throughput assumed is 1 Gbps

4.2.6.1.4. Simulation Model

The simulation model as shown in the Figure 4-14 consists of the following modules

- Aircraft Data Traffic Generator
- Data Traffic Scheduler
- Performance Report Generator

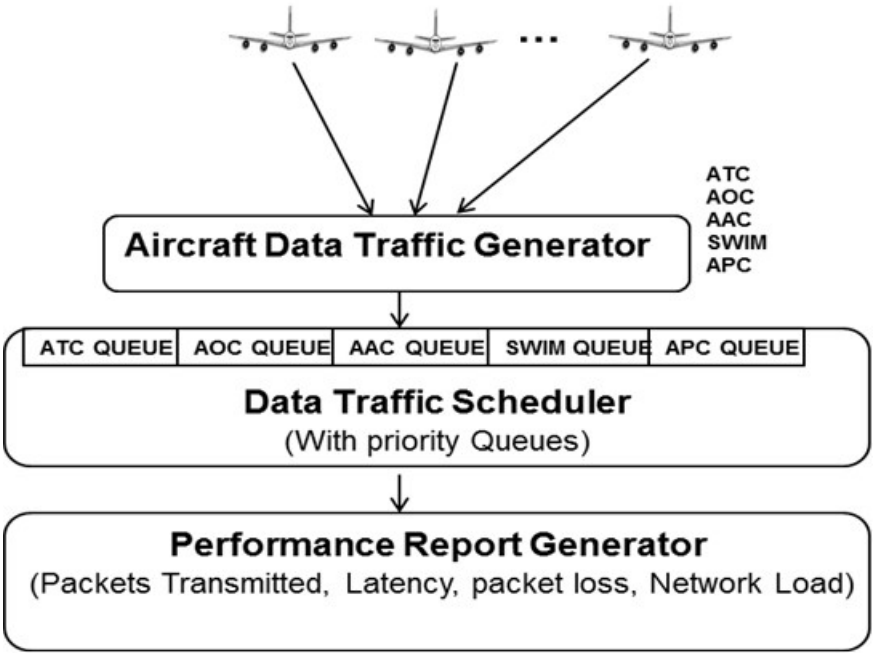


Figure 4-14 Cellular Single Tower Simulation Model

4.2.6.1.4.1. Aircraft Data Traffic Generator

This module generates all types of traffic namely, ATC, AOC, AAC SWIM and APC. Per-aircraft traffic considered in the simulation is:

- ATC - 100 Kbps, with packet size of 100 bytes

- AOC- 100 Kbps, with packet size of 500 bytes
- AAC- 100 Kbps, with packet size of 500 bytes
- SWIM- 2 Mbps, with packet size of 2000 bytes
- APC- 90 Mbps, with packet size of 2000 bytes

The packets are generated for different classes of traffic based on the estimated rates and sizes. These packets from all the aircraft are time stamped and channelized into five First In, First Out (FIFO) buffers with ATC traffic FIFO having highest schedule priority and APC traffic FIFO having lowest schedule priority. Packets are dropped if the respective FIFO is full.

This module also maintains the various statistics viz. number of packets generated, number of packets dropped and the number of packets which are scheduled for transmission.

4.2.6.1.4.2. Data Traffic Scheduler

The data traffic scheduler module simulates the packet transmissions between the aircraft and the tower based on priority queuing scheme. As shown in the Figure 4-15, at a given scheduler time instant, the highest priority packets are transmitted first and lower priority packets are scheduled only when there are no higher priority packets to be transmitted. One Transmission Unit (TU) is the smallest data unit at physical layer level that is sent without preemption and scheduler Time Sample (TS) is the time taken to transmit one TU.

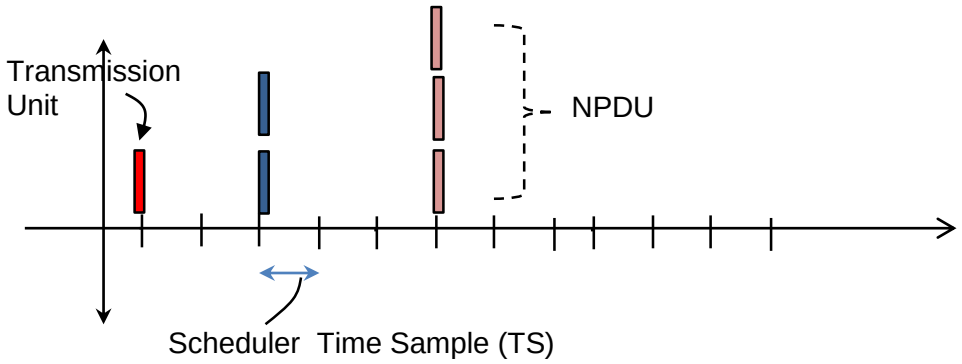


Figure 4-15 Packet Scheduling Scheme

An example calculation is provided below.

Example:

Output Channel Throughput	= 1Gbps
TU size	= 100 bytes
TS = (100 x 8)/ 1e9 sec	= 0.8 µsec

AOC data rate	= 100 kbps per aircraft
AOC packet Size	= 500 bytes.
AOC arrival interval	= (8 x 500)/(100 x 1e3)
	= 40 ms
	= 50,000 TS per aircraft

Hence on an average, for every 50,000 TS one AOC packet will be sent and one AOC NPDU contains 5 TUs.

Figure 4-16 gives the flowchart of the Data Traffic Scheduler module showing logic and processing for ATC, AOC and AAC traffic. Processing for SWIM and APC traffic (not shown) are similar, in priority order. The module checks the availability of packets in different FIFOs based on the FIFO priority and schedules a packet transmission. The packet is time stamped again at the time of transmission to calculate the queue latency for the packet.

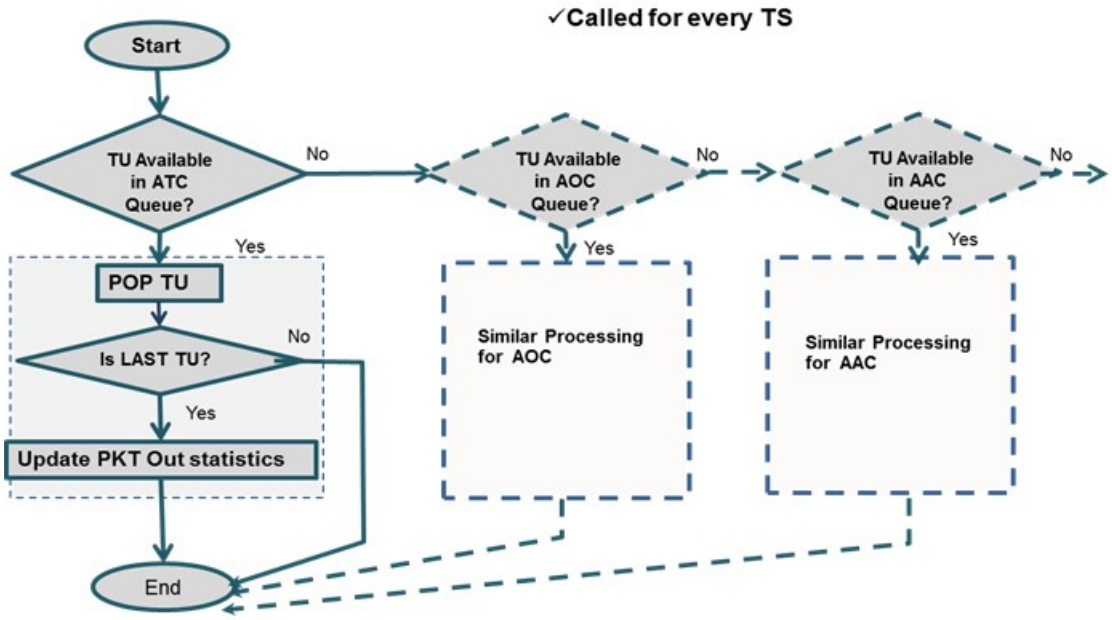


Figure 4-16 Flowchart of Data Traffic Scheduler Module

4.2.6.1.5. Performance Report Generator

This module generates reports of various network performance parameters viz. number of packets transmitted, queue latency for each packet, mean latency, network utilization for all classes of traffic simulated in the network model. The following subsections provide the network performance statistics for a single cell domain.

4.2.6.1.5.1. Latency

The overall latency of the cellular network is the summation of various delay components like MAC Layer Delay (at aircraft), propagation delay between the aircraft and the cellular tower,

queue delay and the delay inherent in the network beyond the base station (BS) delay (access network).The queue delays involved in the transmission of packets with different traffic classes on the link between the aircraft in the cell and the cellular base station are simulated. The trend in the queue latency experienced by various traffic classes as the aircraft count increases in the single cell domain is shown the Figure 4-17.

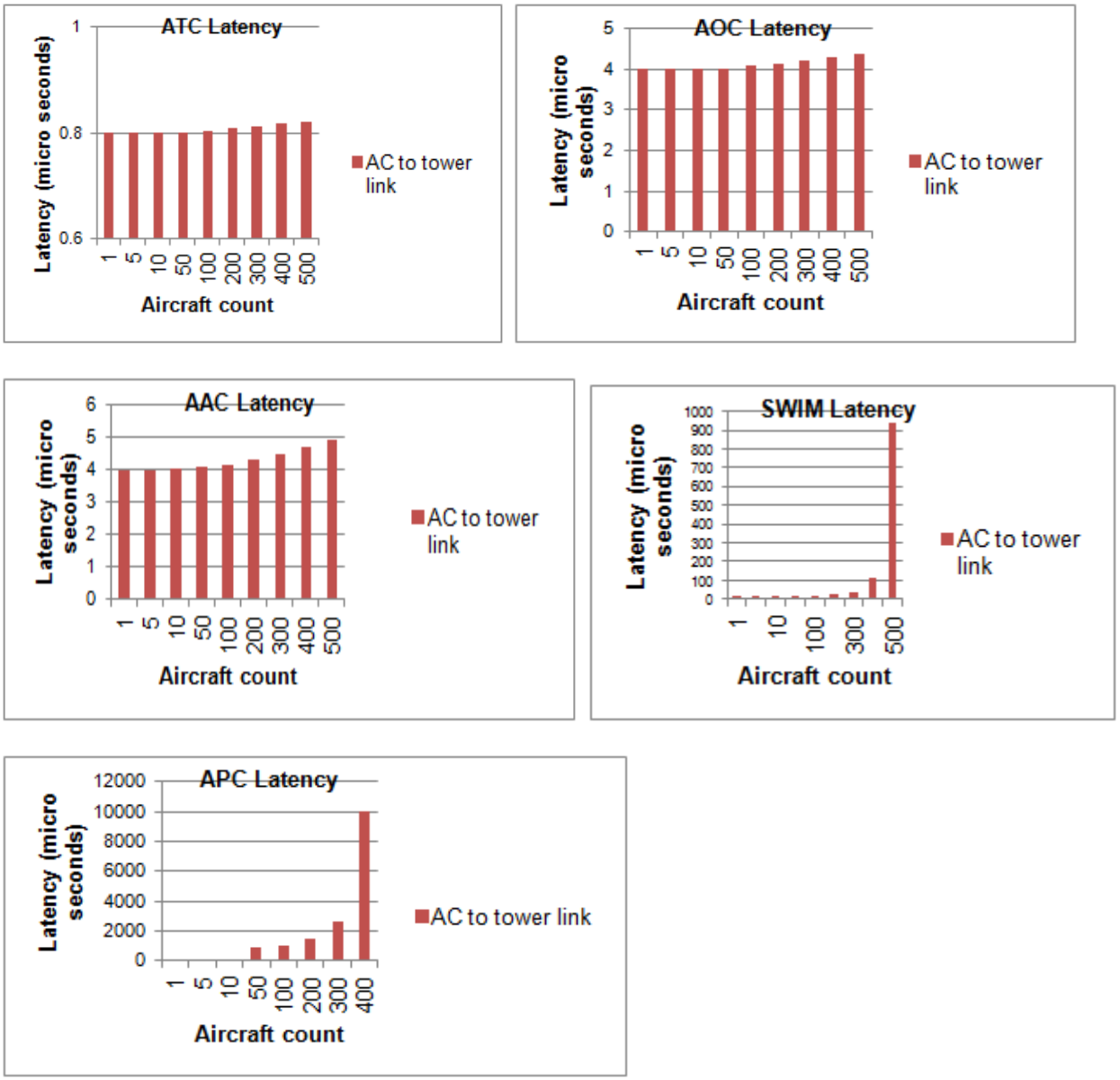


Figure 4-17 Queue Latency for Cellular Link

The overall latency of the cellular network with increasing number of aircraft in a given base station coverage for various traffic types is shown in Figure 4-18. There is no significant degradation observed in latency for supporting aircraft traffic up to 400 aircraft per cell (AC/cell). Beyond 400 AC/cell, there is no bandwidth available to transmit APC traffic. Hence beyond 400 AC/cell, the latency of APC traffic becomes noticeably greater but the latencies of higher priority traffic classes do not increase significantly.

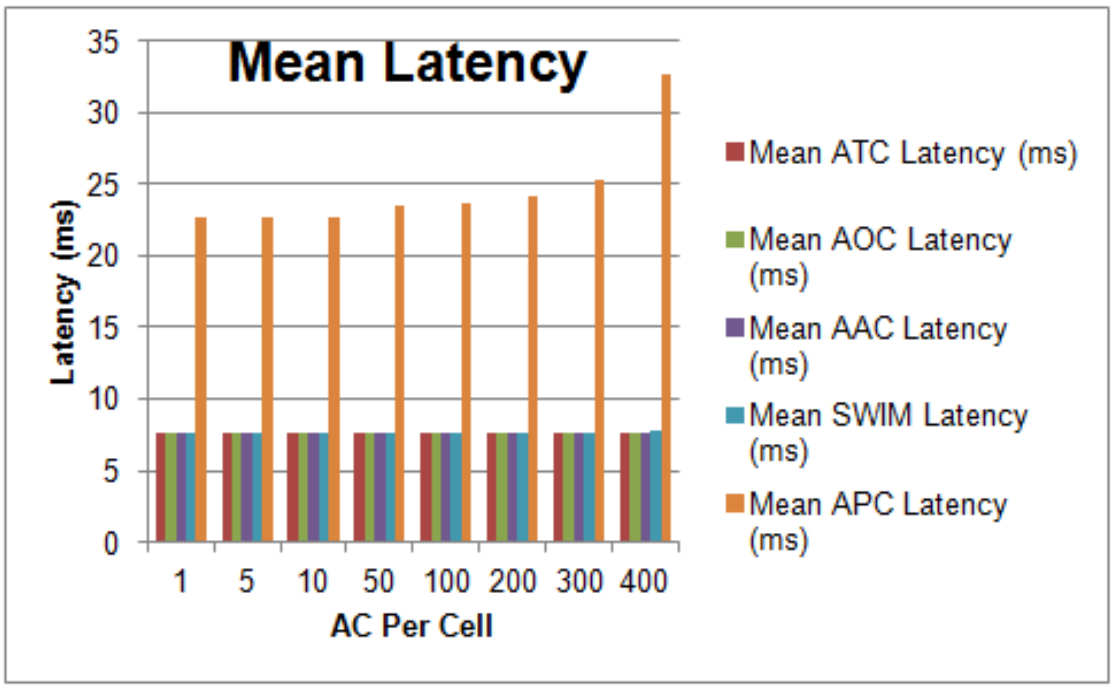


Figure 4-18 Mean Latency in Cellular Network

The measure of the various delay components in the overall latency for transmission of packets in the cellular network in the scenario of 200 AC/cell is shown in Figure 4-19.

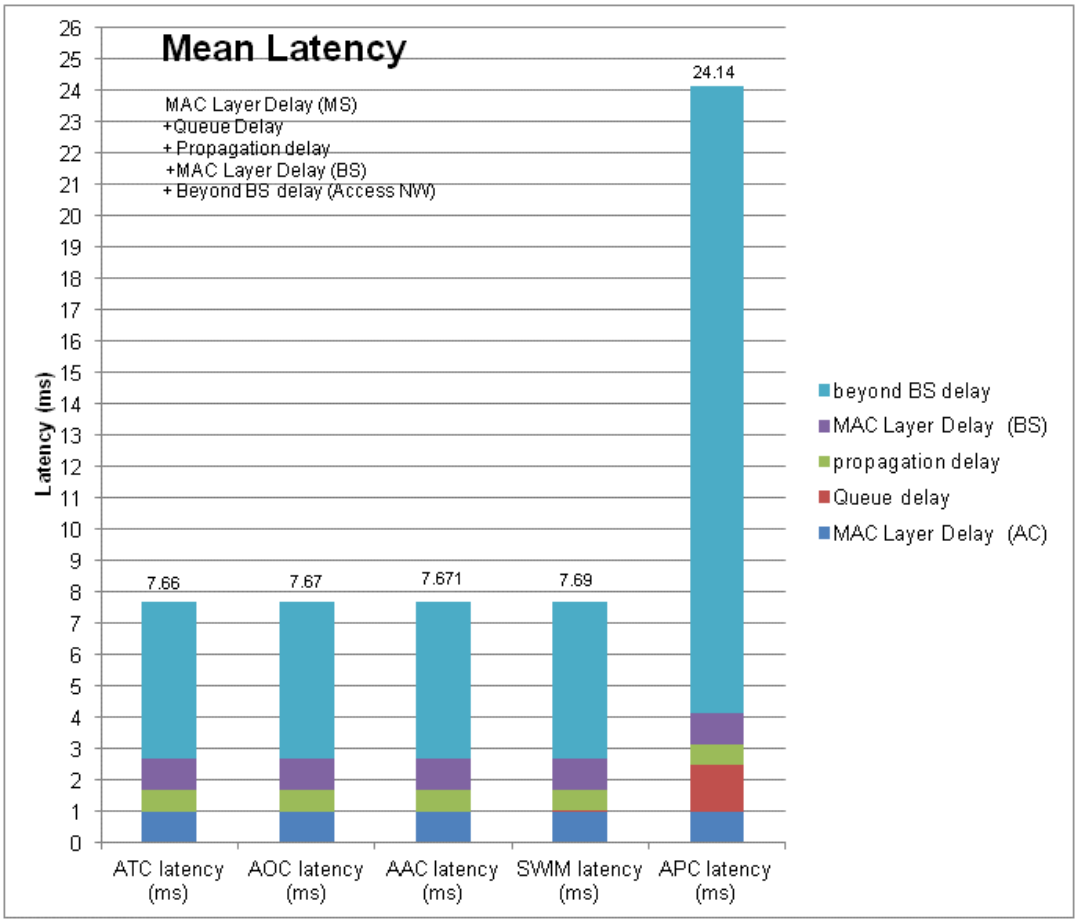


Figure 4-19 Latency Components in Cellular Network, 200 AC/Cell

4.2.6.1.5.2. Channel Bandwidth Utilization

Figure 4-20 gives the channel bandwidth utilization for different traffic classes on the link between the aircraft in the cell and the cellular base station for different aircraft density levels in the cell. As depicted in the Figure 4-20, in low dense aircraft conditions, non-safety traffic classes (AAC and APC) and SWIM will get channel share along with the safety critical traffic (ATC and AOC). However in high dense aircraft conditions, major portion of the link is used for the safety critical traffic and the non-safety traffic class may experience higher packet loss and latency.

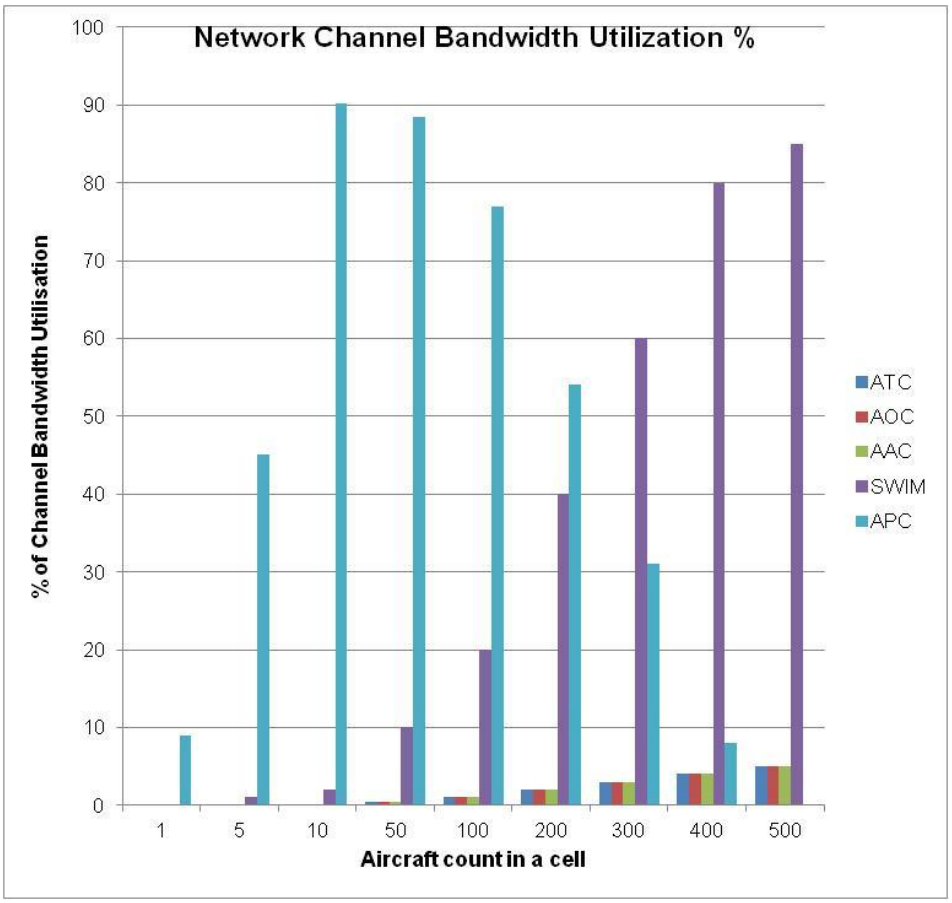


Figure 4-20 Channel Bandwidth Utilization of Cellular Link

4.2.6.1.5.3. Packet Loss (Theoretical analysis)

Figure 4-21 gives the packet loss percentage for different traffic classes on the aircraft-to-ground base station (AC ↔ BS) link for different aircraft density levels in the tower coverage area. In the simulation implementation, the packet loss was arrived considering limited buffer size in the system. The packet loss shall differ from one system to other system based on the FIFO size considered for each traffic type. Hence in theoretical analysis, no limitation in queue size is considered and, packet loss estimates loss due to channel unavailability is provided as shown in Figure 4-21. The packet loss is given by Equation 4-3.

Packet Loss % = (Arrival rate – available Channel Capacity)*100/ Arrival rate **Equation 4-3**

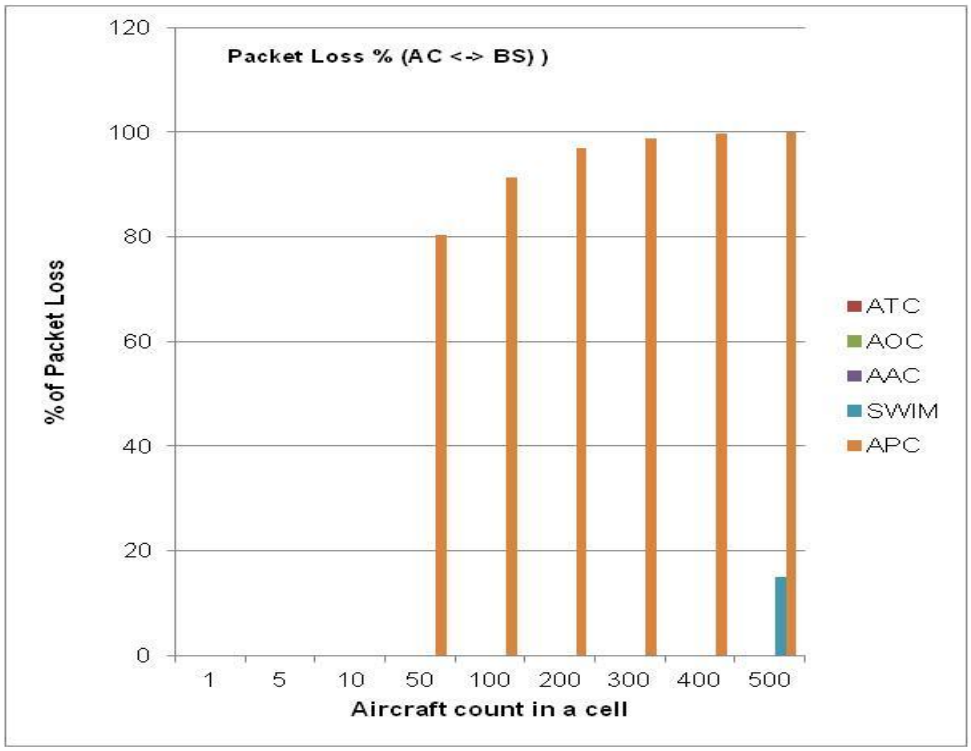


Figure 4-21 Packet Loss on Cellular Link

4.2.6.1.6. Observations and Conclusions

The following are observations and conclusions based on cellular network analysis and simulation, assuming cellular tower channel link capacity up to 1 Gbps and the tower coverage range up to 200Km.

- No significant degradation observed in latency for supporting aircraft traffic up to 400 AC/Cell. The 95th percentile latency with up to 400 AC/Cell is ATC: 22.96 ms; AOC: 22.98 ms; AAC: 22.981ms; SWIM: 23.3 ms; APC: 97.8 ms
- For 300 to 400 AC/Cell, the network should be able to support the offered load up to SWIM Services. Beyond 400 aircraft, no bandwidth will be available for low priority APC traffic.
- No Loss of safety critical traffic in the network with up to 400 AC/Cell.
- However, significant APC traffic loss will be experienced beyond 50 AC/Cell.

With adequate placement of cellular towers across the whole COUNUS region, it may be possible for aircraft to manage the entire safety critical air/ground communication.

4.2.6.2. HAP-BASED CELLULAR NETWORK MODEL AND SIMULATION

In the HAP network architecture it is assumed that multiple airborne HAP platforms optimally placed over the CONUS region together provide coverage for the aircraft flying over the whole CONUS. Each HAP platform relays traffic from the aircraft flying in its coverage region to the ground gateway station, which in turn carries the traffic to the backend aeronautical network, as

shown in Figure 4-22. The HAP platforms may also be interconnected by FSO links to offer uninterrupted communication to aircraft. In the simulation it is assumed that the each HAP platform can communicate directly to one of the ground gateway station.

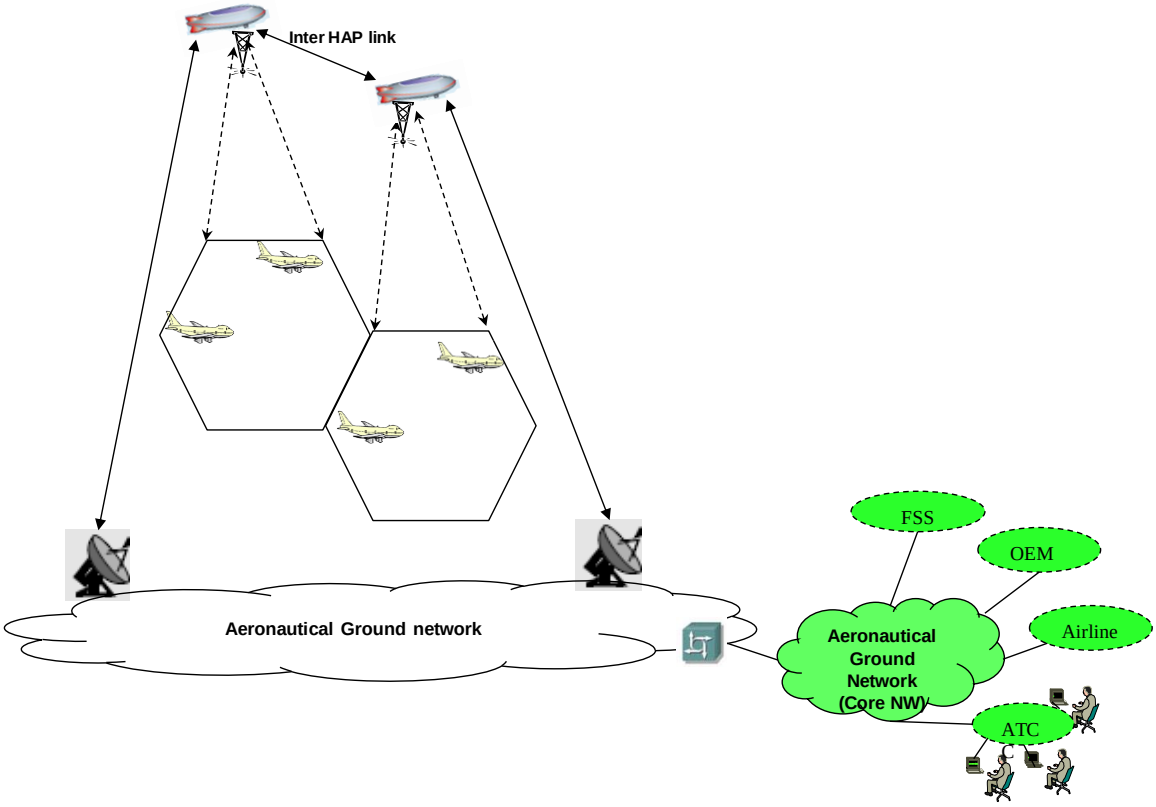


Figure 4-22 Integrated terrestrial-HAP Network

4.2.6.2.1. Single HAP Platform service volume

The coverage of an airborne HAP platform is represented as covering one hexagonal grid area as shown in Figure 4-23.

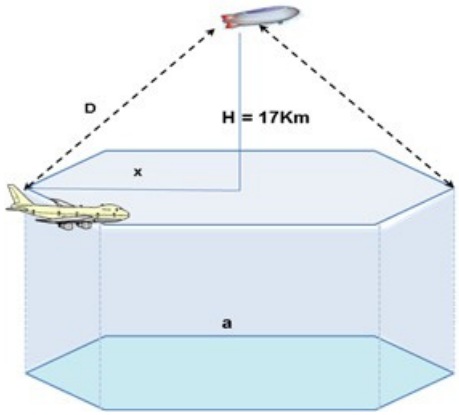


Figure 4-23 HAP Cell Service Volume

The maximum range for a HAP node can be calculated using Equation 4-4.

$$D = \sqrt{(R+H)^2 - R^2}$$ **Equation 4-4**

Where

D is the maximum range of a HAP node
R is the radius of the earth and
H is the altitude of the HAP

Considering a HAP altitude between 17 and 22 km, the maximum range of the HAP will be roughly between 465 and 530 km. With the assumption that a single HAP providing service up to 30,000 square miles, around 125 HAP platforms will provide coverage across the entire CONUS region.

4.2.6.2.2. HAP Platform Simulation Model

Figure 4-24 shows the network model considered for communication performance analysis using a HAP platform. For a single HAP, the airborne network service coverage range is assumed to be 470Km approximately. All the aircraft falling in the service coverage of the HAP communicate directly with the HAP which offers a total bandwidth up to 1Gbps, similar to Cellular link bandwidth. The data link for the communication between the HAP and ground gateway (GW) could be either a cellular link with up to 1Gbps bandwidth or could be a FSO link with up to 10Gbps bandwidth. The rest of the ground network beyond gateway i.e. the access network and the aeronautical ground network is considered to be same as that in the Cellular network simulation model.

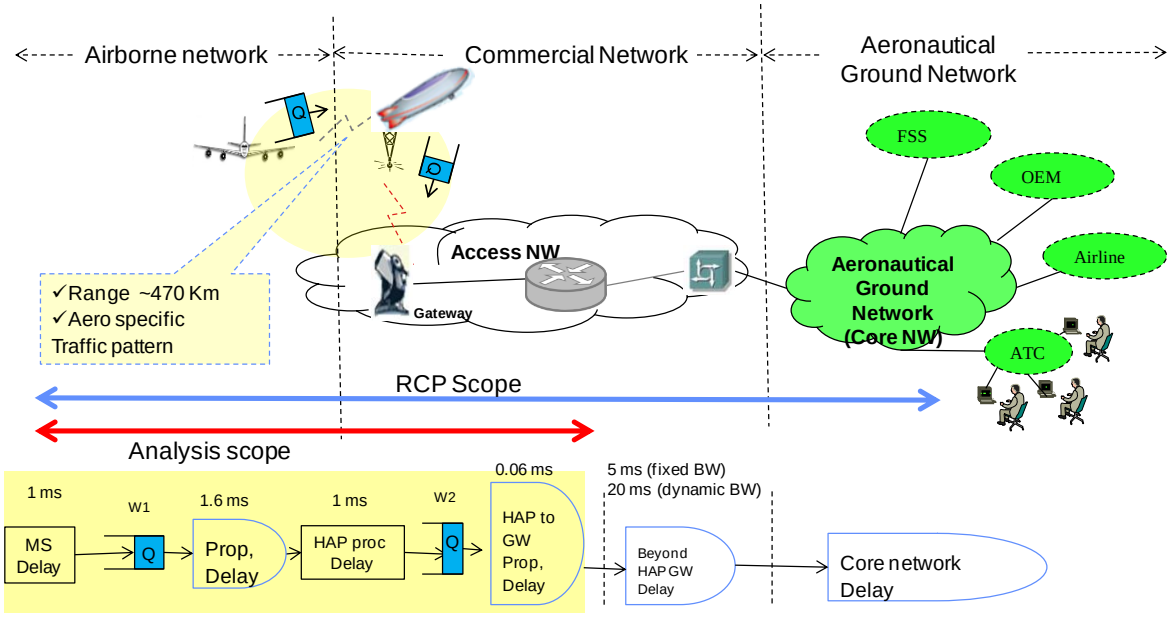


Figure 4-24 HAP Network Model

4.2.6.2.3. Simulation Assumptions

The following are the assumptions made with respect to HAP network model simulation.

- Pre-provisioned connections are assumed between the aircraft and the HAP.
- MAC Layer processing latency at aircraft and the HAP is assumed to be 1 ms
- The signal propagation latency between the aircraft and the HAP is up to 1.6 ms, considering the aircraft flying at a maximum distance of 470Km from the HAP.
- The commercial network beyond the base station may introduce latency up to 5 ms in case of fixed leased bandwidth allocation and latency up to 20 ms in case of dynamic bandwidth for the aircraft services. High priority traffic (ATC, AOC, AAC, and SWIM) is assumed to have fixed bandwidth allocation with 5 ms latency and lower priority APC traffic type to have dynamic bandwidth allocations with up to 20 ms latency.
- Aircraft-to-HAP (Aircraft ↔ HAP) link channel throughput assumed is 1 Gbps
- The feeder link between the HAP and ground gateway could be a cellular data link with 1Gbps channel throughput or it could be an FSO link with up to 10 Gbps channel throughput. Simulations are carried out for both scenarios.

4.2.6.2.4. Simulation Model

The simulation model as shown in the Figure 4-25 consists of the following modules

- Aircraft Data Traffic Generator
- Aircraft Data Traffic Scheduler
- HAP Data Traffic Scheduler
- Performance Report Generator

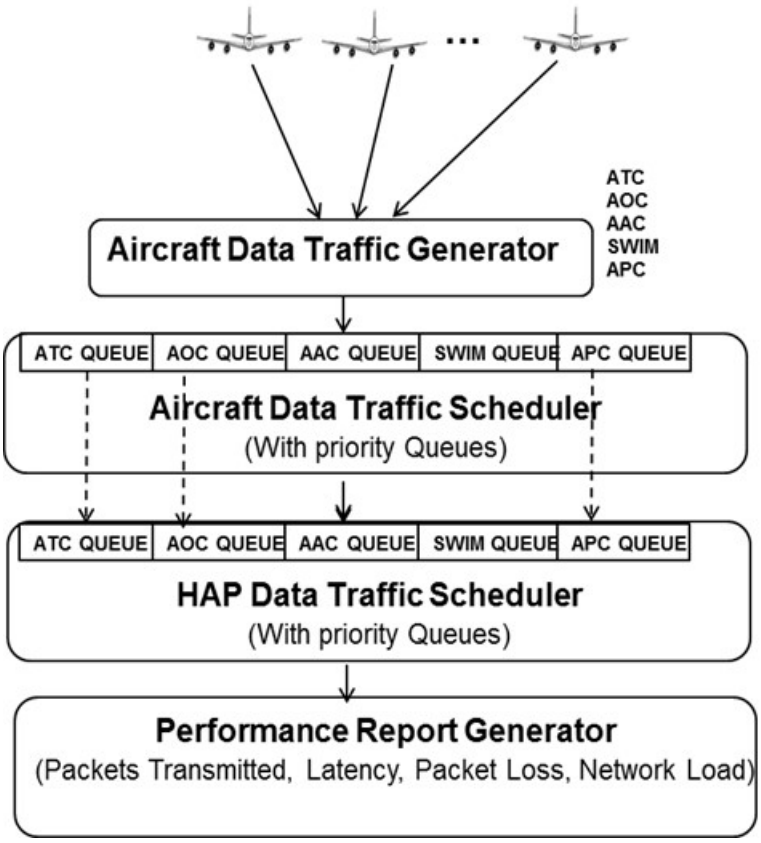


Figure 4-25 Single HAP Simulation Model

4.2.6.2.4.1. Aircraft Data Traffic Generator

The Aircraft Data Generator is the same as the one used for ground-based cellular network. Refer to section 4.2.6.1.4.1

4.2.6.2.4.2. Aircraft Data Traffic Scheduler

The Aircraft Data Traffic Scheduler is the same as the one used for ground-based cellular network. Refer to section 4.2.6.1.4.2

4.2.6.2.4.3. HAP Data Traffic Scheduler

The HAP Data Traffic Scheduler module simulates the relay of the aircraft data traffic to the ground gateway. The HAP data traffic scheduler priority scheme between HAP platform and the ground gateway is similar to that in the aircraft traffic scheduler module. The relay link between the HAP platform and the ground gateway could be a cellular data link of 1 Gbps bandwidth or it could be a FSO data link of 10 Gbps. Hence the performance analysis is carried out for these two feeder link cases.

4.2.6.2.5. Performance Report Generator

The performance report generator provides the link statistics for both links (Aircraft ↔ HAP link and HAP-to-Ground Gateway, HAP ↔ Ground Gateway, link) involved in the transmission of a packet from an aircraft to the ground gateway via the HAP platform.

4.2.6.2.5.1. Latency

The overall latency of the HAP network is the summation of various delay components like MAC layer delay (at aircraft), Aircraft Data Traffic Scheduler delay , propagation delay between the aircraft and the HAP, MAC layer delay (at HAP), propagation delay between the HAP and the ground gateway and the delay inherent in the network beyond the gateway (Access NW). The queue delay involved in transmission of packets on Aircraft ↔ HAP link and HAP ↔ Ground Gateway link is simulated. The trend in the queue latency experienced by various traffic classes as the aircraft count increases in the HAP coverage domain on the two links (Aircraft ↔ HAP link, HAP ↔ Ground Gateway link) is shown in the Figure 4-26 and Figure 4-27.

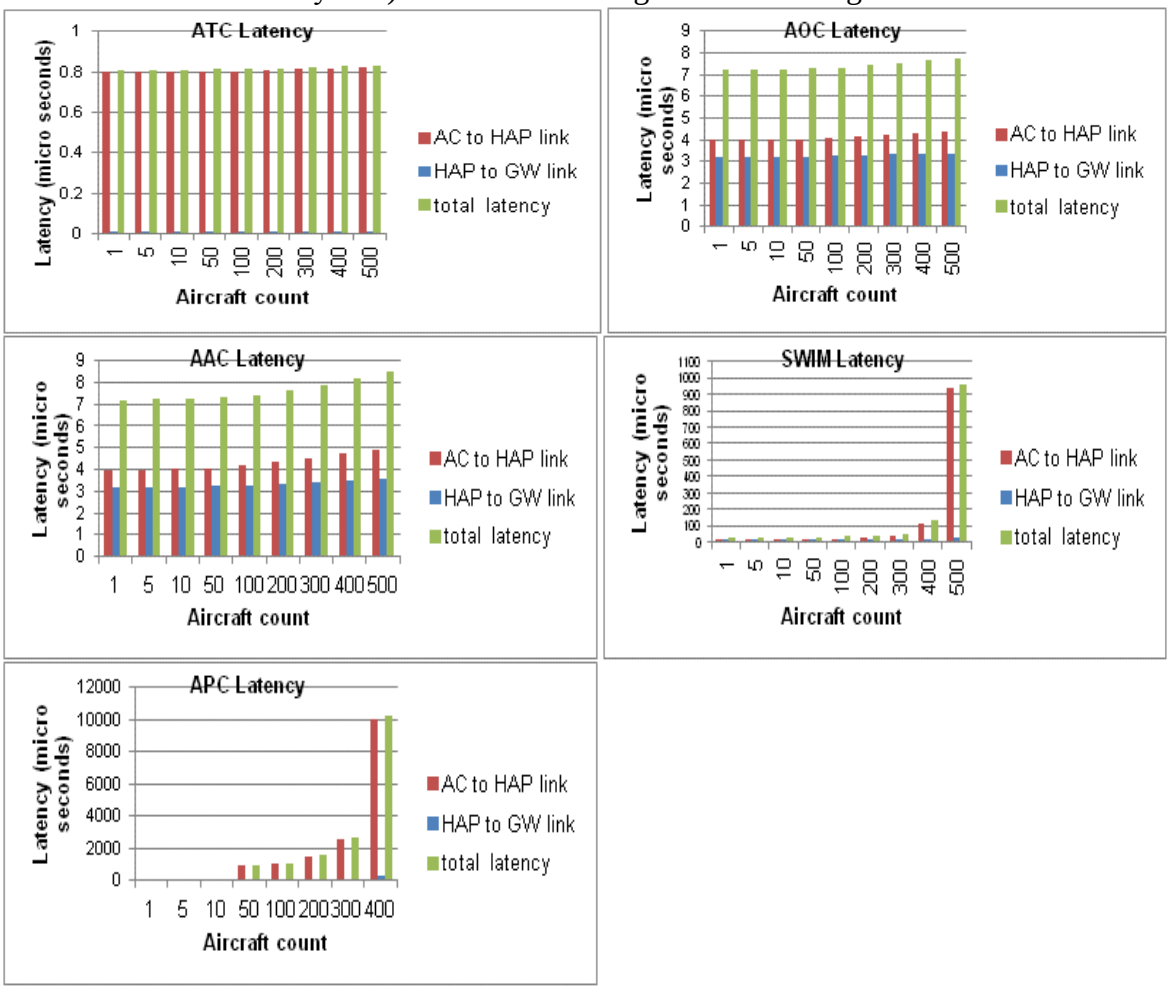


Figure 4-26 Queue Latency, Feeder Cellular Link

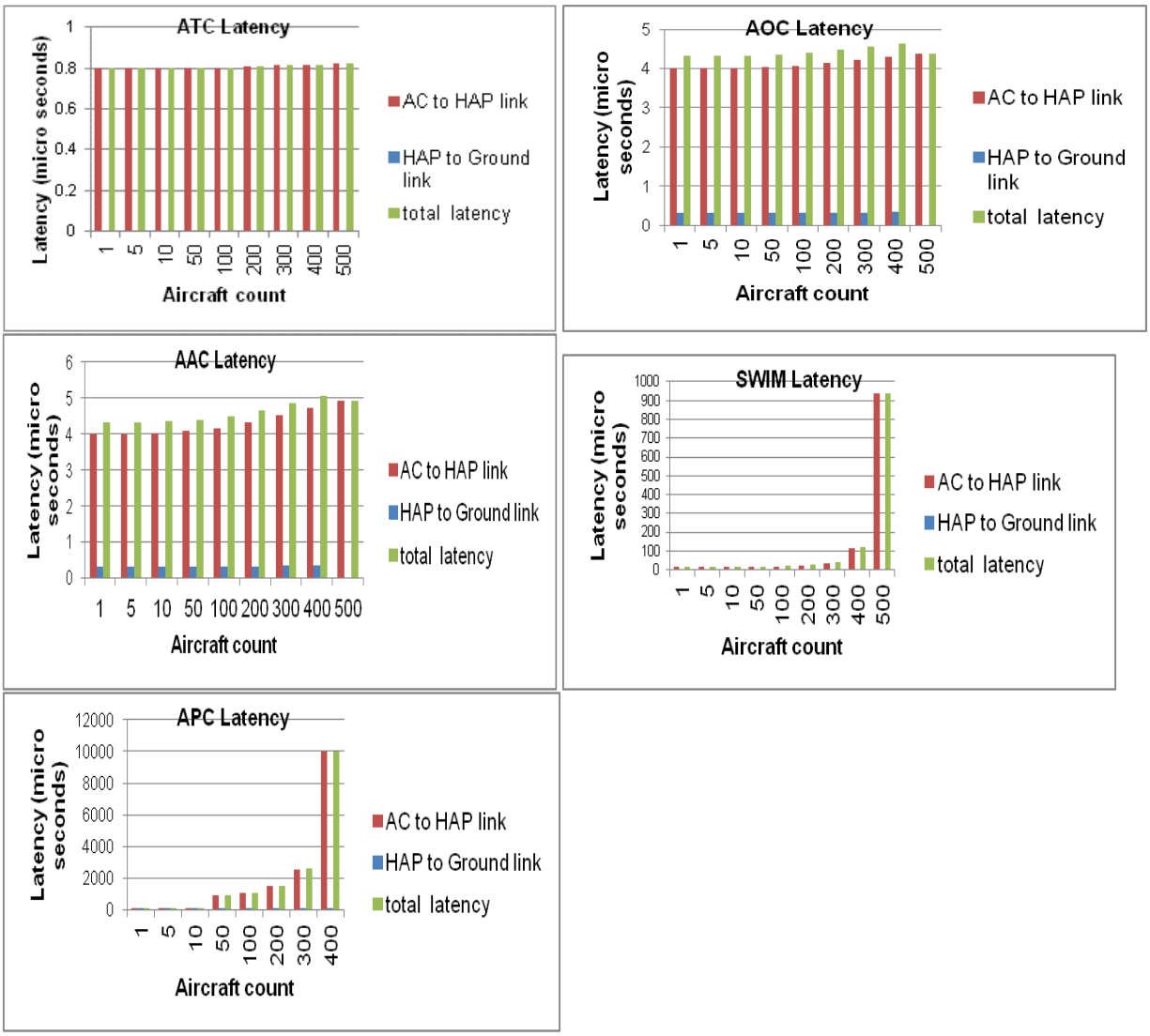


Figure 4-27 Queue Latency, Feeder FSO Link

The overall latency with increasing number of aircraft in a given HAP coverage for various traffic types is shown in Figure 4-28 and Figure 4-29.

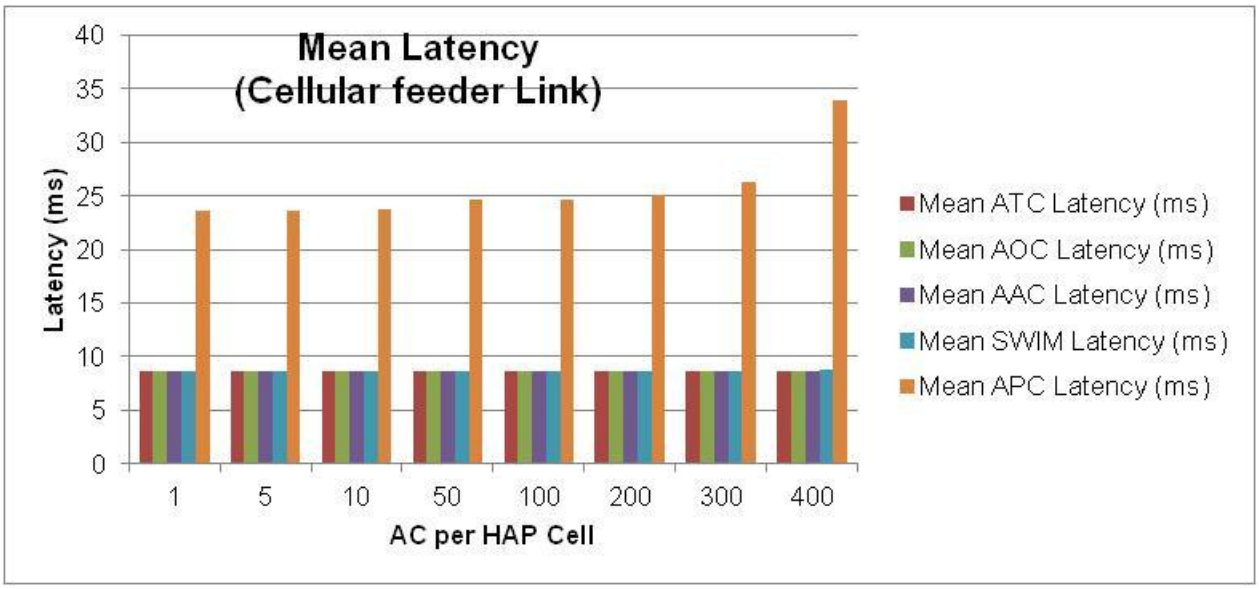


Figure 4-28 Mean Latency, Feeder Cellular Link

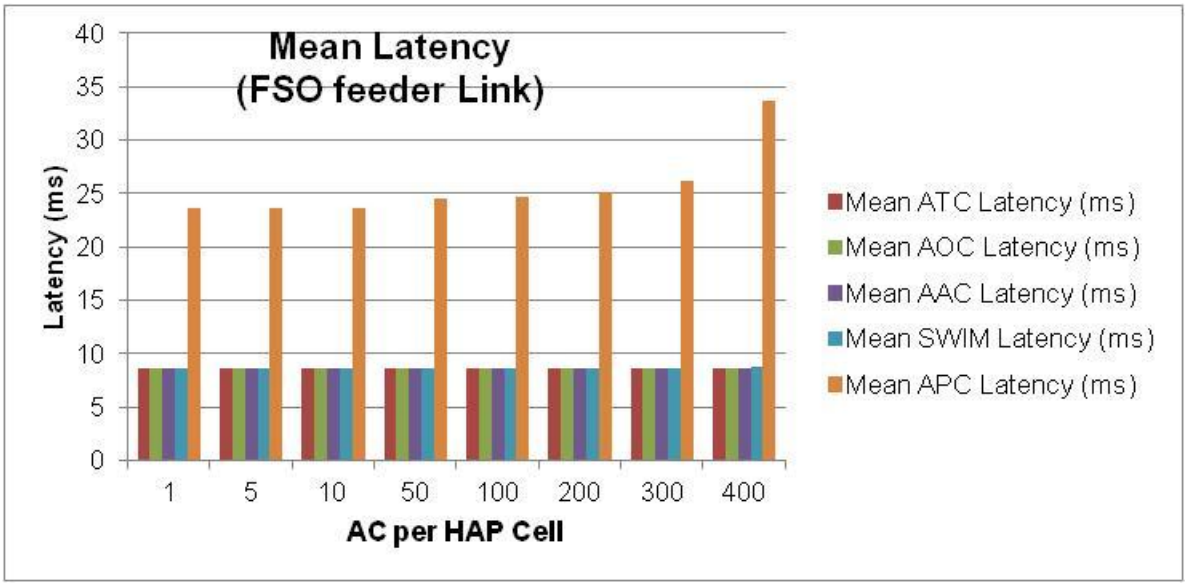
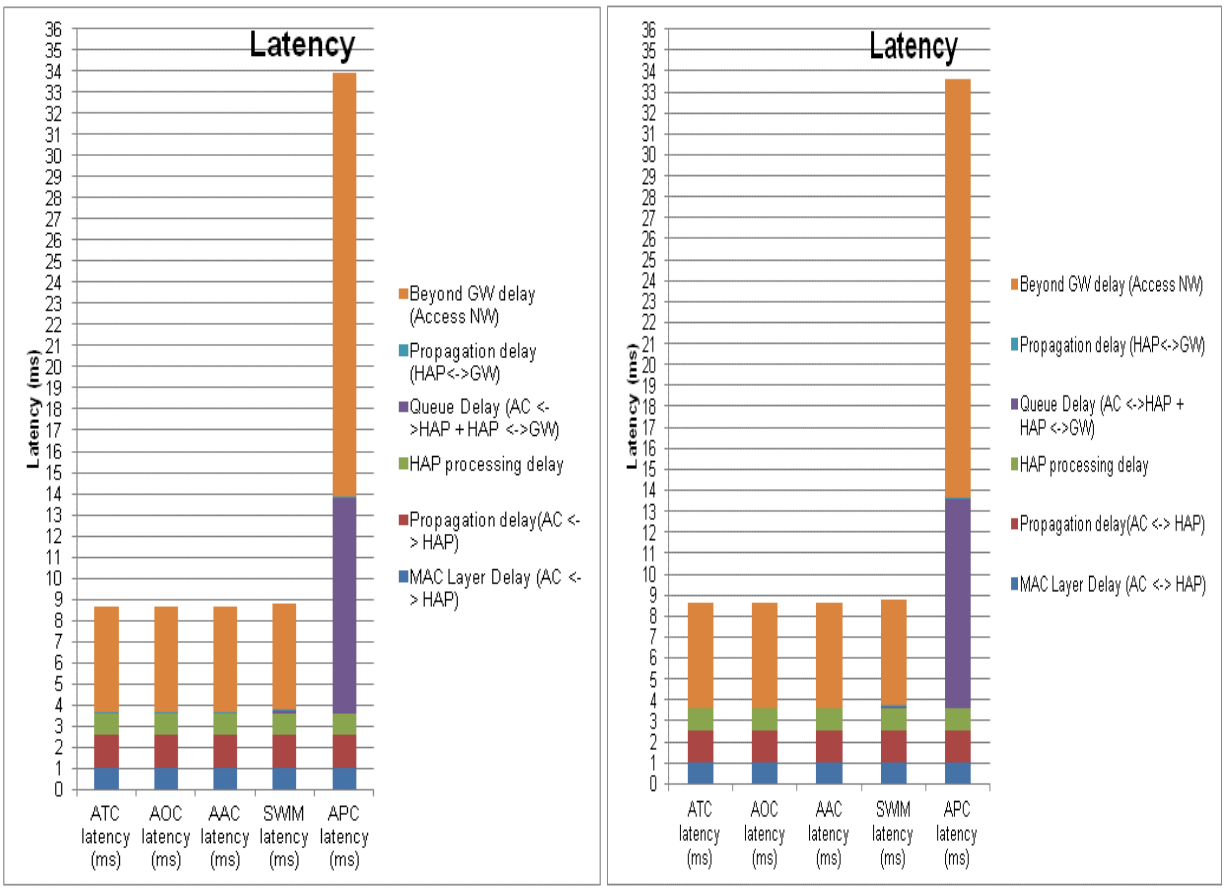


Figure 4-29 Mean Latency, Feeder FSO Link

The measure of the various delay components in transmission of packets on the Aircraft ↔ HAP link and on the HAP ↔ Ground Gateway link for the scenario of 400 AC/ HAP cell is shown in the Figure 4-30. There is no significant degradation observed in latency for supporting aircraft traffic up to 400 AC per HAP Cell. Beyond 400 AC/cell, there is no bandwidth available to transmit APC traffic. Hence, beyond 400 AC/cell, the latency of APC traffic becomes noticeably greater but the latencies of higher priority traffic classes do not increase significantly.



(a) With HAP ↔ Ground Gateway Cellular Link (b) With HAP ↔ Ground Gateway Feeder FSO Link

Figure 4-30 Latency Components, 400AC/HAP-Cell

4.2.6.2.5.2. Channel Bandwidth Utilization

Figure 4-31 (a), (b), (c) gives the Channel Bandwidth utilization for different traffic classes on the links involved in the transmission of a packet from aircraft to the ground gateway via the HAP, for different aircraft density levels in the HAP coverage area. As depicted in the Figure 4-31 (c), the feeder link channel utilization is limited by the traffic on the other link (Aircraft ↔ HAP link). The Aircraft ↔ HAP link being the bottle-neck, the HAP ↔ GW link is not utilized fully in case of FSO feeder link.

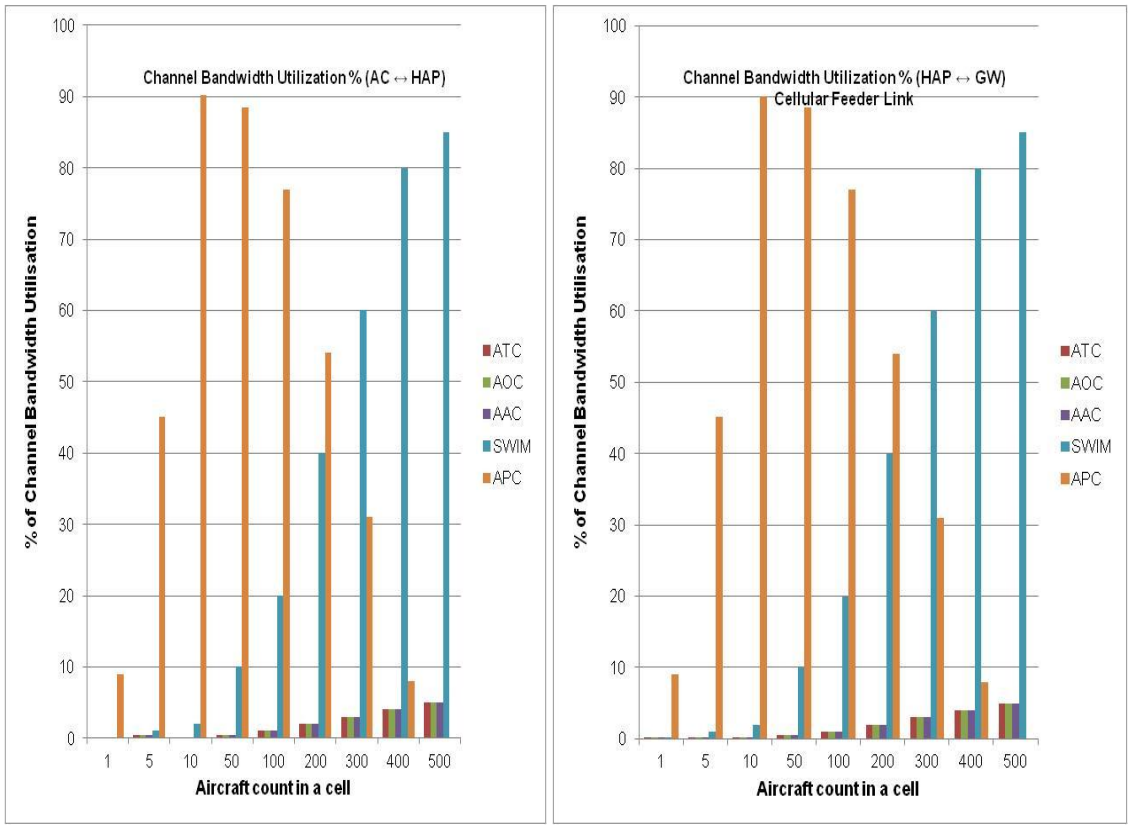


Figure 4-31 Channel Bandwidth Utilization of HAP Links

4.2.6.2.5.3. Packet Loss (Theoretical analysis)

Figure 4-32 gives the packet loss percentage for different traffic classes on the links (AC ↔ HAP link and HAP ↔ GW link) involved in the transmission of a packet from aircraft to the ground gateway via the HAP, for different aircraft density levels in the HAP coverage area. Majority of the packet loss can be observed on AC ↔ HAP bottleneck link. There is no loss on FSO feeder link as incoming traffic rate on the link is less than the FSO link capacity.

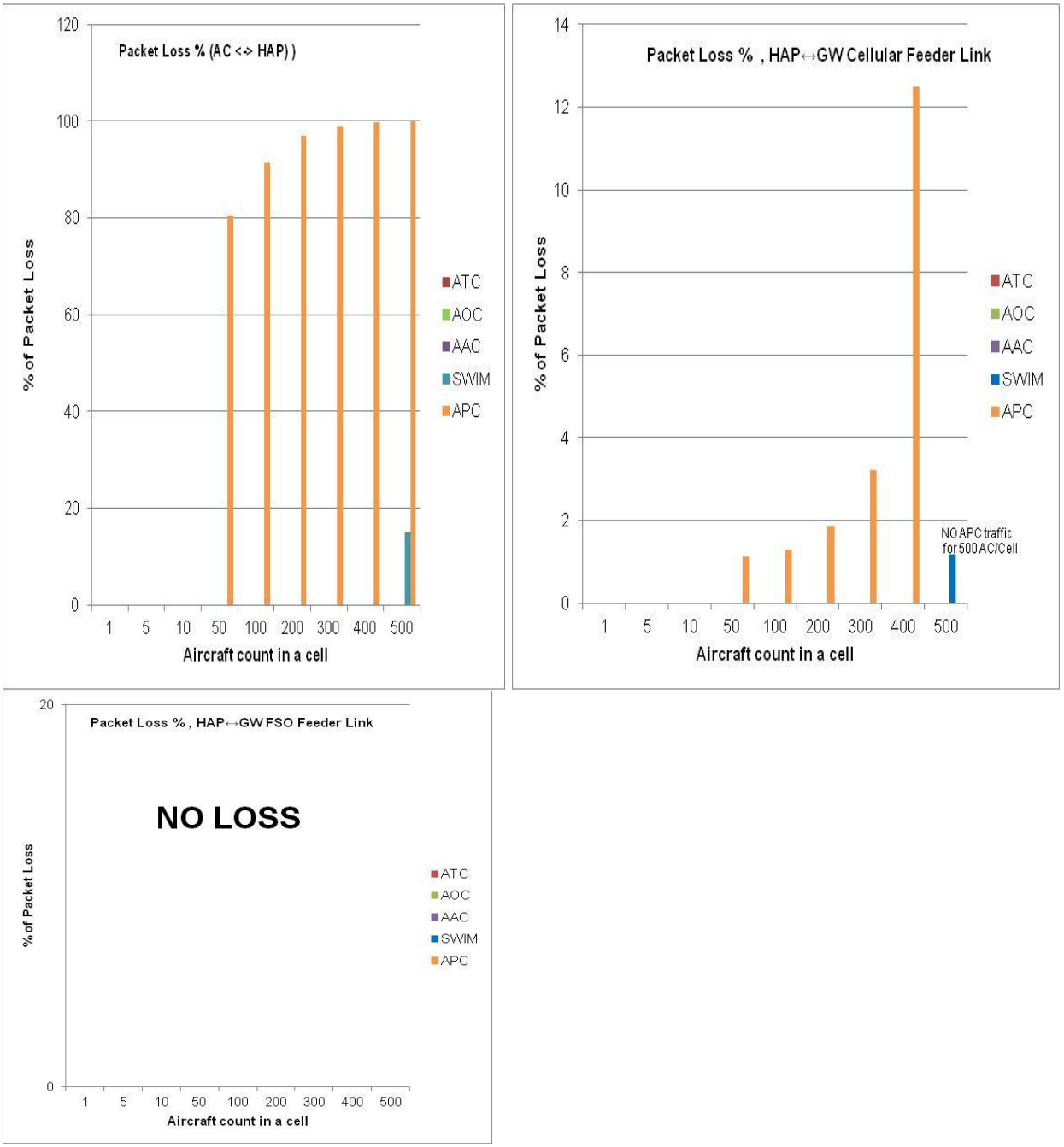


Figure 4-32 Packet Loss on HAP Links

4.2.6.2.6. Observations and Conclusions

The following are observations and conclusions based on HAP network analysis and simulation, assuming HAP tower channel link capacity up to 1 Gbps and the HAP coverage range up to 500 Km

- No significant degradation observed in latency for supporting aircraft traffic up to 400 AC per HAP Cell. The 95th percentile latency for 400 AC/Cell is ATC: 8.635 ms; AOC: 8.656 ms; AAC: 8.657 ms; SWIM: 9.038 ms; APC: 54.31 ms
- For 300 to 400 AC/Cell, the HAP network should be able to support the offered safety critical load.
- The aircraft-to-HAP link is found to be the bottleneck, with a greater number of aircraft per HAP cell as compared to that of the ground-based cellular base station cell. Majority of the packet loss can be observed on AC-to-HAP bottleneck link.

The HAP network is expected to provide performance similar to that of the ground-based cellular network, but with fewer HAP-based stations deployed across the whole CONUS region than the number of ground-based stations. However, as HAP-based coverage is higher than the coverage of a ground-based tower, higher link capacity is required between aircraft and HAP to support the larger aircraft count per HAP cell.

4.2.6.3. SATELLITE NETWORK MODEL AND SIMULATION

In the satellite network architecture analysis, a GEO satellite system with spot beam coverage is considered. A single GEO satellite with the ability to generate 100 narrow spot beams may be sufficient to provide services for all the aircraft flying over the whole CONUS region. The single spot beam footprint would have an area of 38,000 square miles and the 100 spot beams together would cover the entire CONUS of 3.71 million square miles. Figure 4-33 shows the network model considered for communication performance analysis using a GEO satellite platform.

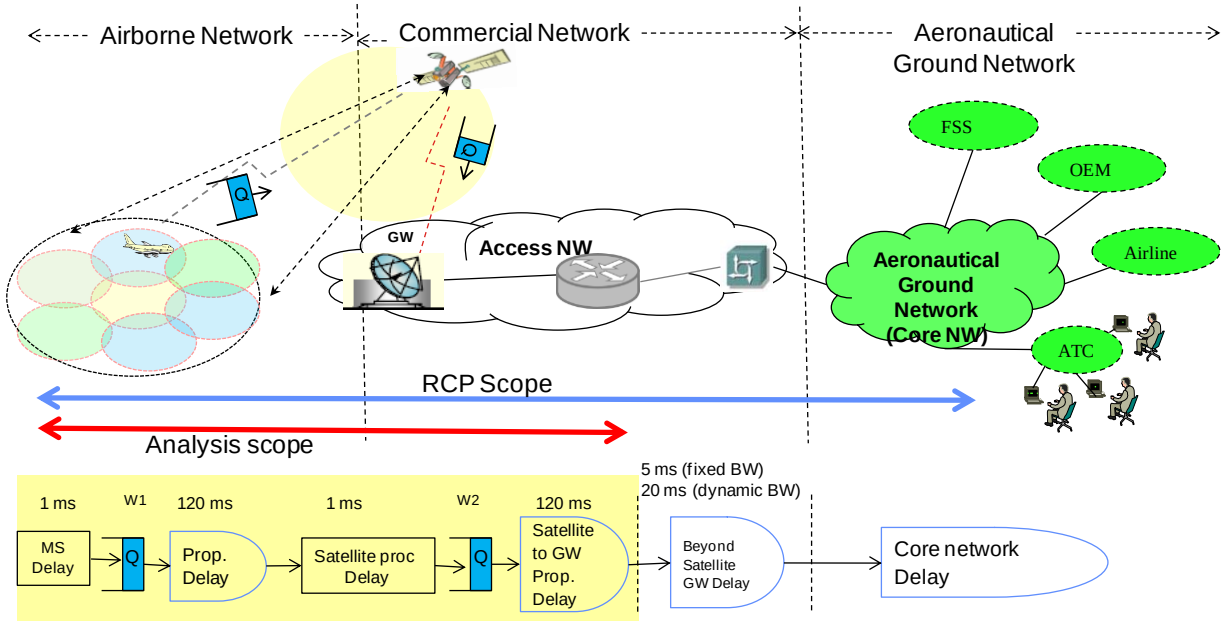


Figure 4-33 Satellite Network Model

The satellite with multiple transponders performs like a system which forms multiple towers in the sky providing coverage for data communication between the aircraft and the core aeronautical ground network. For the network analysis, assuming the total user capacity offered by a single satellite with up to 100 spot beams is 40 Gbps, the per-spot beam link capacity would be 400 Mbps. The feeder link channel bandwidth between the satellite and the ground gateway is assumed to be 10 Gbps.

4.2.6.3.1. Performance Analysis

For a satellite network with up to 100 spot beams per satellite, a theoretical approach and not simulation is conducted for analysis due to limitation in computer processing power to execute the simulation for such a large number of spot beams. The simulation runtime is very high to simulate the communications with the number of spot beams greater than 5.

As shown in the Figure 4-34, the cascaded queue model analysis is carried out, as essentially the traffic from each queue per spot beam is multiplexed over the single queue between the satellite and the gateway. The channel capacity per spot beam considered is 400 Mbps to derive the network performance statistics for the messages between aircraft and satellite. The channel capacity between the satellite and the ground gateway considered is 10 Gbps to derive the network performance statistics for the messages between satellite and gateway.

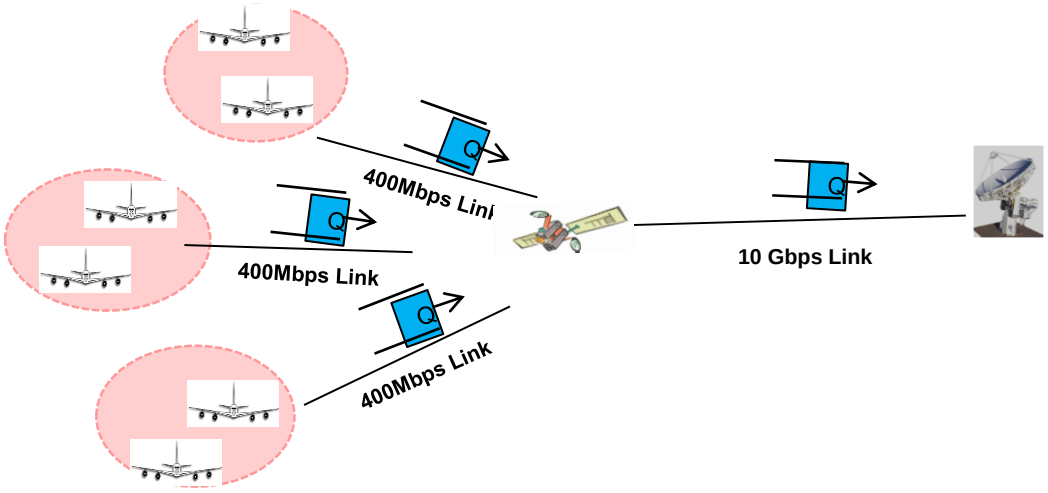


Figure 4-34 Satellite Network Analysis Model

4.2.6.3.1.1. Assumptions

The following are the assumptions made with respect to satellite network model analysis.

- Per Aircraft Traffic
  - ATC data rate: 100 kbps
  - AOC data rate: 100 kbps
  - AAC data rate: 100 kbps
  - SWIM data rate: 2 Mbps
  - APC data rate: 90 Mbps
- Packet size is 100 bytes , for each traffic type
- Per spot beam channel capacity: 400 Mbps
- Satellite-to-access network channel capacity: 10 Gbps
- Aircraft–to-satellite range: 36,000 Km
- Pre-provisioned connections are assumed between the aircraft and the satellite.
- MAC layer processing latency at aircraft and the satellite is assumed to be 1 ms
- The signal propagation latency between the aircraft and the satellite and between the satellite and the GW is up to 120 ms.
- The commercial network beyond the base station may introduce latency up to 5 ms in case of fixed leased bandwidth allocation and latency up to 20 ms in case of dynamic bandwidth for the aircraft services. High priority traffic (ATC, AOC, AAC, and SWIM) is assumed to have fixed bandwidth allocation with 5 ms latency and lower priority APC traffic type to have dynamic bandwidth allocations with up to 20 ms latency.

4.2.6.3.1.2. Latency

The overall latency of the satellite network is the summation of various delay components like MAC layer delay (at aircraft), queue delays in the aircraft-to-satellite link (Aircraft ↔ SAT link) and in the satellite-to-ground gateway link (SAT ↔ GW link), signal propagation delay between the aircraft and the satellite, MAC layer delay (at satellite), signal propagation delay between the satellite and the ground gateway and finally the delay inherent in the network beyond the gateway (Access NW). The queue delay involved in transmission of packets on Aircraft ↔ SAT link and SAT ↔ GW link is arrived using the Equation 4-5 [REF- QUEUES]. This equation is used for different classes of traffic with common packet size. The theoretical equation used for arriving at the latency for different traffic classes assume bit level preemption with common packet size for all the traffic classes. In actual simulation, preemption is considered at a basic TU level and different traffic classes have different packet sizes. Hence to arrive at the actual latency estimates with different packet sizes for different traffic classes, a correction factor, C, is applied as shown in Figure 4-35 for the theoretical traffic latency estimates. The Correction factor C is derived based on the latency result from cellular network's simulation and theoretical analysis as given in Equation 4-6.

$$E(W_q^k) = \frac{\frac{1}{2}\sum_{j=1}^{K} \lambda_j E(S_j^2)}{(1-\rho_1-\cdots-\rho_{k-1})(1-\rho_1-\cdots-\rho_k)}$$

Equation 4-5

Where

K traffic classes are indexed by k = 1…K.
Class k arrivals are Poisson distributed with arrival rate of λ_k.
Class k service times is S_k
μ is outgoing rate (Channel Capacity)
ρ is system utilization such that ρ = λ/ μ

Correction factor for latency = (Latency from Simulation)/ [(Latency from Theory)*(packet size)]

Equation 4-6

For ATC traffic packet size = 1 TU
For AOC traffic, packet size = 5 TUs
For AAC traffic, packet size = 5 TUs
For SWIM traffic, packet size = 20 TUs
For APC traffic, packet size = 20 TUs

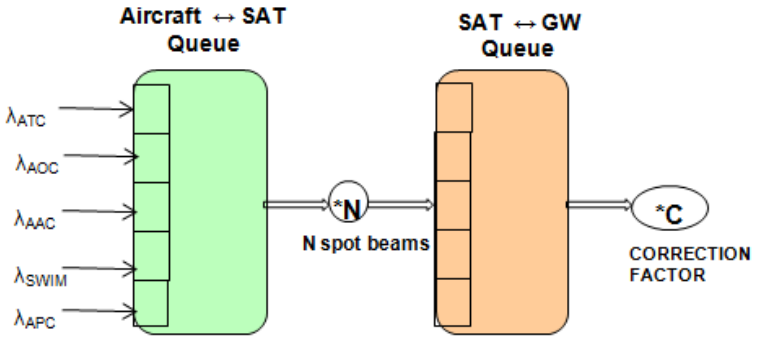


Figure 4-35 Cascaded Queue Model for Latency Estimation

The trend in the queue latency experienced by various traffic classes as the aircraft count increases in the satellite spot beam coverage domain on the two links (Aircraft ↔ SAT link, SAT ↔ GW link) is shown in the Figure 4-36.

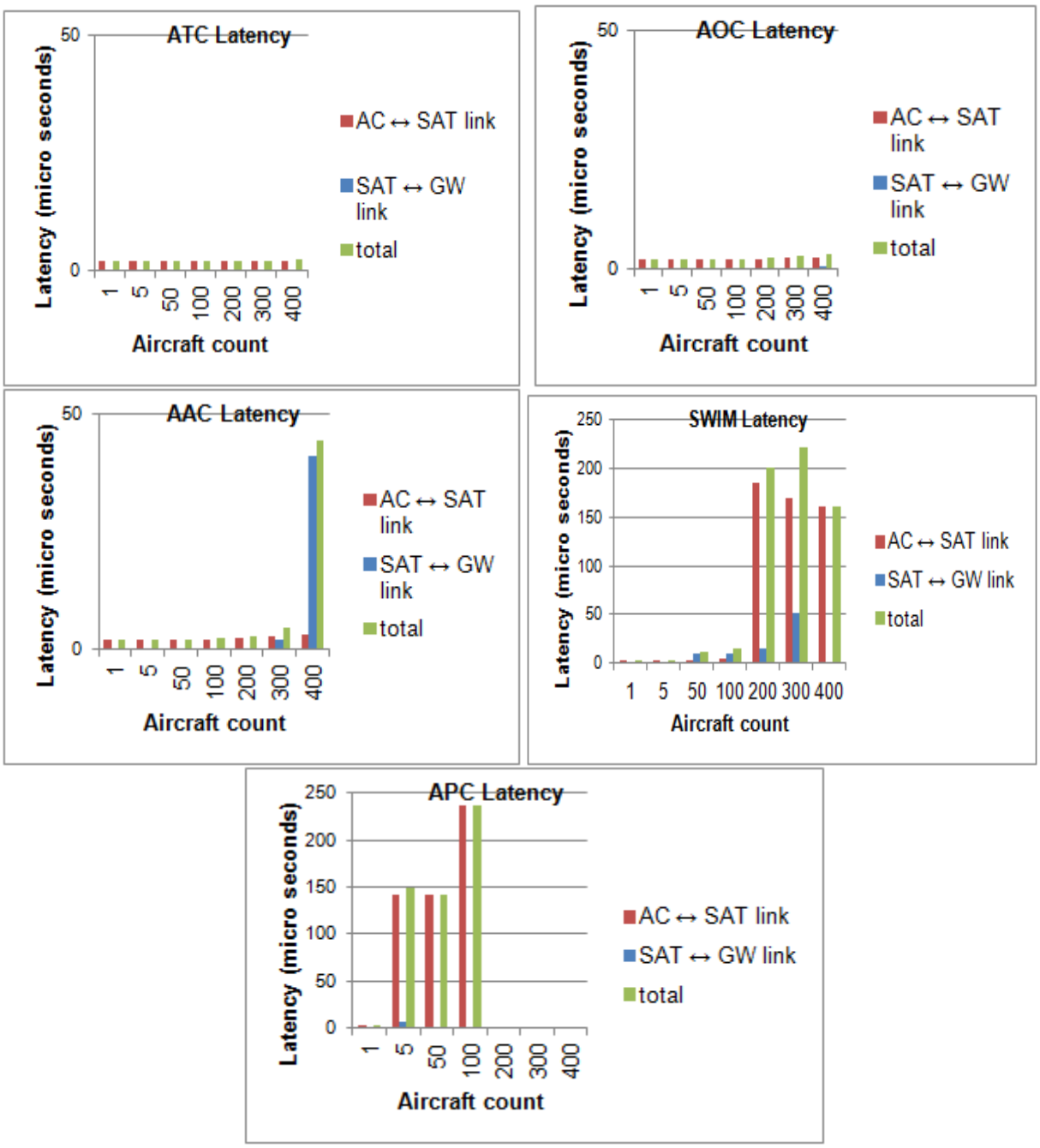


Figure 4-36 Queue Latency on Satellite Links

The overall latency with increasing number of aircraft in a given satellite coverage for various traffic types is shown in Figure 4-37. Beyond 100 aircraft per spot beam the APC traffic experiences 100% loss on the AC ↔ SAT link, hence no latency estimates for APC traffic on that link beyond 100 aircraft load per spot beam.

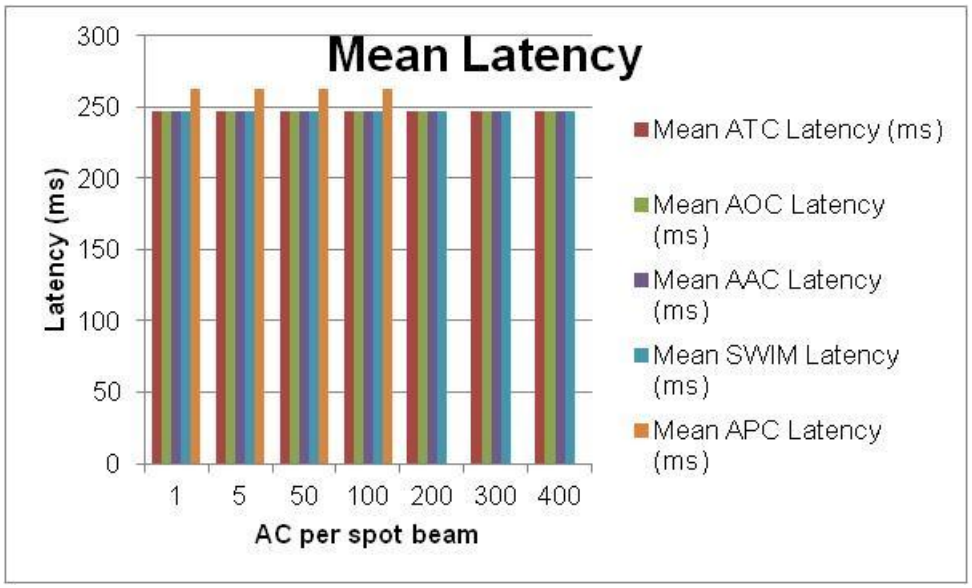


Figure 4-37 Mean Latency with Satellite Network

The measure of the various delay components for transmission of packets in a satellite network for the scenario of 100 aircraft per spot beam (AC/spot beam) is shown in Figure 4-38. The overall latency of the satellite network is: ATC - 247.0021 ms; AOC - 247.0022 ms; AAC - 247.0023 ms; SWIM - 247.0146 ms; APC - 262.237 ms, as shown in the Figure 4-38. The 95th percentile latency estimates are: ATC - 247.0064 ms; AOC - 247.0066 ms; AAC - 247.0069 ms; SWIM - 247.043 ms; APC - 262.71 ms.

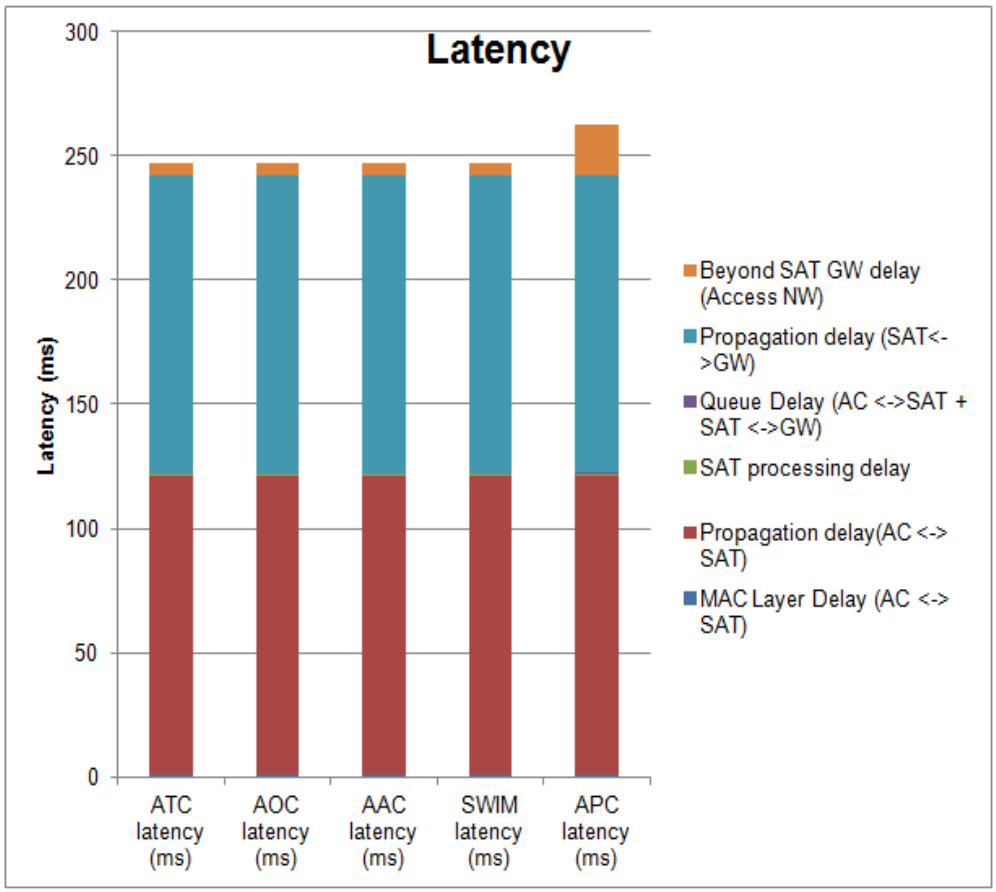


Figure 4-38 Latency Components in Satellite Network with 100 AC/Spot Beam

4.2.6.3.1.3. Channel Bandwidth Utilization

Figure 4-39 and Figure 4-40 give the channel bandwidth utilization for different traffic classes on the links (AC ↔ SAT link and SAT ↔ GW link, respectively) involved in the transmission of a packet from aircraft to the ground gateway via the satellite, for different aircraft density levels in the spot beam coverage area. With up to 100 AC in a spot beam, sufficient link data bandwidth is available for safety critical ATC and AOC, AAC, SWIM and up to 41% remaining for non-safety critical APC traffic. Under heavy traffic conditions (more than 100 AC in all the 100 spot beams) the SAT ↔ GW link becomes a bottleneck. The SAT ↔ GW link is the bottleneck as traffic from all the spot beams aggregate on this link. It is observed that no bandwidth is available for low priority APC traffic on SAT ↔ GW link beyond 10 aircraft per spot beam.

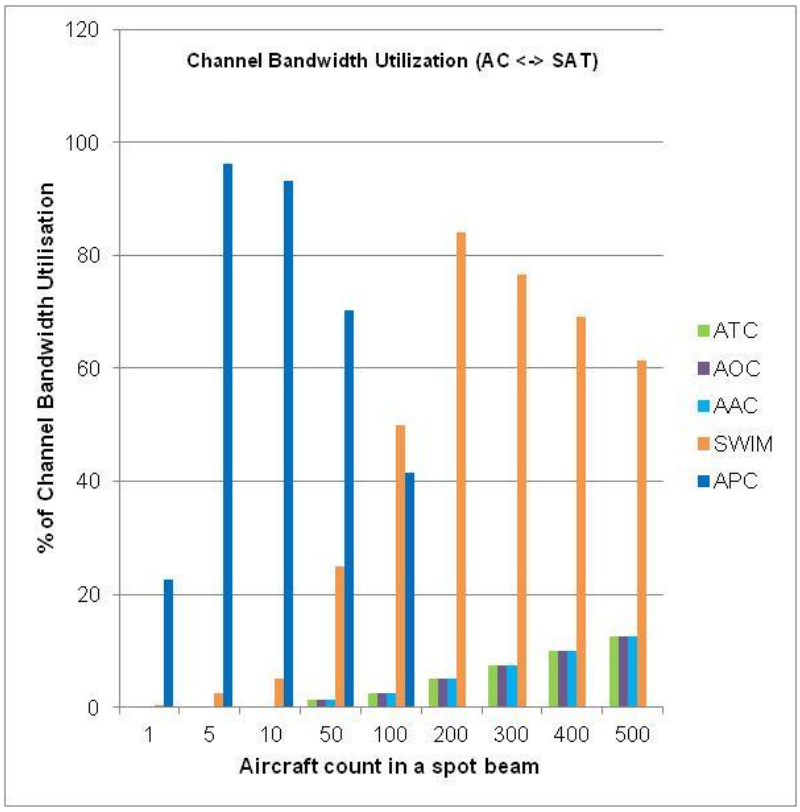


Figure 4-39 AC ↔ SAT link Channel Bandwidth Utilization

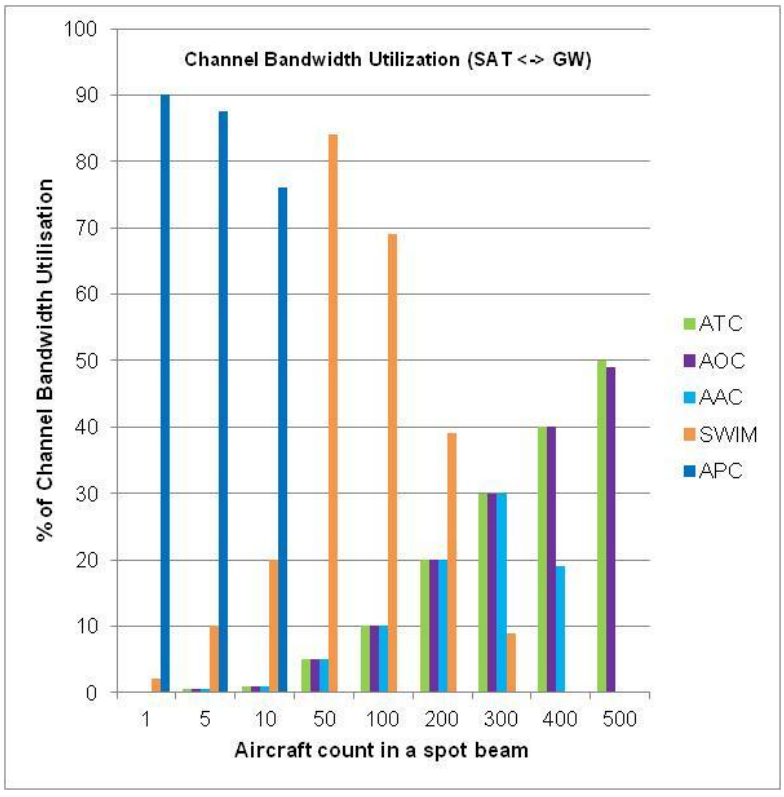


Figure 4-40 SAT ↔ GW Link Channel Bandwidth Utilization

4.2.6.3.1.4. Packet Loss

Figure 4-41 and Figure 4-42 give the packet loss percentage for different traffic classes on the two links (AC ↔ SAT link and SAT ↔ GW link) for varying number of aircrafts per spot beam. Beyond 100 AC per spot beam, SWIM and APC traffic loss occur on the AC ↔ SAT link. However besides APC traffic loss, SWIM traffic loss (16%) can be observed on the SAT ↔ GW link even with 50 AC/spot beam.

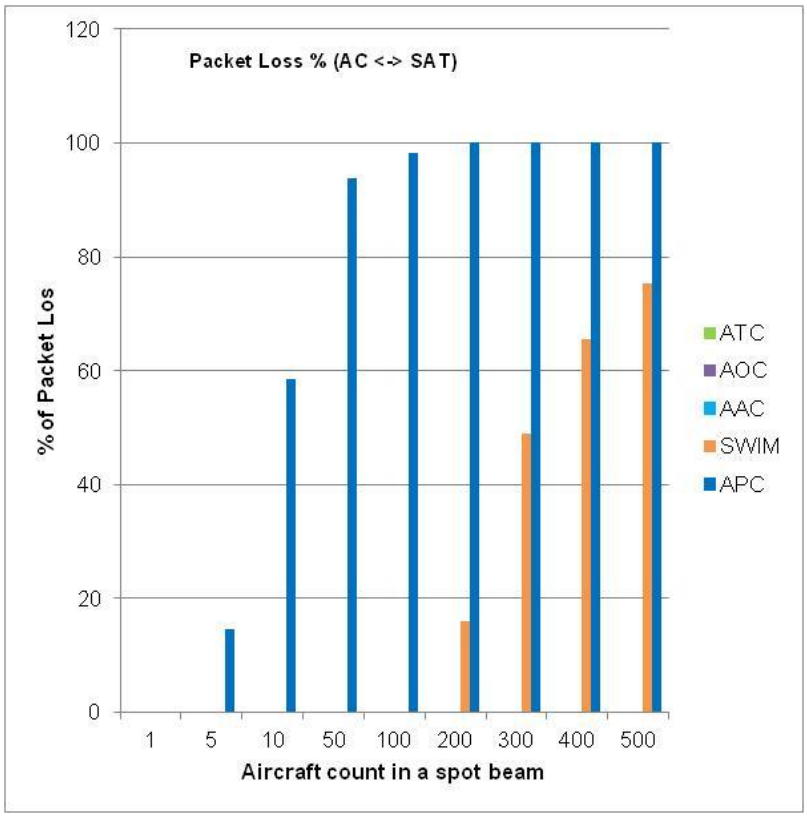


Figure 4-41 Packet Loss over AC ↔ SAT Link

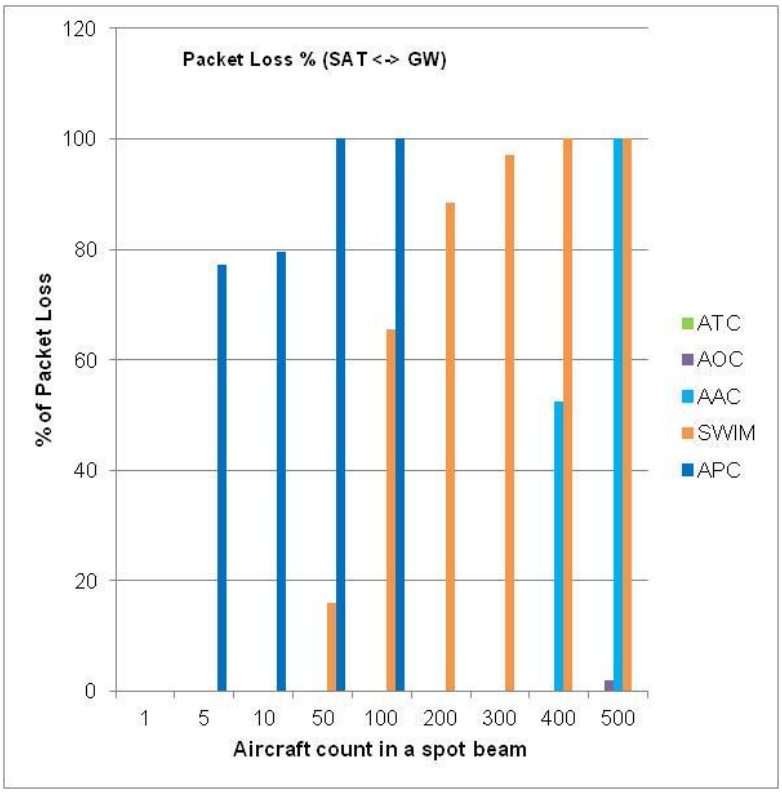


Figure 4-42 Packet Loss over SAT ↔ GW Link

4.2.6.3.2. Observations and Conclusions

The following are observations and conclusions based on satellite network analysis.

- Latency is higher on a satellite link owing to the inherently higher propagation delay, and hence not suitable for latency critical real-time applications. The 95th percentile latency with up to100 AC per spot beam is: ATC - 247.0064431 ms; AOC - 247.0066738 ms; AAC - 47.0069925 ms; SWIM - 247.0439507 ms; APC - 262.71018 ms
- Optimum channel utilization can be observed on the satellite spot beam network, owing to higher satellite coverage and higher number of aircraft served by the satellite.
- The network is able to support all of the safety critical traffic (ATS and AOC) and AAC with up to 300 aircraft per spot beam. However, SWIM and APC traffic Loss can be observed even with as low as 5 AC/spot beam.
- With cellular and HAP networks, the majority of packet loss can be observed on uplink (AC ↔ BS and AC ↔ HAP, respectively), whereas SAT ↔ GW link is the bottleneck in the satellite network. Significant cabin and crew service degradation can be observed as the aircraft count per spot beam increases. An APC traffic loss of 77% occurs even with as low as 5 aircraft per spot beam. Hence, a high bandwidth FSO link may be good alternative link between satellite and GW.

4.2.6.4. AIRCRAFT-TO-AIRCRAFT NETWORK MODEL AND SIMULATION

The aircraft-to-aircraft communication network has the potential to capture the benefits associated with short-range links while at the same time offering high-capacity and good scalability. Specifically, this communication system could be used to improve the efficiency of air traffic control. Air-to-air communications may an enabler for relaxation of spacing requirements and provision of more energy-efficient paths.

4.2.6.4.1. Communication Model

Figure 4-43 shows the network model considered for communication performance analysis for aircraft-to-aircraft communication. The major components of the aircraft-to-aircraft communication model comprises of air segment and ground segment.

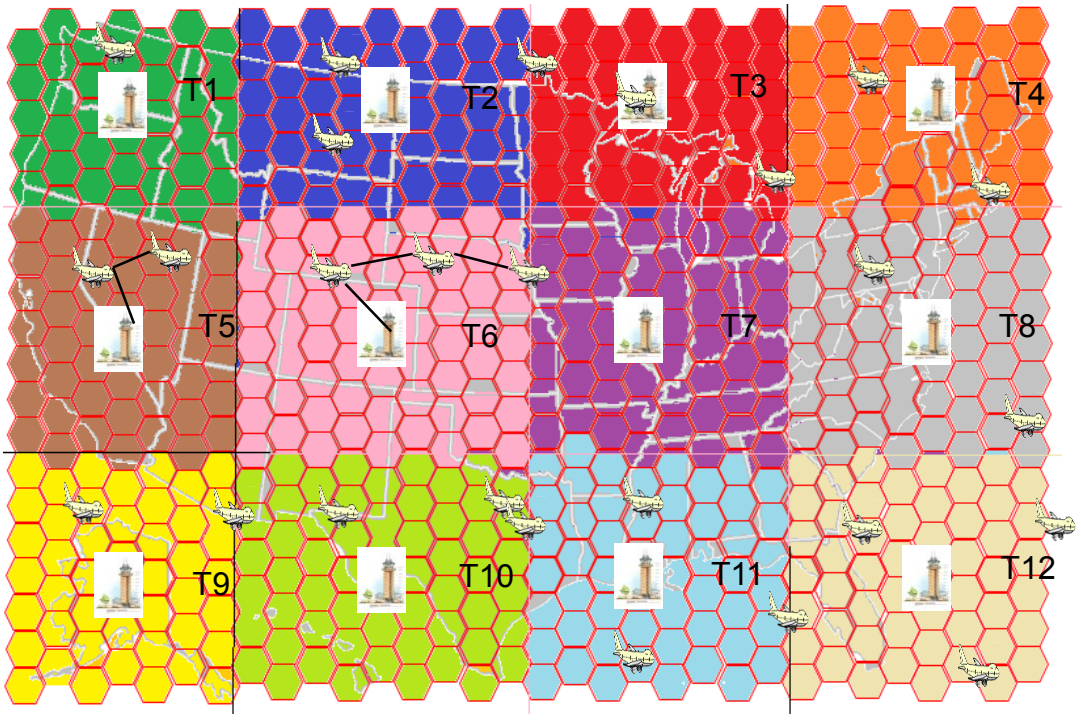


Figure 4-43 Aircraft-to-Aircraft Communication Network Model

4.2.6.4.1.1. Air Segment

The air segment essentially comprises of aircraft flying routes in accordance with the airline schedules. In the analysis, aircraft traffic in the air segment is characterized by the airline data obtained in the form of ADSI data from Honeywell GDC. The data includes flight number, the location and time of departure and arrival, latitude position, longitude position, etc.

4.2.6.4.1.2. Ground Segment

In addition to mobile aircraft nodes, the model includes a network of ground stations. These stations serve as the gateways between the airborne network and ground infrastructure such as the aeronautical ground network. The ground stations are considered to be placed at major centers across the CONUS such that at any given point of time all the aircraft can get connectivity to at

least one ground station. An area comprising a group of pseudo cells is assumed to be serviced by the nearest ground station. The actual position of the ground stations considered in the analysis is provided in the Table 4-11. Any pseudo cell as depicted in Figure 4-43 is assumed to be serviced by the nearest tower based on distance proximity.

Table 4-11 Ground Stations' Positions

airport_ident	latitude	longitude
KMWH	47.20858	-119.319
KHLN	46.60681	-111.983
KGCC	44.34892	-105.539
KMIC	45.06199	-93.3539
KRNO	39.49911	-119.768
KSLC	40.78839	-111.978
KLNK	40.85089	-96.7591
KCMI	40.03883	-88.2778
KMHV	35.05864	-118.151
KPHX	33.43428	-112.012
KDEN	39.86167	-104.673
KMEM	35.04242	-89.9767
KBOW	27.94336	-81.7834
KSJT	31.35776	-100.496
KNEW	30.04242	-90.0283
KPIT	40.49147	-80.2329
KBTV	44.47186	-73.1533
KATL	33.6367	-84.4279
KGFK	47.94728	-97.1738
KEWR	40.6925	-74.1687
KSAW	46.35364	-87.3954

4.2.6.4.2. Aircraft Connectivity Analysis

Air-to-air network communication is essentially relay communication from aircraft to the base station.

In the air-to-air connectivity analysis algorithm, each base station and aircraft is referred as a node. Each node maintains the list of adjacent nodes. It starts with the list of base stations available in the CONUS region. For this analysis, 21 base stations (see Table 4-11) are used across the CONUS region.

The aircraft nodes traverse along their flight paths past other aircraft and base stations and use the air-to-air and air/ground communication networks to capture information on the list of adjacent

nodes (connected aircrafts) for connectivity to the base stations. They update the connection status of adjacent nodes in the list.

Each node recursively looks at its list of adjacent nodes and searches for the number of nodes connected to the each connected node.

Each aircraft has a range of 120 nm (range circle with 2 degree radius) and an aircraft is said to be connected if it satisfies anyone of the below criteria:

1. If the aircraft falls in the range of another aircraft which falls in the range of a ground station
2. If the aircraft falls in the range of another aircraft which is subsequently connected to a ground station through other aircraft

An aircraft that is isolated and does not fall within range of any aircraft or ground station is disconnected as shown in Figure 4-44. This figure shows a snapshot of a simulated air-to-air communication network, taken from the NAS Network Simulation and Visualization program, which is presented in section 4.2.7. The aircraft nodes are represented as circles proportional to the radio range of the aircraft. A blue circle indicates connectivity to a ground base station. A red circle indicates the aircraft does not have connectivity to a ground base station.

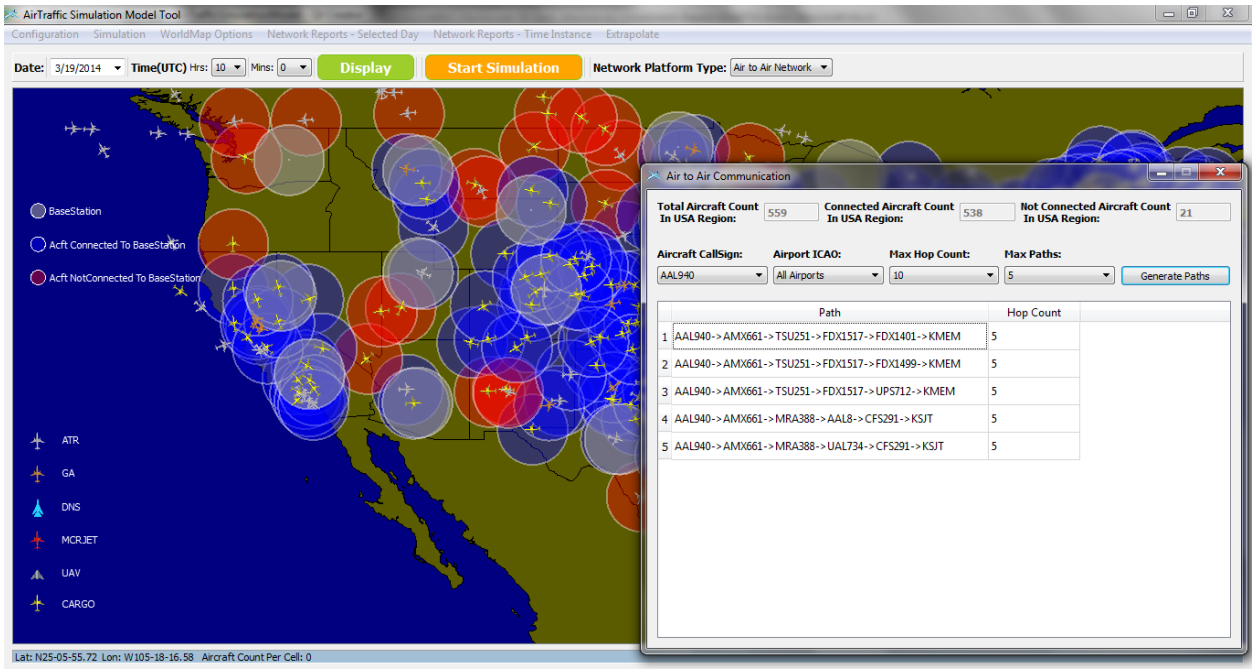


Figure 4-44 Aircraft-to-Aircraft Communication Connectivity Report

4.2.6.4.3. Air-to-Air Data Traffic Estimates

The estimated data traffic for aircraft-to-aircraft communication is similar to that provided in the Table 4-9 for ATC, AOC and AAC traffic. The high bandwidth requirement traffic types viz.; SWIM and APC traffic are not considered in aircraft-to-aircraft communication as the aircraft-to-

aircraft communication may not be able to, and maybe should not, handle this traffic. Besides the unicast traffic from the aircraft, broadcast traffic in a 100 nm Cell service domain is also considered in the aircraft-to-aircraft communication. However, only the unicast traffic is considered to be relayed between aircraft towards the ground station. The broadcast traffic is not relayed beyond the Cell domain. Table 4-12 gives the broadcast traffic rate within a 100 nm Cell service domain as provided in the COCR document for COCR Phase 2 [REF_COCR]. The APT domain COCR Phase 2 broadcast traffic rate is extrapolated at 2.5% YoY to obtain the estimates for the year 2060. Table 4-13 gives the broadcast traffic estimates for 2060, within a 100 nm Cell service domain.

Table 4-12 COCR Phase 2 Broadcast Traffic Rate within a 100 nm Cell Service Domain

Information Transfer Rate (kbps) - 100 NM Range	**APT**	**TMA**	**ENR**	**ORP**	**AOA**
	816	544	145	NA	NA

Table 4-13 Broadcast Traffic Rate Estimates within a 100 nm Cell Service Domain for 2060 Timeframe

Estimated traffic in 2060 (Kbps) – Broadcast Traffic in a 100 nm Service Domain	**Broadcast**
ATR	1,712
Microjet	1,712
Business Jets	1,712
UAS	1,712

4.2.6.4.4. Performance Requirement Analysis

The aircraft-to-aircraft communication performance analysis is carried out at the cellular level. All the aircraft traffic in a given Cell is assumed to be relayed to one of its adjacent Cells towards the nearest ground station, as shown in Figure 4-45. Hence the area serviced by a ground station is a group of Cells belonging to different levels, where the traffic in a higher level Cell is directed towards the lower level Cells. The number of Cells in each level is given below.

- Level 0 – 1 Cell, (Level 0 has one cell, the ground station located in the Cell)
- Level 1 – 6 Cells
- Level 2 – 12 Cells
- Level 3 – 18 Cells
- Level 4 – 24 Cells
- And so on…

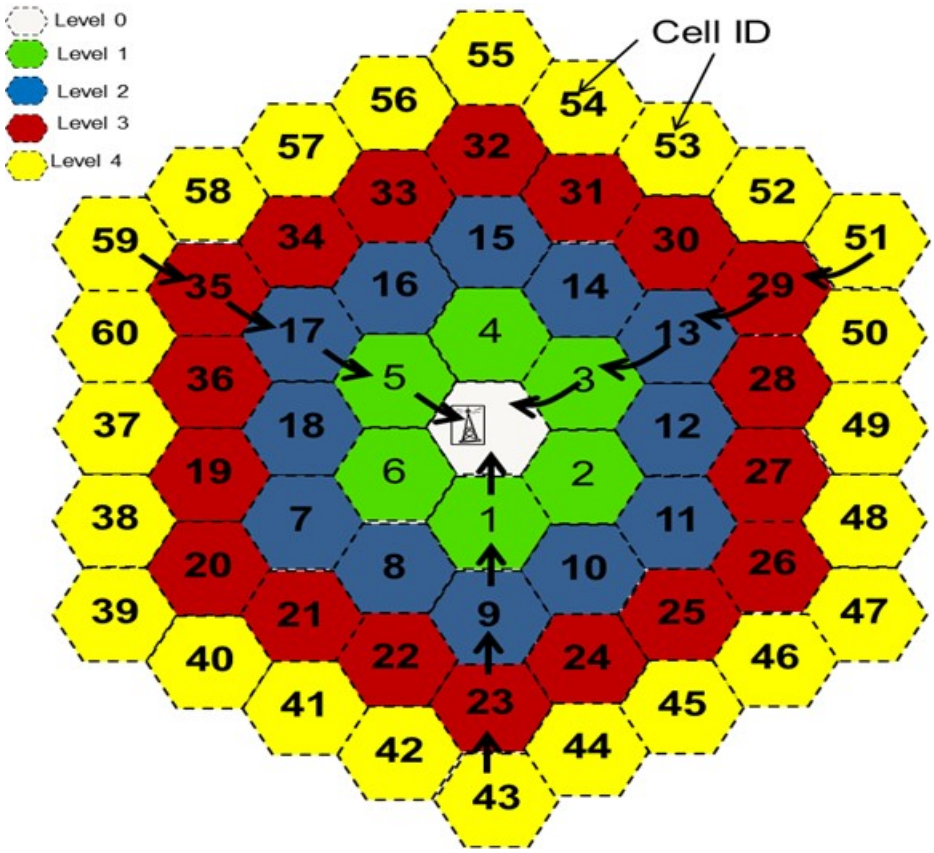


Figure 4-45 Cell Arrangement in Aircraft-to-Aircraft Communication Network

The total traffic in a Cell is the sum of the Cell's Self-Traffic and relay unicast traffic from higher level Cells. The Cell's Self -Traffic is given by the Equation 4-7.

Cell's Self -Traffic = (No. of aircraft in the Cell)* (Per aircraft unicast traffic) + Broadcast traffic
Equation 4-7

Three technology links viz. VHF, L-band and FSO are considered for the aircraft-to-aircraft communication performance measurement in a Cell. The channel bandwidth assumed for the different links are

- VHF band: 14 Mbps
- L-band: 150Mbps
- FSO: 10 Gbps

The air-to-air network load and Cell-wise communication performance is determined using the NAS Network Simulation and Visualization program described in section 4.2.7. The performance of the aircraft-to-aircraft communication network is presented in section 4.2.7.3.

4.2.7. NAS Network Simulation and Visualization

The Air Traffic Simulation Model Tool is a NAS network simulation and visualization tool that generates the statistics characterizing the performance of the simulated network architectures. The key requirement that is considered to be fulfilled by the network architectures is the provision of guaranteed network bandwidth at least for safety critical services. The criterion which are defined for the assessment of network performance are the one-way packet latency, total achieved throughput and packet loss rate for the different kinds of services.

The tool is developed using C++ and the Qt toolkit. The Qt toolkit is a cross-platform application framework that is used for developing application software with a graphical user interface (GUI) and it supports C++. All the configuration data is stored and processed in memory only to do the analysis and generate reports, i.e., no database is used for data storage in this simulation tool.

Honeywell GDC organization has the capability to monitor all air traffic across the globe in real-time. Current air traffic information called Aircraft Situation Display to Industry (ASDI) is obtained from the Honeywell GDC database and is used by the Air Traffic Simulation Model Tool. ASDI data covers only the North America region.

4.2.7.1. SIMULATION SCHEDULER

The simulation scheduler module reads the aircraft, airport and single cellular network tower data from the CSV (comma separated values) files either explicitly or can be selected using the browse option provided. It takes files as inputs which are placed in the default configured folder path.

The user can overlay the aircraft display on the world map using Configuration → ASDI data menu item. See Figure 4-46. ASDI data is categorized and plotted based on the call sign of an aircraft. The simulation executes and displays the aircraft position at every 5 minute simulated time interval.

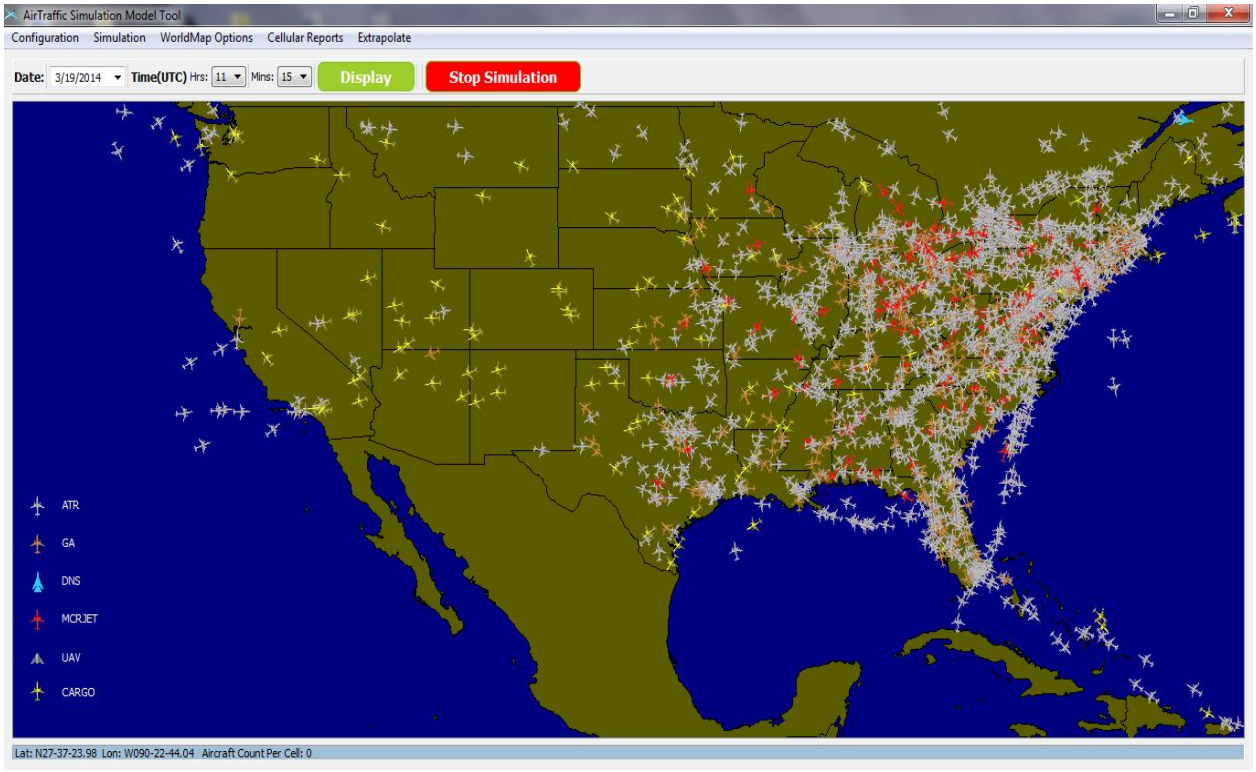


Figure 4-46 Overlay of Aircraft Display on Map

Display and Run Simulation options are provided to display and simulate aircraft position data on the map to analyze the air traffic congestion zones in the CONUS region. The user can select the time (UTC time zone) and display the air traffic data for that instance of time. Run Simulation option runs the simulation up to 2 hours at 2 seconds screen refresh rate and displays the aircraft position data for every 5 minute simulated time interval.

For the Single Cellular Network performance analysis, the tool provides the aircraft count and network performance report to analyze the network performance at a particular instance of time. The data is classified for different categories of aircraft such as ATR, General Aviation, military aircraft, microjets, cargo aircraft and UAVs and data service types, including ATC, AOC, AAC, SWIM and APC.

4.2.7.2. USER INTERFACE

The main menu of the tool includes the menus, namely Configuration, Simulation, World map options, Network Reports – Selected Day, Network Reports – Time Instance and Extrapolate.

The Configuration menu consists of the options to load the ASDI data, Airport Information, Communication Information, Network Configuration (Cellular, HAP, Satellite) and Air-to-Air Network Configuration. Selecting the ASDI data will open up a browse option to select a CSV file to render the aircraft position data present in the file. Likewise, options are available for the Airport Information to render the airports and Communication Information to render the Communication Towers.

Network Configuration (Cellular, HAP, Satellite) opens a pop-up window in which channel bandwidth can be input, as shown in Figure 4-47. A user can also modify and save the data traffic rate for different aircraft and different network users.

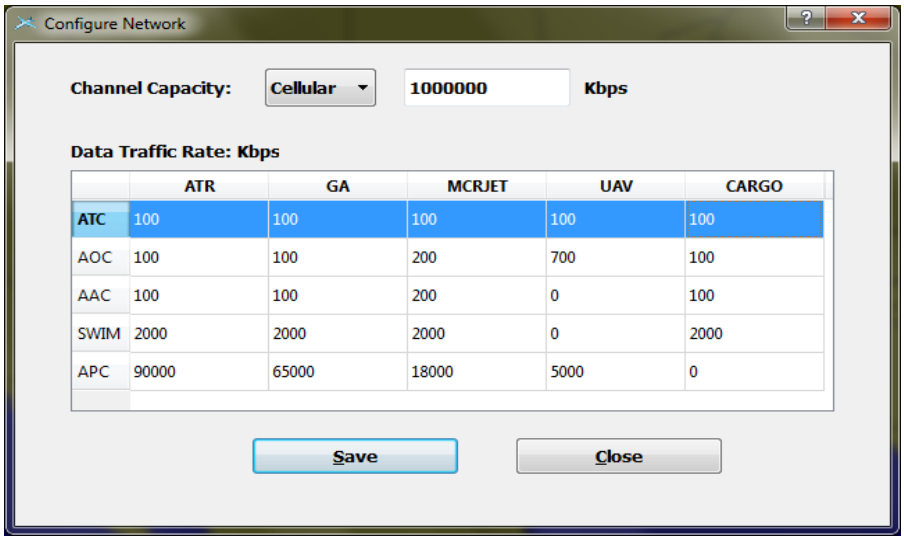


Figure 4-47 Configuration Network Dialog - Cellular, HAP and Satellite

Air-to-Air Network Configuration opens a similar network configuration window with Broadcast and Unicast data traffic options as shown in Figure 4-48. A user can also select the type of air-to-air link and can also input the corresponding data traffic in Kbps. The user can also modify the Broadcast and Unicast data traffic and can save the data traffic rate for different aircraft and different data service types.

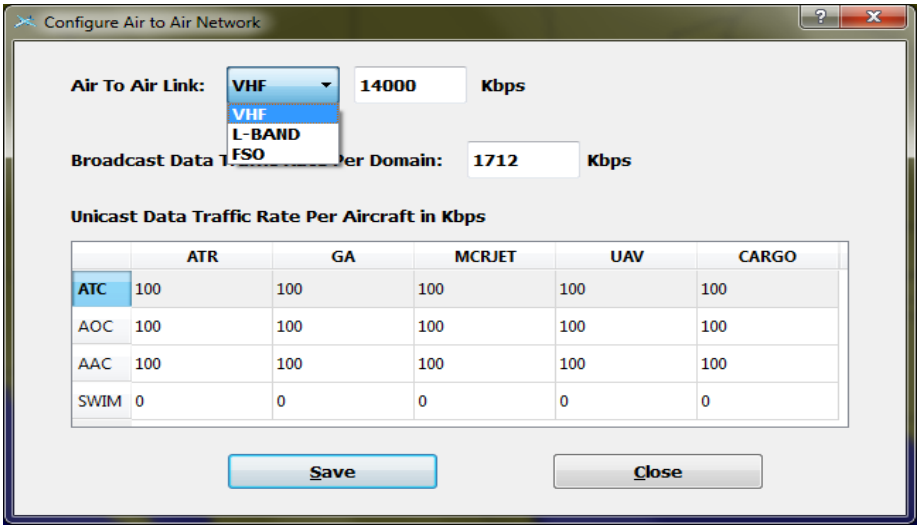


Figure 4-48 Air-to-Air Network Configuration Dialog

The tool menu consists of the Start Simulation and Stop Simulation options, which enables and disables the run simulation feature, respectively.

The World Options menu has the zooming and pan options for effective viewing. This menu also has options to load the ASDI data, communication towers and airport information and uses as inputs files placed in the default configured folder. The display grid option displays a dotted line for every 5 degrees and a plain line for each degree, so the plain line grid indicates a 1 degree by 1 degree grid. Display Airport Identifiers option lists the ICAO identifiers for all the airports in the CONUS and the "find ident" option takes a particular ICAO identifier as input and locates it on the map.

The Network Reports menu provides the options to see the summary report on the map and generates the network coordinate information. This network report lists different aircraft category counts for all grids available in the CONUS region.

There is an option in the menu called Extrapolate which takes the estimated percentage growth for every year and extrapolate year as inputs, as shown in Figure 4-49. It instantly displays the increased density of aircraft over the map upon clicking the "Extrapolate and Display" button.

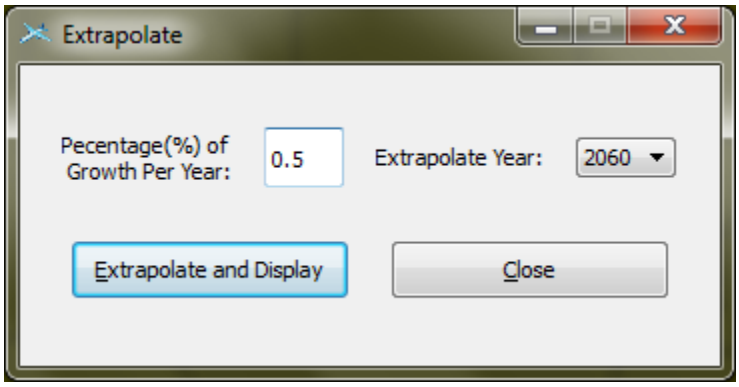


Figure 4-49 Extrapolate Dialog

Extrapolate displays the aircraft density based on the time period to increase the number of aircraft in the CONUS region and to analyze the network demand for a future time frame such as 2060. Note that UAVs are added only to the 2060 timeframe based on the population in major cities as explained in section 4.2.3.2.

Left click with a mouse device over the map displays a menu called context menu which has frequently used options like network performance statistics per grid, ASDI, airports, communication, zooming and display grid. The tool provides a context menu option to move the map between world map and CONUS region only.

A toolbar is available at the top of the tool's window where Date and Time selection is provided in UTC time zone. The Date field is populated automatically by reading data from the input ASDI data file. Time can be input by selecting values from the drop-down box and clicking on the display button to render the aircraft traffic data on the map at that selected time instant.

The bar below the map is called the status bar which shows the Lat-Lon position of the cursor and also displays the number of aircraft in a particular hexagonal grid.

4.2.7.3. PERFORMANCE STATISTICS REPORTS AND DISPLAYS

The user can select the network type using a combo box available with the network types – Cellular, HAP, Satellite and Air-to-Air networks. The corresponding links in the Network Reports (selected day and time) menu are enabled when the user selects the network.

The tool has the capability to extract the following four network summary reports for the three networks, namely Cellular, HAP and Satellite networks:

1. Network Performance Statistics Report for the selected time instance for the North American region network grids
2. Network Report for the Aircraft Count for the selected time instance for the North American region network grids
3. Network Performance Statistics Report for the selected day for the North American region network grids
4. Network Report for the Maximum Aircraft count for the selected day for the North American region network grids

A Network Performance Statistics Report provides all the air traffic data over the network grids (Cellular, HAP and Satellite), which are overlaid in the North America region map. The traffic demand, generated traffic, system delay percentile and loss probability are listed for each grid for all the types of data service types, namely ATC, AOC, AAC, SWIM and APC. This data is saved in a CSV file which serves as input to a Microsoft ® Excel ® spreadsheet in which all the graphs are displayed.

Network Report for the Aircraft Count gives the grid-wise air traffic data with latitude and longitude positions, different aircraft types and also the total number of aircraft per grid.

Network Report for the Maximum Aircraft count for the selected day gives the maximum aircraft count along with the time instant in the selected day. For all the communication networks, performance statistics per grid reports can be generated for the desired time period. The user navigates to the specific grid and clicks on the network performance per grid option. It pops up the single grid report input dialog to enter the start time and end time to analyze the reports for that grid. See Figure 4-50.

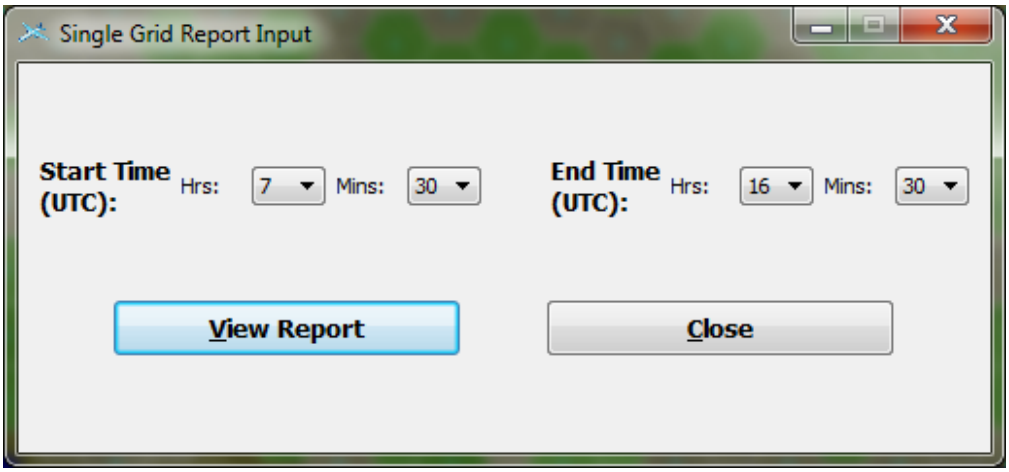
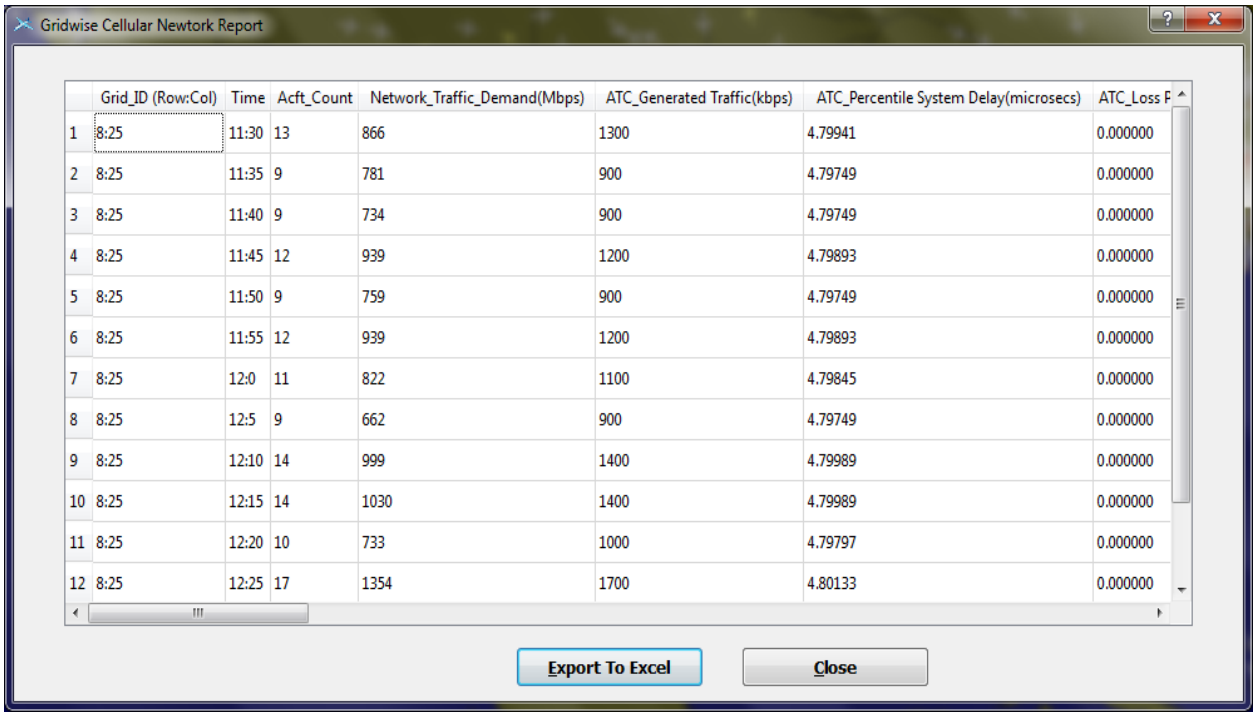


Figure 4-50 Single Network Performance Report Input Dialog

Once the user clicks on View Report option, the network performance data is displayed in a tabular format in grid wise network report dialog, as shown in Figure 4-51. This report provides the traffic demand, generated traffic, system delay percentile and loss probability for the selected grid for all the data service types, namely ATC, AOC, AAC, SWIM and APC, from the selected start time to the selected end time 5 minute time intervals.

Export to Excel button exports the tabular data to a CSV file to generate graphs using the Microsoft ® Excel ® graph template functionality.



	Grid_ID (Row:Col)	Time	Acft_Count	Network_Traffic_Demand(Mbps)	ATC_Generated Traffic(kbps)	ATC_Percentile System Delay(microsecs)	ATC_Loss P
1	8:25	11:30	13	866	1300	4.79941	0.000000
2	8:25	11:35	9	781	900	4.79749	0.000000
3	8:25	11:40	9	734	900	4.79749	0.000000
4	8:25	11:45	12	939	1200	4.79893	0.000000
5	8:25	11:50	9	759	900	4.79749	0.000000
6	8:25	11:55	12	939	1200	4.79893	0.000000
7	8:25	12:0	11	822	1100	4.79845	0.000000
8	8:25	12:5	9	662	900	4.79749	0.000000
9	8:25	12:10	14	999	1400	4.79989	0.000000
10	8:25	12:15	14	1030	1400	4.79989	0.000000
11	8:25	12:20	10	733	1000	4.79797	0.000000
12	8:25	12:25	17	1354	1700	4.80133	0.000000

Figure 4-51 Grid Wise Cellular Network Report Dialog

4.2.7.3.1. Ground-based Cellular Network Display

Figure 4-52 provides an example of the Ground-based Cellular Network performance statistics display. It shows the display for the selected day on the CONUS map and includes all categories of aircraft and data service types. A hexagonal cellular grid covers about 2 degree by 2 degree grid with a channel capacity of 1Gbps and around 360 grids cover the entire CONUS region. The user can configure the channel capacity and data traffic of different sources and aircraft types. A legend showing the different hex grid colors for different traffic options like Traffic but NO Loss, All Category Traffic Loss, AOC+AAC+SWIM+CABIN Loss, SWIM+CABIN Loss, Only Cabin Loss and No Traffic gives effective display for understanding the summary report on the map. The maximum aircraft count in that particular grid at the particular time in the selected day is displayed in the center of each grid.

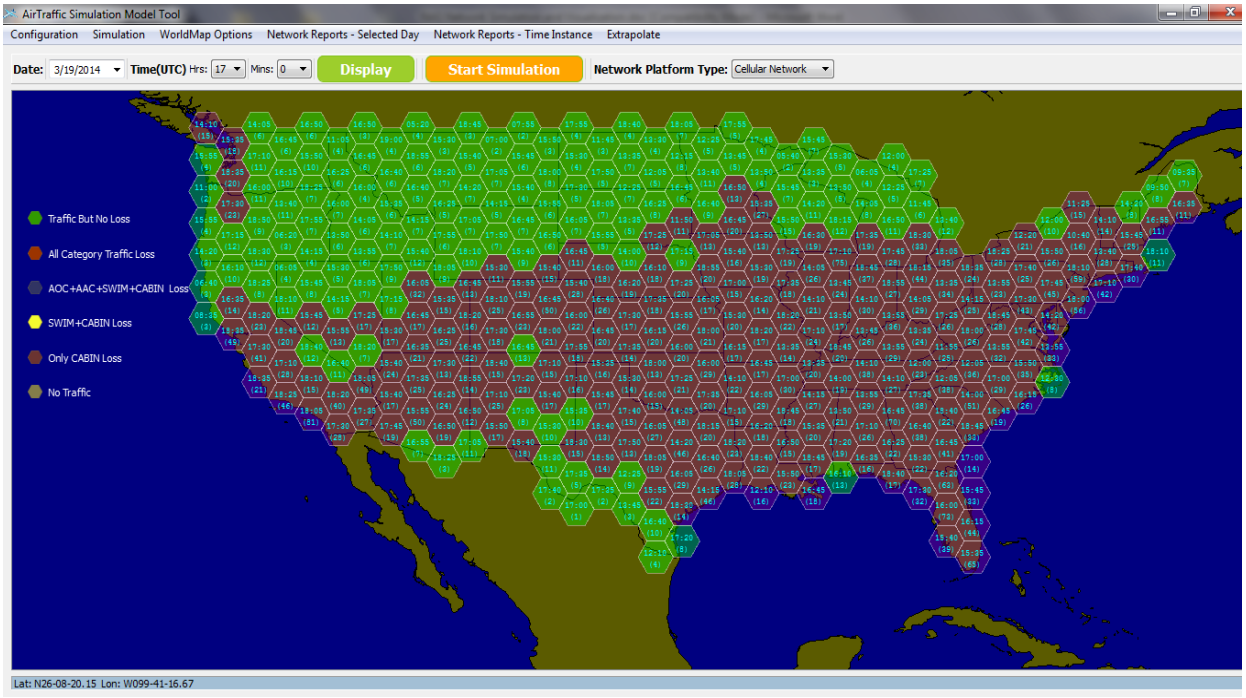


Figure 4-52 Ground-based Cellular Network Performance Statistics Display for Selected Day

4.2.7.3.2. HAP-based Cellular Network Display

Similarly, the HAP-based Cellular Network is shown in Figure 4-53. The display has around 100 HAP platforms covering the CONUS region, Figure 4-53 which is depicted as 4 degree by 4 degree HAP cell with a channel capacity of 1 Gbps. The same legend of the data traffic loss is depicted for all the communication networks.

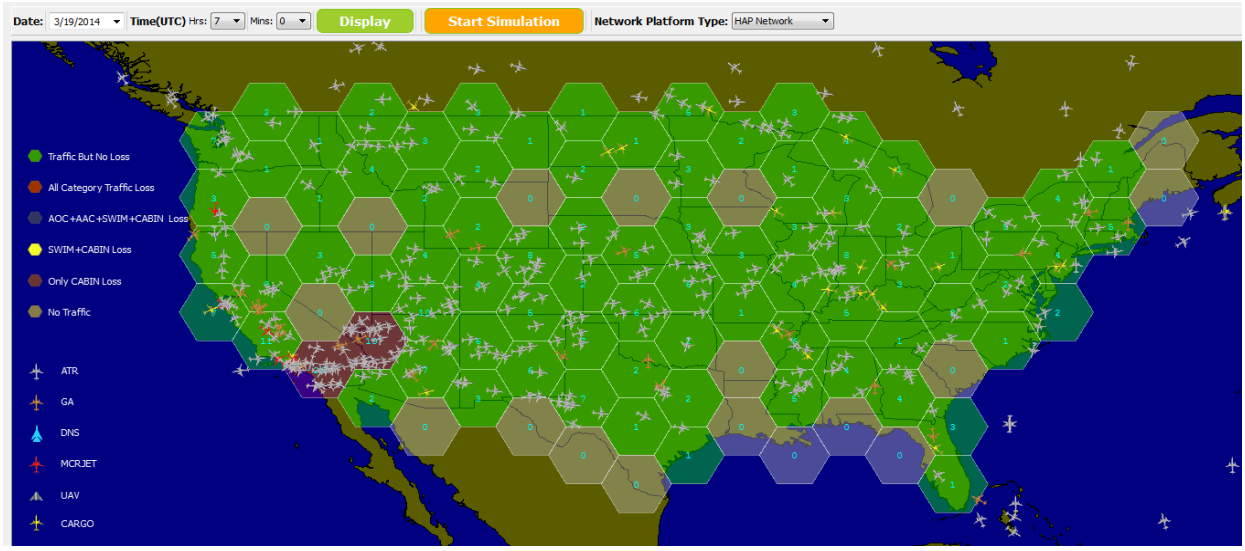


Figure 4-53 HAP Network Performance Statistics Display for Selected Time Instance

4.2.7.3.3. Satellite Network Display

In the Satellite Network display, about 100 spot beams covers the entire CONUS region as shown in Figure 4-54 the network is depicted as 4 degree by 4 degree spot beams, each with a channel capacity of 400 Mbps.

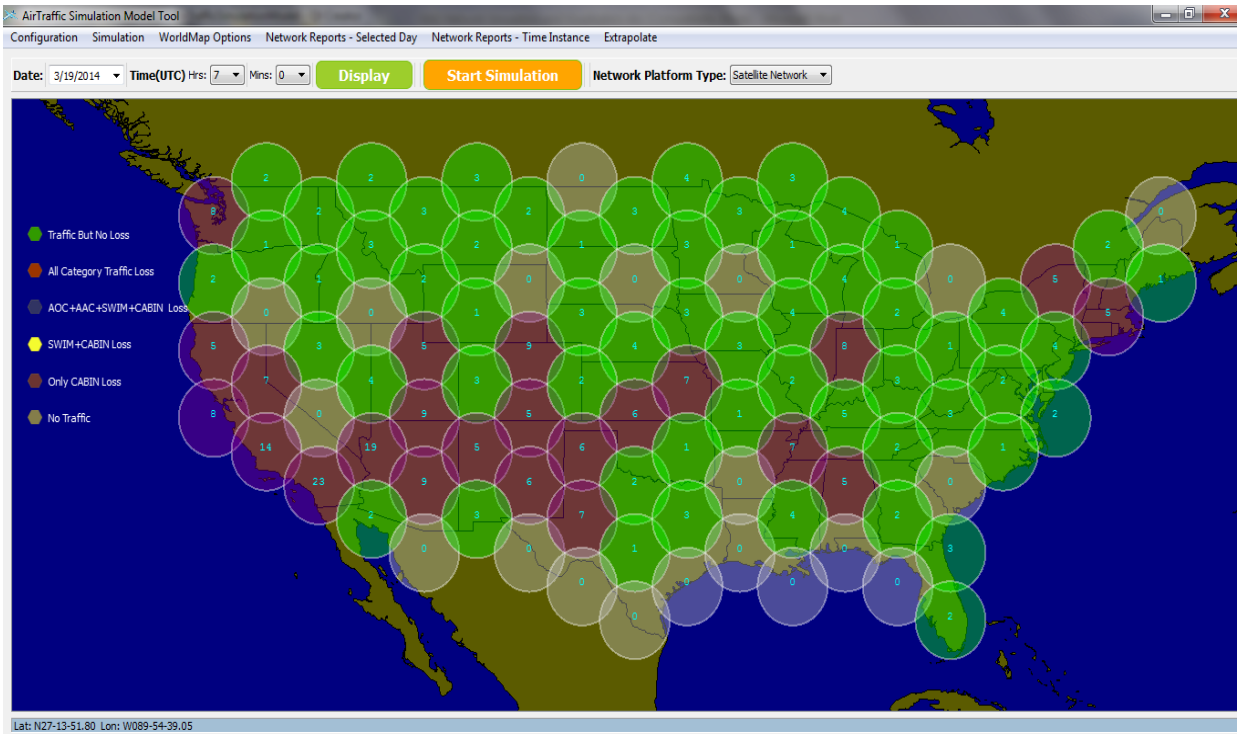


Figure 4-54 Satellite Network Performance Statistics Display for Selected Time Instance

4.2.7.3.4. Air-to-Air Network Display

In the Air-to-Air network, the CONUS region is covered with the 21 ground stations located at larger airports where air traffic control towers are present. Each aircraft has a range of 120 nm (range circle with 2 degree radius). The number of connected aircraft is dependent on the data traffic of the aircraft at each time instance. The connected aircraft are displayed in the color blue and the disconnected aircraft are displayed in the color red as shown in Figure 4-55.

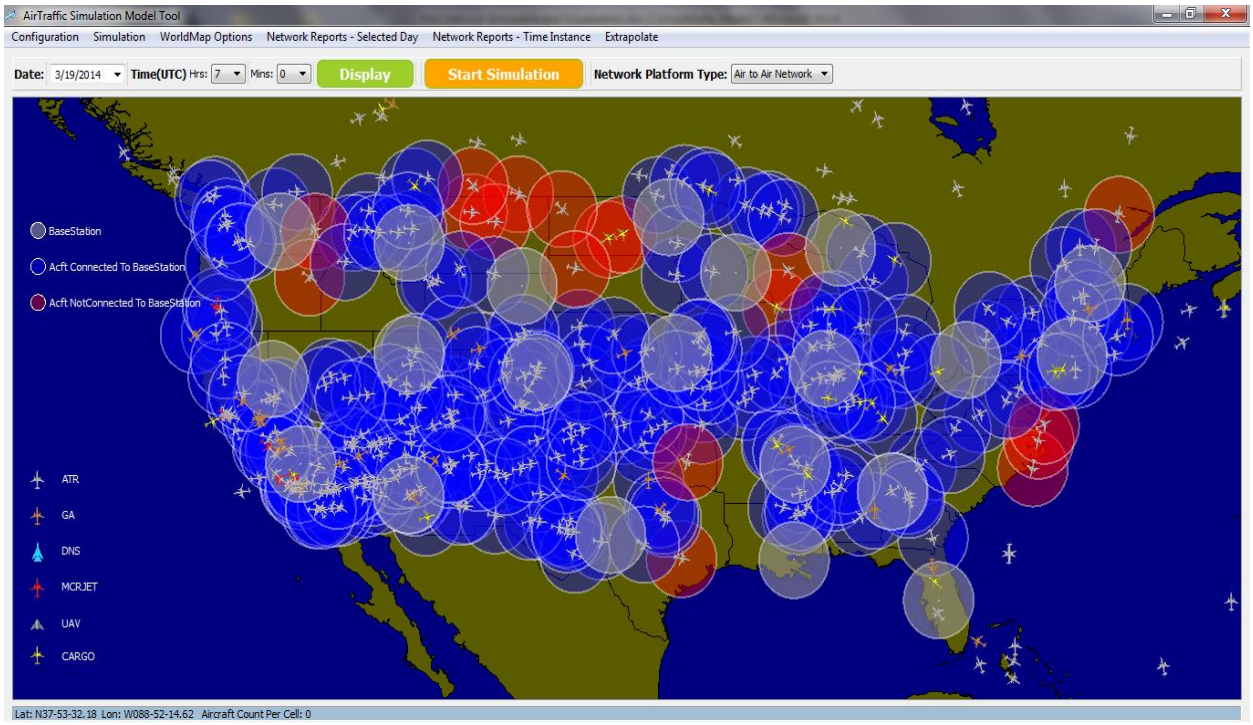


Figure 4-55 Air-to-Air Communication

The user can view the connected aircraft by selecting the Air to Air network connectivity under the Network Reports – Time Instance menu. It displays a window in which the total connected and disconnected aircraft counts are displayed. The paths can be generated from any aircraft to any airport with intended Maximum Hop count and Maximum number of paths. The aircraft call sign and one airport or all airports can be selected to generate the paths. The paths generated are displayed in a table as shown in the Figure 4-56.

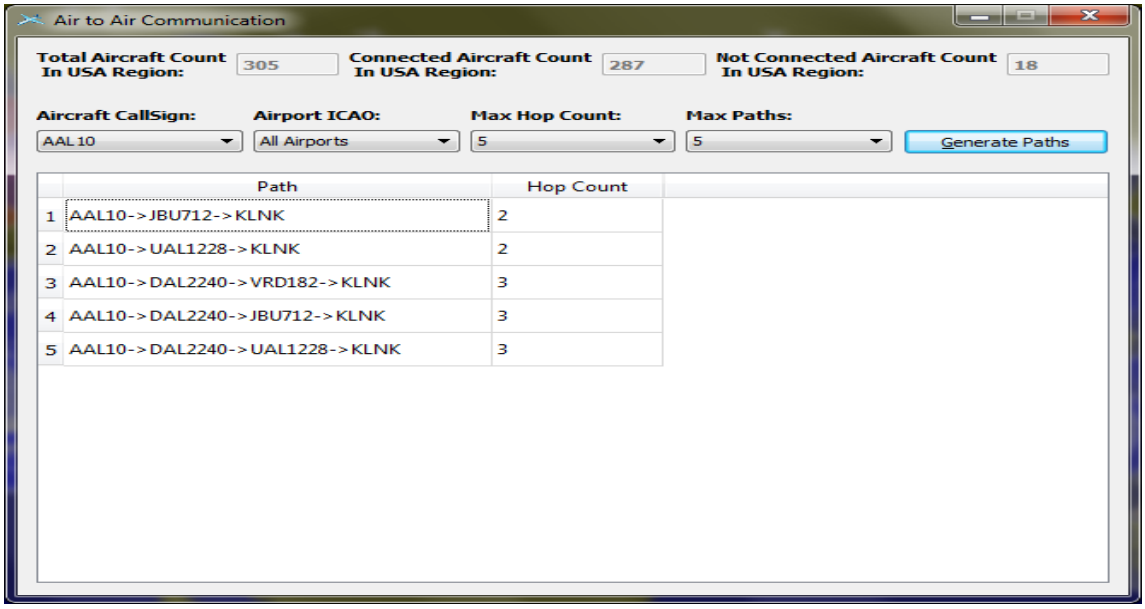


Figure 4-56 Air-to-Air Communication Generated Paths

Figure 4-57, Figure 4-58, and Figure 4-59 provide the displays of air-to-air network performance using the following types of links:

- VHF (Figure 4-57)
- L-band (Figure 4-58)
- FSO (Figure 4-59)

The number inside a Cell indicates the aircraft count and the number in braces in a Cell indicates the relay count of the grid. Relay count is the summation of the air traffic of the adjacent cells that are relaying traffic towards the cell. A legend showing different hex grid colors for different traffic options like Traffic but NO Loss, All Category Traffic Loss, AOC+AAC+SWIM+BROADCAST Loss, SWIM+ BROADCAST Loss, Only BROADCAST Loss and No Traffic Loss provides effective display for understanding the traffic load in different regions.

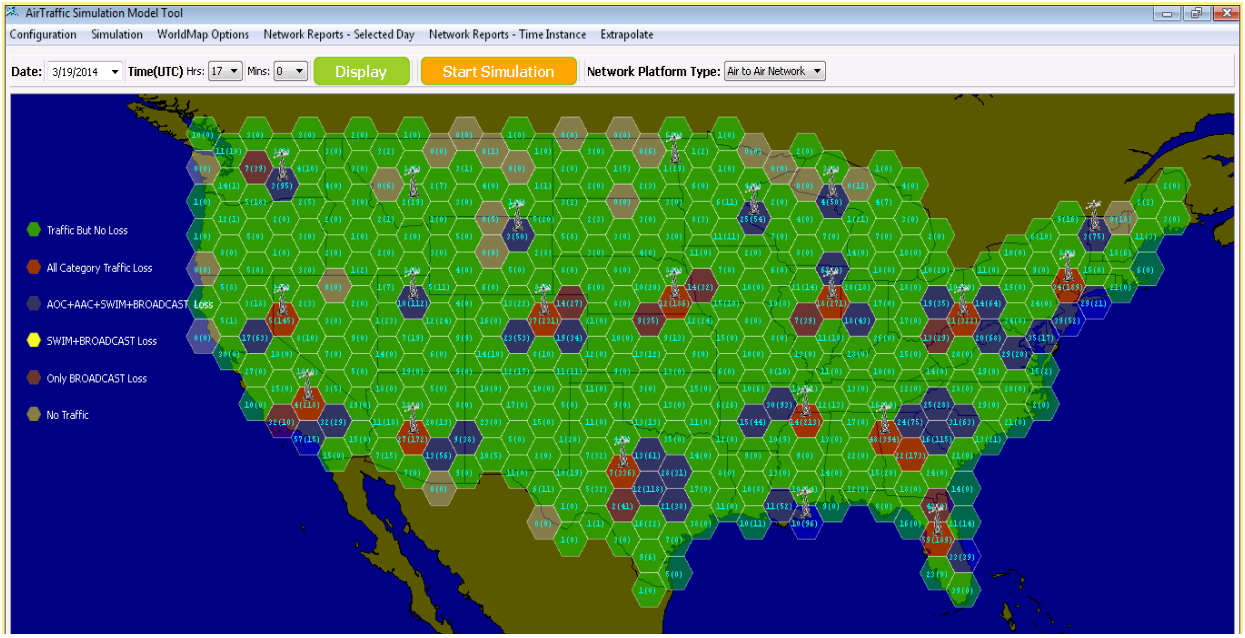


Figure 4-57 Air-to-Air Communication (VHF Air-to-Air Link)

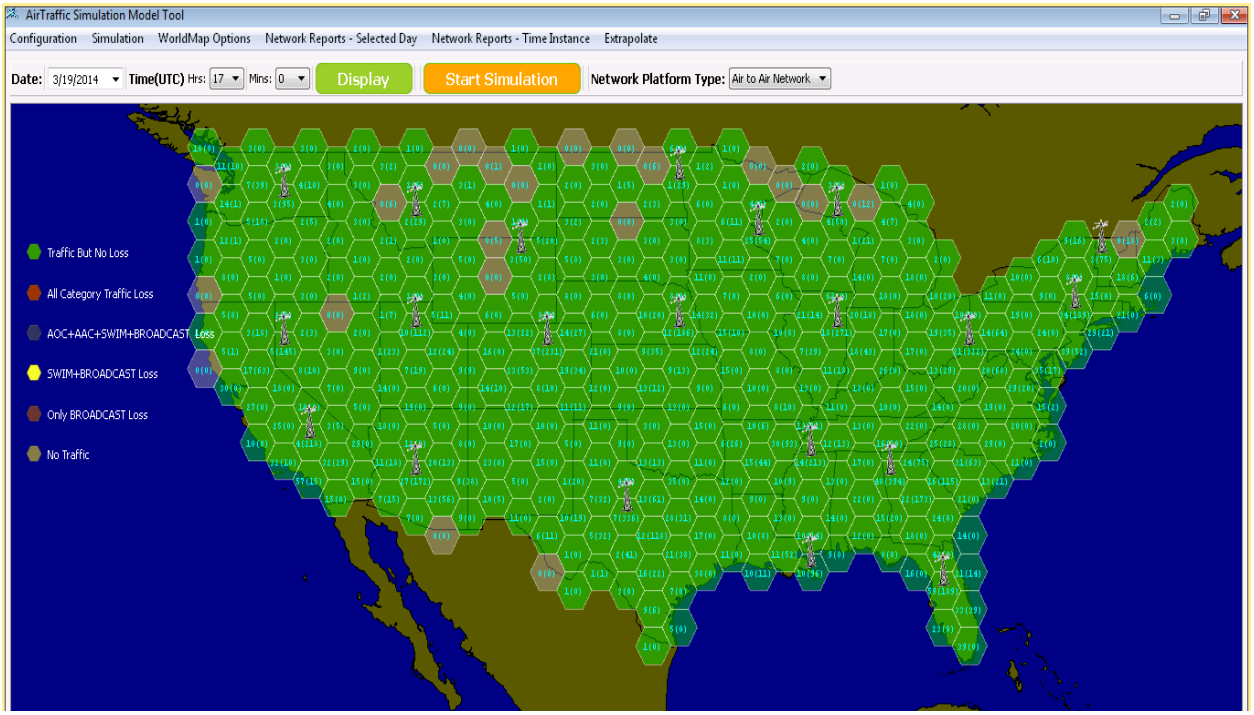


Figure 4-58 Air-to-Air Communication (L-band Air-to-Air link)

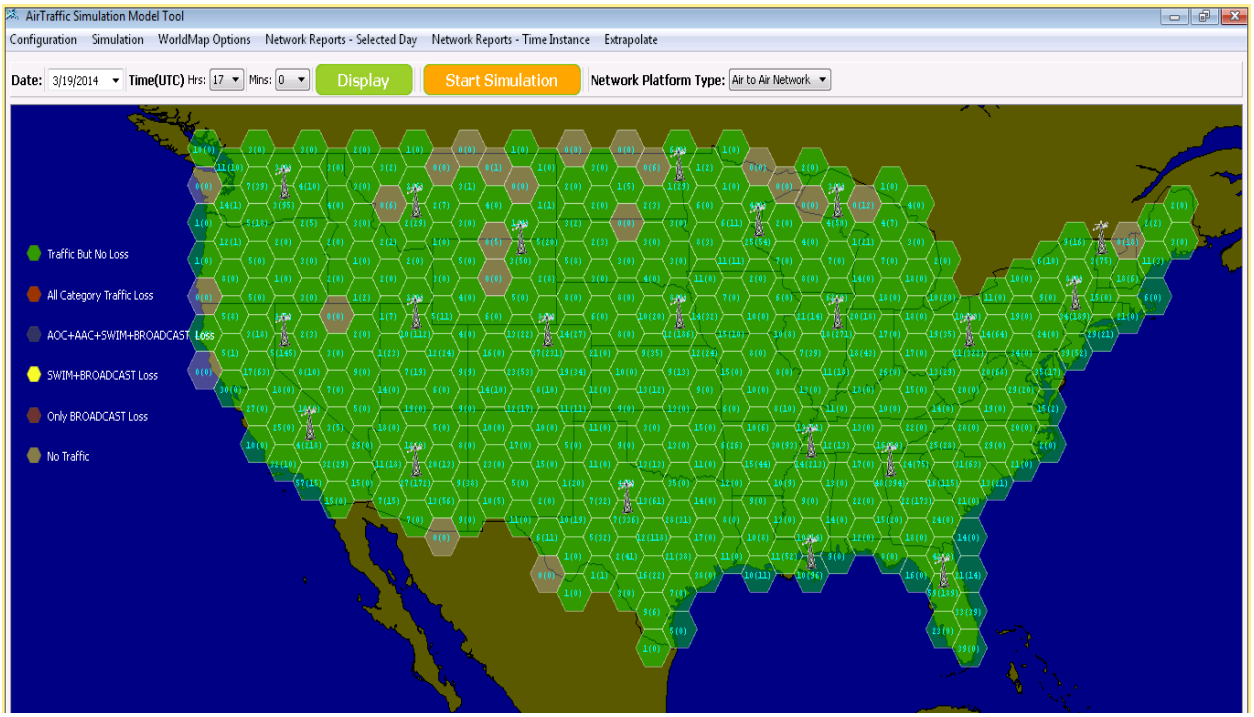


Figure 4-59 Air-to-Air Communication (FSO Air-to-Air Link)

4.2.8. Summary Analysis of Simulation Results

Table 4-14 gives a summary of the observations based on the simulation modeling analysis and results. Results explained above in section 4.2 are again summarized below.

- For Ground-based Cellular and HAP-based Cellular networks, no significant degradation is observed in latency for supporting aircraft traffic of up to 400 aircraft in a Cell.
- Latency is higher for geostationary satellite link owing to higher propagation delay, and may not be suitable for latency critical real-time applications.
- As HAP coverage is higher than ground-based coverage, higher link capacity is required between aircraft and HAP to support the larger aircraft count per cell.
- Optimum channel usage can be observed on the satellite spot beam network, owing to higher satellite coverage and higher number of aircraft served by the satellite.
- With ground-based cellular and HAP-based cellular networks, the majority of packet loss is observed on the AC ↔ BS link and AC ↔ HAP link, respectively, whereas SAT ↔ GW link is the bottleneck in the satellite network.
- Significant cabin and crew service degradation can be observed as the aircraft count per spot beam increases. APC traffic loss of 77% was estimated with as low as 5 aircraft per spot beam

Table 4-14 Simulation Analysis Observations

	Latency	Packet Loss
Ground-based Cellular	Low	No Loss of safety critical traffic in the network with up to 400 aircraft per Cell
HAP-based Cellular	Low	No Loss of safety critical traffic in the network with up to 400 aircraft per Cell
Satellite	Latency is higher owing to higher propagation delay	77% APC traffic loss even with as low as 5 aircraft per spot beam and SWIM traffic loss is observed with 50 aircraft per spot beam

5. SECURITY ASSESSMENT

Phase 1 activities in the NASA CDTI Project concluded that it might not be possible for a single technology or a platform to support the requirements of all airspaces and applications in a cost effective manner. For instance, the cost of deploying network platforms like Terrestrial towers, HAPs and Satellites would differ widely across airspaces such as oceanic, en-route, airport surfaces, etc, to achieve the required NAS datalink environment capabilities. Hence hybrid networks were recommended in phase 1 reports comprising multiple technologies and platforms. It is also envisaged that adapting some of the Commercial Off The Shelf (COTS) technologies for aeronautical commutations may become inevitable in the future, considering the merits of these technologies such as low cost systems, additional spectrum utilization, broader infrastructure support, etc. However, these adaptations may necessitate major security precautions for safety critical aeronautical applications. Hence, in phase 2 of the Project, security assessment was performed to identify and assess the safety threats to the communication infrastructure and make recommendations to address safety concerns.

5.1. APPROACH FOR SECURITY ASSESSMENT

Phase 1 reports predicted that the overall aeronautical network may span over both public and dedicated networks seamlessly and the boundaries between the networks will eventually disappear through 2060 timeframe. Aircraft will be using hybrid networks for safety critical applications such as air navigation, surveillance, Air Traffic Control (ATC) etc., which would demand higher levels of robustness and integrity from these networks, compared to requirements of regular commercial applications. The extended connectivity to public networks may also expose aircraft to all kinds of security threats in an open environment and hence, it becomes necessary to assess all security risks of aircraft in various architectures and recognize mechanisms to ensure their safety against the threats. Figure 5-1 illustrates the approach for security assessment performed as part of phase 2 activities.

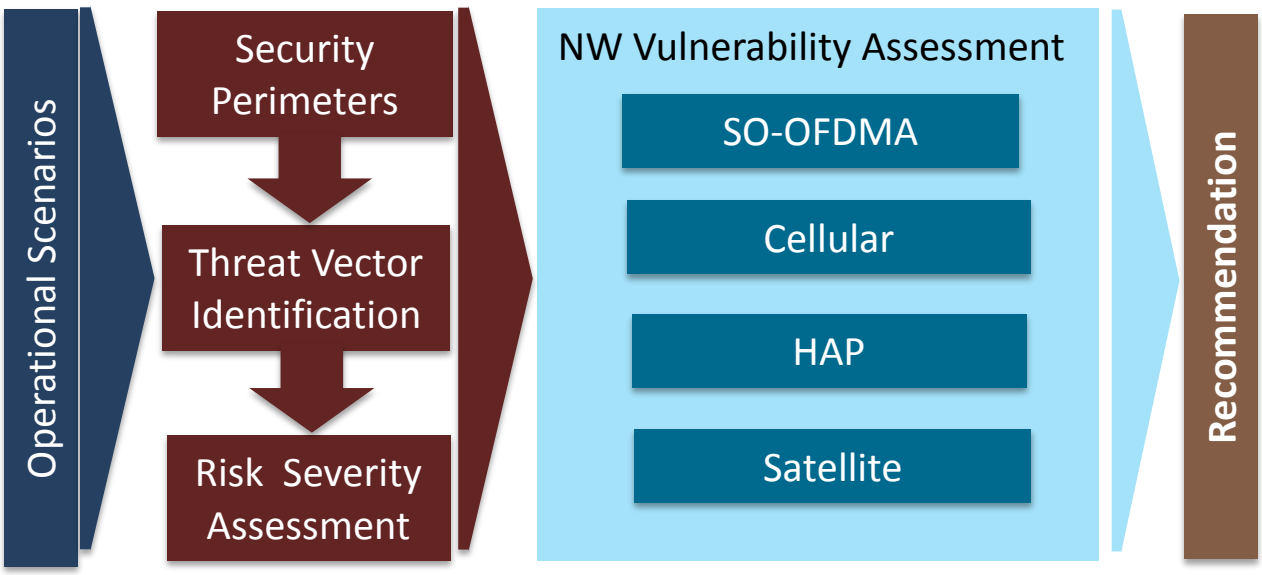


Figure 5-1 Approach for Security Assessment

The initial task starts with the identification of the security perimeters of networks. In the context of the aeronautical network, a security perimeter is considered as a boundary between a regulated network and an unregulated network. A perimeter could be a device or a network entity in the regulated domain that is visible to the attackers outside the regulated domain. Some of the examples of network perimeters are radios, gateways, applications, etc., which are accessible to the external world. The scope of this assessment is limited only to the architectures discussed in phase 1 reports and considered in section 4.

The next step is to identify the threat vectors such as mechanisms, paths and tools used by the intruders to attack the perimeters and gain access into the network and its critical information. Hence, in this task, all possible attacks to the networks are captured.

COCR safety assessment [REF-COCR] identified the top level operational hazards that may arise during the use of datalink services such as: 1) Loss of Service and 2) Loss of Data Integrity. Loss of Service is attributed to the network failure that inhibits communications between two aeronautical systems. Threats such as Denial of Service (DOS), jamming, flooding of messages, etc., may cause loss of communications in the NAS environment. Loss of Data Integrity refers to corrupted messages, wrongly delivered messages, late or missing messages and out-of-sequence messages that are delivered undetected. As most of the communication protocols are equipped with robust error-detection algorithms such as, 64/128-bit Cyclic Redundancy Checks, the probability of an accidentally corrupted message, passing through all layers of communication protocols undetected, is very remote. However, the attacks like man-in-middle, masquerading, etc., may cause intentional damage to the data integrity of the systems. This assessment mainly focuses on such intentional threats to datalink services, as most of the non-intentional interferences are covered in the earlier technology assessment reports published in phase 1 reports. See Task 2 report [TASK2RPT].

Table 5-1 provides the COCR assessment of hazard severity categorization for Loss of Service and Loss of Data Integrity for various datalink services and the safety objectives needed for risk free operations (COCR ATS Phase 2). Figure 5-2 provides a standardized hazard severity categorization per COCR.

Table 5-1 COCR Operational Safety Assessment and Safety Objectives for Datalink Services

Service Category	Loss of Service		Hazardously Misleading Information	
	Severity Class	Safety Objective	Severity	Safety Objective
Data Communications Management Services (DCM)	4	Probable	3	Remote
Clearance/Instruction Service (CIS)	3	Remote	2	Extremely Remote
Flight Information Service (FIS)	4	Probable	2	Extremely Remote
Advisory Services (AVS)	3	Remote	2	Extremely Remote

Service Category	Loss of Service		Hazardously Misleading Information	
	Severity Class	Safety Objective	Severity	Safety Objective
Flight Position/Intent/ Preference Service (FPS)	3	Remote	2	Extremely Remote
Emergency Information Service (EIS)	4	Probable	3	Remote
Delegated Separation Service (DSS)	3	Remote	2	Extremely Remote
Miscellaneous Services (MCS)	1	Extremely Improbable	1	Extremely Improbable

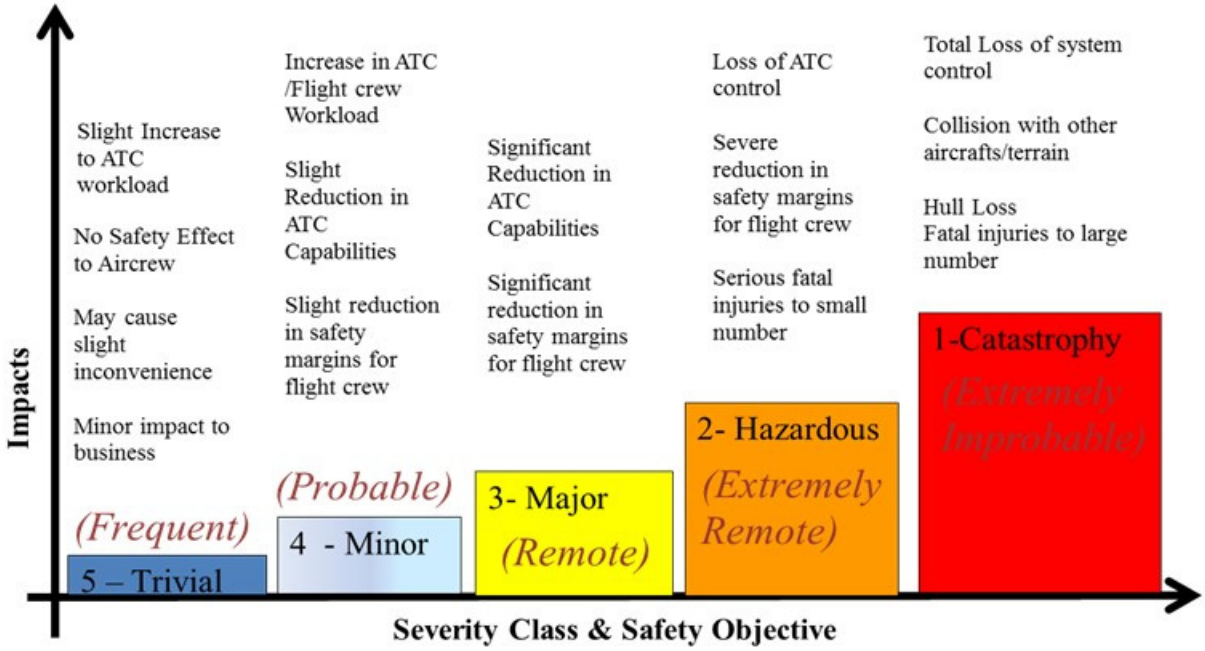


Figure 5-2 COCR Hazard Categorization

The severity levels of the hazards are different for various datalink services. For example, the hazard severity level of "Loss of Service" for "Data Management Service (DCM)" is "Minor", while it is "Catastrophic" for "Miscellaneous Service (MCS)". MCS comprises services such as "Autoexec" for controlling aircraft remotely from ground through datalink. Hence the requirements of MCS are more stringent than that of DCM. The safety objectives represent the degree of tolerance applicable to each class of hazard. Hazards of class 4 (Minor/Probable) category can occur more frequently than that of class 3 (Major/Remote) category, class 3

(Major/Remote) can occur more frequently than class 2 (Hazardous/Extremely Remote) and so on. Hence, if MCS service is deployed over a datalink, the loss of service should be "extremely improbable", but for DCM service "loss of service" can be "probable".

For the purpose of network vulnerability assessment, risks of various threats are assessed based on: 1) Threat Impact and 2) Required Capabilities to effect threats. Threat Impact is rated based on the potential damage that would be caused to NAS data exchange environment if the threat materializes. The score is given as a percentage of the estimated loss of communications to the overall NAS network infrastructure. For instance, if NAS extends over an area of 10 million square kilometers and if a threat causes outage over 1 million square kilometers, the Threat Impact score is 10%. The score for Required Capabilities is estimated based on the availability of technical and financial capabilities needed to cause the threat. If the required capabilities to implement a threat are high, then the chances for carrying out such attacks are unlikely and vice versa.

Finally the hazard score for a threat is calculated by multiplying "Threat Impact" and "Required Capabilities" as shown below.

$$Hazard\ score = \ Threat\ Impact\ \times Required\ Capabilities$$

Based on hazard probability score, the level for a hazard is classified into five categories as provided in Table 5-2

Table 5-2 Safety Hazard Level Classification

Hazard Score	Probability Level
<0.25%	Extremely Improbable
0.25% to 1%	Extremely Remote
1%-10%	Remote
10% - 25%	Probable
Above 25%	Frequent

The estimated hazard probability levels of various threats identified in a network are compared against the against the safety objectives of different datalink services as shown in
Table 5-3.

Table 5-3 Format of Threat Assessment for a Network

		Network 1		
Service Category	Loss of Communications Safety Hazard / Safety Objective	Threat 1	Threat 2	Threat 3
		Extremely Remote	Extremely Remote	Extremely Improbable
Data Communications Management Services (DCM)	Probable	No Threat	No Threat	No Threat
Clearance/Instruction Service (CIS)	Remote	No Threat	No Threat	No Threat
Flight Information Service (FIS)	Probable	No Threat	No Threat	No Threat
Advisory Services (AVS)	Remote	No Threat	No Threat	No Threat
Flight Position/Intent/ Preference Service (FPS)	Remote	No Threat	No Threat	No Threat
Emergency Information Service (EIS)	Probable	No Threat	No Threat	No Threat
Delegated Separation Service(DSS)	Remote	No Threat	No Threat	No Threat
Miscellaneous Services(MCS)	Extremel Improbable	Threat	Threat	No Threat

If a hazard probability level of a threat is higher than the safety objective needed for a datalink service, then the network may not be suitable to handle such datalink services and if it is the only network deployed in NAS, there could a possibility of safety hazards impacting NAS operations. For example, if the safety objective of MCS service is 1 (extremely improbable) and if there are threats in a network that have hazard levels at “Remote” or “Probable”, then that network alone cannot be deployed for MCS service. Thus the table gives an overall idea about the possible threats that can impact network safety and the suitability of the network to handle various datalink services.

The vulnerability assessment is done for the three network architectures identified in Phase -1 of the project namely, Cellular, Satellite and broad band Very High Frequency (VHF) networks. The susceptibility of various network architectures to support the required level of robustness for performing safety critical operations are compared and prioritized. Finally, the recommendations are made to mitigate the high priority threats and to improve the overall operations of the networks.

5.2. SCOPE OF ASSESSMENT

In the earlier days, the only possible mode of data transfer to an aircraft was through physical media such as, floppy diskettes or magnetic tapes and aeronautical-specific air/ground datalinks in closed systems dedicated to aeronautical-specific data transfer only. Hence, the aircraft’s security perimeter was confined to the physical boundaries of its closed datalink systems. However, in the recent years, with the deployment of new communication technologies and internet, the security perimeters have started expanding limitlessly, covering the entire globe virtually. Hence it becomes necessary to identify security perimeters at all levels to safeguard the aeronautical network against all threats. Figure 5-3 provides the overall context of security perimeters that are possible in NAS data exchange environment.

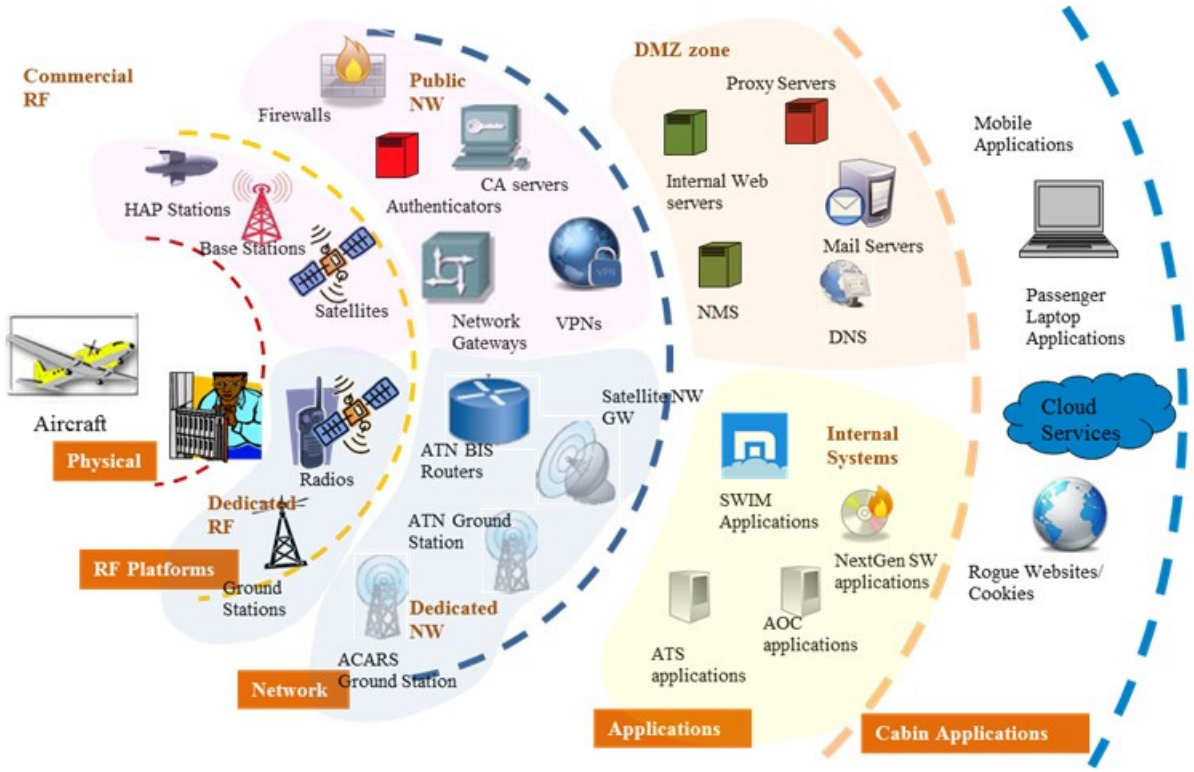


Figure 5-3 Context of Security Assessment

As shown in Figure 5-3, some of the security perimeters identified at various layers are provided below.

- Physical access to avionics
- Radios, Ground stations, Base stations, Satellite Ground stations etc,
- ATN routers/Gateways, ACARS Gateways, NextGen IP routers, Authenticators, VPN servers and other network devices that are accessible to the external world.
- All application servers and end nodes that communicate with ground peers.
- Proxy servers, DNS servers, Mail Servers and other servers in DMZ zones
- Cabin entertainment systems, passenger laptops, Tablets, mobile and virtually any device that communicates with the internet are potential security perimeters.

The scope of this assessment is limited only to the Air/Ground networks identified in Phase 1. Hence the assessment is performed only for RF Platform layer and Networking layer as identified in Figure 5-4.

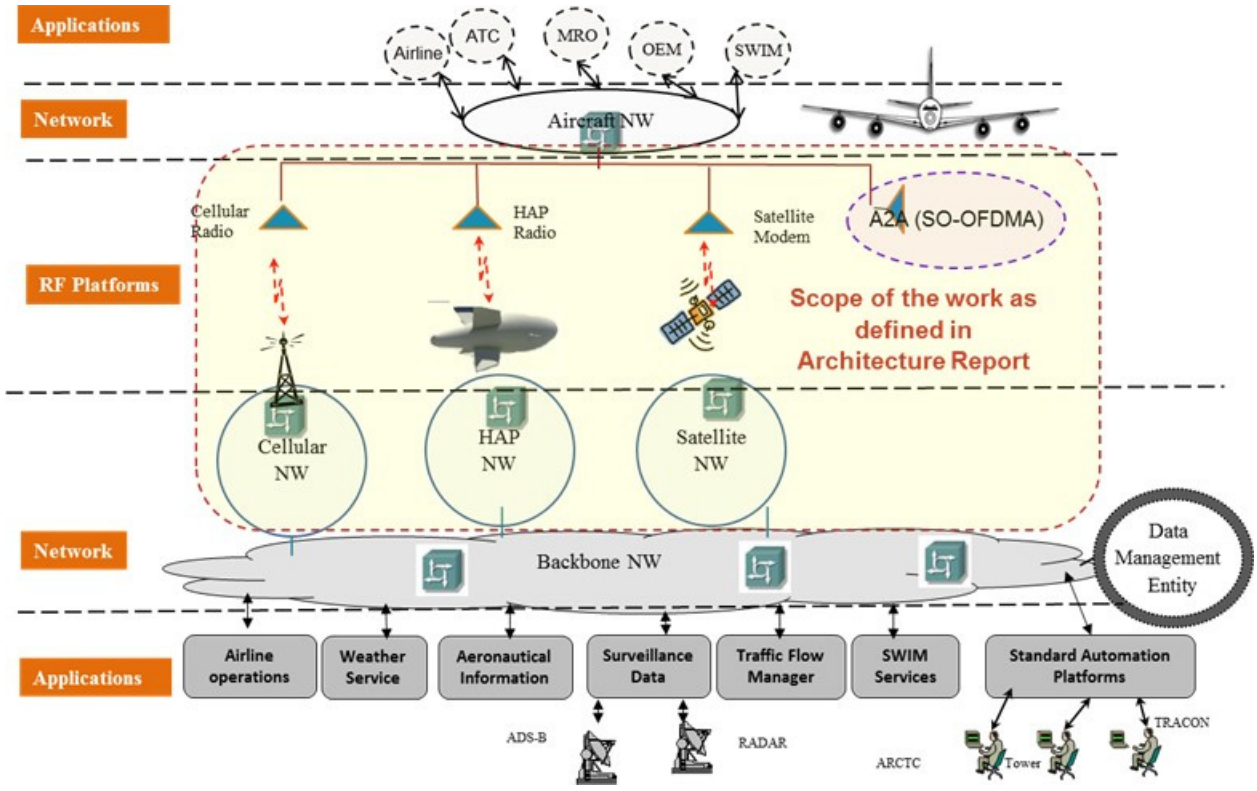


Figure 5-4 NAS Data Communication Environment

Considering, the overall NAS communication environment as provided in Figure 5-4, various network segments identified in the architecture are given below:

- Aircraft network supporting both safety critical applications and non-safety critical services.
- Air/Ground network providing connectivity to aircraft to reach ground network.
- Air-to-Air network that interconnects aircraft
- Ground-to-Ground backbone network that offers connectivity to ANSPs, Airline Operation Centers, ground sensors and other aeronautical services providers.
- Various Ground networks supporting ATC, AOC operations and other aeronautical services.

The assessment is done only for Cellular, HAP, Satellite and SO-OFDMA networks in the context of the architectures as defined in Phase 1 Task 3 Report [REF-TASK3RPT].

5.3. ASSUMPTIONS ABOUT NETWORK

The aeronautical network is expected to have multiple domains as shown in Figure 5-5. A domain represents a logical network entity, managed under a single administrative control or policy, but at physical level, a domain may span over multiple private/public networks and internet.

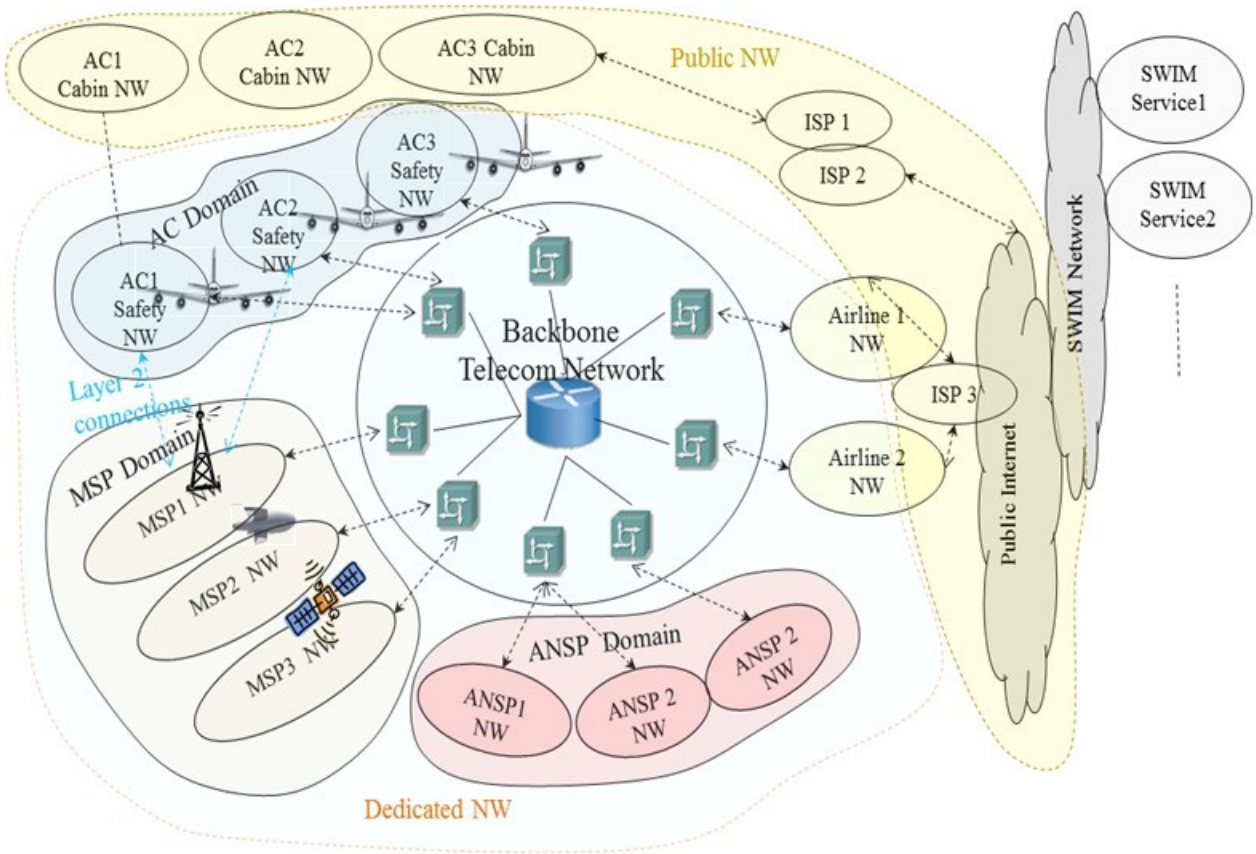


Figure 5-5 Network Domains

Some of the domains identified in Figure 5-5 are,

- Backbone network domain – managed by telecommunications service providers
- ANSP domain – managed by CAA and other Air Navigation Service Providers
- Mobile Service Provider (MSP) domain – managed by Air/Ground network service providers
- Airline Domain – Airline Private Network
- SWIM – Semi-regulatory network managed by SWIM service providers.
- Aircraft Autonomous Domain – airborne network.
- Cabin network domain

The assumptions considered in this analysis are:

- Air/Ground networks may provide layer 2 connectivity between aircraft and ground regulated network, with the network level traffic abstracted from the access network domains. Network level connection establishment between safety network domains may be handled transparent to MSP network.
- Multiple MSPs may exist in the future and the MSPs may deploy their services through public network infrastructure.

- Airborne network segments/devices may require simultaneous connectivity to multiple ground network domains such as ANSP, Airlines, SWIM services, etc.
- Airborne network will have appropriate security framework and the policies that govern both ingress and egress traffic in various domains.
- Inter/Intra domain routing protocol or any other similar routing mechanism will be deployed across the domains through secured control channels.
- Passenger traffic will be completely isolated from the avionics traffic so that the avionics network is invisible to the cabin network supporting passenger services.
- VPN/VLANs or similar security mechanisms may exist to establish secured connectivity through internets to the safety network on ground. The traffic within VPNs may not be visible to the entities in the public network.

These assumptions are common and applicable to all air/ground networks considered in this analysis.

5.4. ARCHITECTURE OPTION 1 – CELLULAR NETWORK

In this architecture, cellular network is used as an access network to connect aircraft with the ground side aeronautical network. The ground side network is a regulated network, while the access network is a public commercial network. Figure 5-6 shows a typical architecture of cellular network and the possible threat vectors that can act on it.

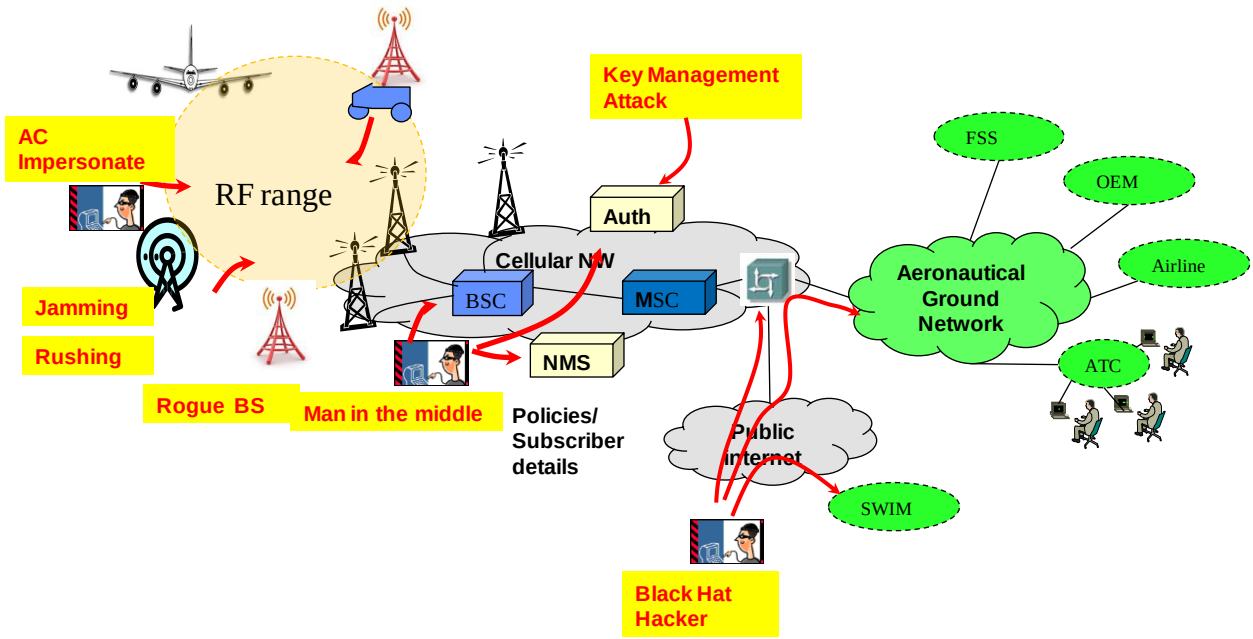


Figure 5-6 Security Threats to Cellular Network

In the future, commercial mobile service providers may offer air/ground service to aircraft in addition to offering services to their existing cell phone subscribers. As discussed in the Phase 1 Task3 report [TASK3RPT], the towers used for aeronautical communications may undergo minor modifications to accommodate communications with aircraft flying at high altitudes and with great

speeds. Other than this front end interface, all other portions of the network may remain the same between aircraft and cell phone users. Hence, beyond base stations, the data traffic from aircraft may pass through the same public network to reach the ground side aeronautical network. This exposes aircraft traffic to various threats and attacks similar to the ones present in the world of internet today. Of course, HAP-based cell towers are not shared with commercial cell phone users.

5.4.1. Threat Analysis

Various threats to the Cellular network are identified in Figure 5-6. The threats possible at RF level, Layer 2 access network and through public internet are discussed in this section.

5.4.1.1. JAMMING

Jamming refers to an intentional transmission of strong noise in order to disrupt the legitimate signal and degrade signal-to-noise ratio of the communication channel. There are commercial cell phone jammers available in the market for blocking mobile phone operations in the restricted areas. The range of jamming for such devices depends upon the strength of the noise generated by them. Generally, these commercial jammers may have shorter range impacting only a few cell phone users in a small area. Hence, practically, these jammers may not have any significant influence over aircraft communications, as aircraft fly at high altitudes and use high power for their communications, compared to the handheld devices, but there is a possibility to build high powered jammers using base station hardware. These jammers may affect a few aircraft in a range equivalent to that of a base station, however, only for a short time, as the current technology in subscriber stations enable them to scan continuously for adjacent base stations and logon to one as soon as its signals are clear and available. In the future, cellular networks may have technologies to handle jamming in a better way. So, in case of jamming, the interruption to aircraft communication is expected to be near-term problem. Considering these factors, loss of communication due to jamming is estimated around 70% of a single cell operation out of an estimated total of 200 cells in the NAS and the availability of capabilities to build such high powered jammer is foreseen as 90% considering the timeframe of 2060.

Hazard Level for "Loss of Communication" due to jamming in a cellular network is concluded as "***Extremely Remote***" (Hazard score: 0.32%). Jamming may not be able to cause "Loss of Data Integrity". Hence the hazard level for "Loss of Data Integrity" is concluded as ***"Extremely Improbable".***

5.4.1.2. SCRAMBLING

Scrambling is a technique in which jamming is done selectively on specific durations of communication to collapse the control flow between base stations and subscriber units. Scramblers may have implementations to understand the frame structure and send high powered short pulses to knock of specific portions of control frames or user frames that would cause maximum damage to the communication. Because of the short pulse transmission, jam-detection systems find these devices difficult to locate compared to the jammers that transmit noise continuously. Moreover scramblers consume lesser power than jammers owing to their intermittent transmission patterns. Hence scramblers could be very effective in causing outage in a cellular network. However, the implementation of a scrambler would require considerable amount of knowledge about the communication technology used in the cellular networks.

Nevertheless, since the cellular technology is a commercial technology and the "system on chip" concepts are more prevalent in the telecom industry, it may be possible to build scramblers with moderate efforts and funding.

Assuming a scrambler can inhibit a base station operation completely, the loss of communication is estimated to be 0.5% in NAS region (1 out of 200 cells in NAS) and the availability of required capabilities is estimated around 50% considering the amount efforts required to build a scrambler from the COTs hardware. Hence, the estimated hazard level for scrambling is "***Extremely Remote***". (Hazard score: 0.25%). Like jammers, scramblers are also expected not to cause any damage to data integrity, considering robust error-check protections available in higher layers and hence, the loss of data integrity is ***"Extremely Improbable".***

5.4.1.3. IMPERSONATING AIRCRAFT

In this attack, a hacker may use a commercial modem with fake aircraft credentials to gain access into the ground network and modify critical data to cause damage to NAS operations. However, mobile networks implement robust authentication mechanisms/algorithms based on digital certificates which are very difficult to break through. Hence gaining illegal access into the network may not be possible, unless the actual aircraft credentials are obtained. (Threats related to key management issues are discussed separately in section 5.4.1.5). But it is possible for a masquerading station to send continuous messages flooding the network and causing denial of service (DOS) to other genuine aircraft in the cell. Hence, Loss of communication using this technique is estimated around 10% in a cell which amounts to 0.05% considering the entire NAS region. The availability of capabilities required to cause such a threat is estimated around 90% (without aircraft credentials). Hence the hazard score for Loss of Service is estimated around 0.045% and its level is ***"Extremely Improbable".***

Even considering the possibility of gaining access to the ground network, NAS may have sufficient policy implementations for data access restricting an aircraft's visibility to NAS's critical data. At the maximum, the hacker may be able to send wrong information about the aircraft being masqueraded, but the hacker may not be able to modify any other data existing in the NAS network. Hence the extent of Loss of Data Integrity is estimated around 20% within a cell and the availability of required capabilities is estimated around 10% considering the difficulty in accessing aircraft credentials. Hence, Loss of Data Integrity score is 0.01% and its level is ***"Extremely Improbable".***

5.4.1.4. ROGUE BASE STATION

Rogue base stations may be used by miscreants to fake the legitimate base station in a region and gain access into aircraft networks. A rogue base station (BS) may listen to the identities and credentials of genuine base station and use them in its broadcast with higher signal power so that aircraft in that region are attracted towards the fake base station. The aircraft trying to logon to the fake base station may be vulnerable to attacks, as the hacker may gain access to aircraft network data. But most of the mobile networks use mutual authentication procedure during logon in which both the base station and the subscriber station (SS) authenticates each other before establishing connectivity. Since the fake base station is just replaying the credentials of an actual base station, it will not have the private secret keys or the unshared secrets required for authenticating itself with the SS. In the future, it can be assumed that mutual authentication would be mandatory in all

mobile networks during link establishment or handover procedures and hence it can be safely assumed that a rogue BS may not be able to break into the aircraft network. But the rogue base stations may cause a temporary denial of service, as it may cause multiple unsuccessful logon attempts at aircraft subscribers. However, as discussed earlier, an SS will look for alternate base stations after maximum logon attempts.

Hence a rogue BS may cause marginal loss to communications within a cell, with an approximate figure of 10% damage to a cell's communication. The capabilities availability is estimated around 80%. The overall loss of communication to NAS environment is calculated as a hazard score of 0.04% which is ***"Extremely Improbable".*** Unless the rogue BS has access to the credentials of a legitimate BS, it may not be able to cause any data integrity issue in the network. Even in extreme cases, where it has access to legitimate BS credentials, the extent of impact to data integrity would be limited to a few aircraft within a cell. Hence, the loss of data integrity is estimated around 0.5% (1 out of 200 cells) and the availability of such capability is estimated around 1% considering robust credential management infrastructure. The overall loss of data integrity to NAS is estimated as 0.005% and ***"Extremely Improbable***".

5.4.1.5. KEY MANAGEMENT ISSUES

The mobile networks use certificates that contain information about shared public keys along with cryptographic suites for data security. Future NAS environment may use multiple such certificates for various purposes like, authentication of different user categories like aircraft, airlines, ATC and other service providers, VPN security, application security, selective authorization for different regions, etc. Hence the industry may develop a robust framework for issuing and managing these certificates. The NASA data exchange architectures discussed in Phase 1 Reports assume a common authentication framework in the ground side regulated network to authorize aircraft to use the networks. The front end access networks do not perform authentication by themselves, but pass the logon credentials to a common authenticator located in the regulated network at the back end. Based on the decision from the common authenticator, the access networks either allow or reject logon requests from aircraft. Such a centralized mechanism would help to avoid variations in the security procedures deployed across access networks compromising the security doctrines laid out for aeronautical applications.

The management of such centralized infrastructure for issuing keys, transferring private secrets securely to the network entities, management of the certificate validities and signing authorities, etc., requires greater level of safety precautions. Any illegal access to the key management infrastructure may permit miscreants to have access or to modify any level of critical data in NAS, and thereby causing catastrophic damage to the overall operations of NAS. The extent of damage to NAS operations is estimated around 80%. However it is presumed that the centralized key management infrastructure would be well protected and it would be highly impossible to break into the system. Hence the capability available for such an act is estimated around 0.1%. Since the key loss may cause both Loss of Communication and Loss of Data Integrity, the final hazard core of 0.008%, which is ***"Extremely Improbable".***

It is also theoretically possible that the aeronautical security framework may evolve independently without including public access networks within their scope of control. In such cases, aircraft may have to use public network credentials to logon to the front end public network and then use the

credentials corresponding to the aeronautical network to log into NAS infrastructure. If there are multiple access networks deployed in the system, aircraft may need to contain that many number of certificates corresponding to each service provider and manage them accordingly. However such implementations are not presumed to be deployed for safety critical services, as the aeronautical security framework is expected to include access networks' safety within its scope of control. Hence, such architecture is not considered in this analysis.

5.4.1.6. MAN-IN-MIDDLE

Man-in-Middle threat considers the scenario where a hacker is present inside the cellular network. The hacker may attack network elements such as routers, firewalls, authenticators or network managers in order to bring down the network. He may also intercept the messages flowing through the network, modify them or divert them to wrong destinations to create confusion in the communication. Since cellular network is a commercial network, there are good chances for commercial network infrastructure being managed by multiple smaller sub organizations. This increases the possibility for an intruder to get into the network from these organizations. Moreover, even a common security breach in such public networks may impact aeronautical communications though the target of the attacker may not be the aeronautical communications. However, the aeronautical messages are expected to be encrypted and secured when they pass through public networks using VPN or any other security mechanisms. Hence the hacker may not be able to intercept and tamper the aeronautical messages, but he can cause denial of service by dropping the packets illegally.

Considering the motivation of a hacker to cause outage in the entire network, the estimated worst case impact that would impact the aeronautical communications before the affected network is brought back to control is considered as 20% and the availability of capabilities to cause such impact is estimated around 2% considering the difficulty in getting into the network and gain access to its critical resource, but insignificant impact to data integrity is anticipated. Hence the hazard level for Loss of Communication is ***"Extremely Remote"*** (0.4%) and Loss of Data Integrity is ***"Extremely Improbable".***

5.4.1.7. BLACK HAT HACKER

As shown in Figure 5-6, the cellular network is connected to the Internet. Hence, any random black hat hacker from the Internet community may try to attack the cellular network. If the attacker gains access to the cellular network gateway, the hacker may try to hack into aeronautical network and cause interruption to its communications. Generally this type of attack is similar to the attacks being carried out on enterprise networks. There are commercial solutions available in the market to handle such attacks. However, it may not be possible to eliminate such attacks on cellular networks completely as they are exposed to the Internet. Hence the aeronautical network may need to deploy sufficient tools, software and processes to monitor such attacks and to take corrective actions.

Assuming sufficient preventive mechanisms are deployed in the network, the expected loss of communication and loss of data integrity to aeronautical communications due to such attacks in the cellular network are considered negligible. Hence the hazard levels are estimated as ***"Extremely Improbable"*** for both "Loss of Communications" and Loss of Data Integrity".

5.4.2. Risk Assessment

Table 5-4 and

Table 5-5 contain consolidation of the threats analyzed in the above sections.
The overall risks associated with the cellular networks to handle various datalink services are consolidated in Table 5-6 and Table 5-7.

Table 5-4 Hazard Assessment for Loss of Communications in Cellular Network

Threat Vector	Description	Estimated Loss of Bandwidth		Access to Required Capabilities		Loss of Communication	
		Score	Remarks	Score	Remarks	Score	Level
Jamming	A strong noise transmitted to affect the legitimate signal to cause denial of service to aircraft in that region	0.35%	70% of the cell affected due to Jamming. 200 cells in NAS	90.00%	Cellular Jammers are commercially Available	0.32%	Extremely Remote
Scrambling	Selective jamming of a specific frames / parts of a frame Knowledge of the frame structure known to scrambler	0.50%	1 cell affected. 200 cells per NAS	50.00%	May be difficult to build. But COTS HW can be used.	0.25%	Extremely Remote
Impersonating Aircraft (AC)	Hacker uses a legal Mobile Device with AC credential to impersonate AC and gain illegal access to the network.	0.05%	Hacker causes Denial of Service At least to 10% of aircraft in a cell	10.00%	Difficult to get AC credentials	0.01%	Extremely Improbable
Rogue BS	The ground station or Base station faked by a Rogue Station. Rogue Station listens to BS ID and other credentials and uses them in its broadcast with higher power so that Mobiles Stations are attracted towards it.	0.05%	10% reduction in the bandwidth. Mutual Authentication will inhibit AC logging into BS. DOS is possible.	70.00%	BS credentials difficult to get. Score for BS without credentials.	0.04%	Extremely Improbable
Key Mgmt issues	Loopholes in key or credential management infrastructure leading to security breach on a large scale.	80.00%	Major issue. May impact the entire NAS.	1.00%	Very difficult to manipulate credentials	0.80%	Extremely Remote
Man in the Middle	Hacker is inside the cellular network and attacks network element such as authenticators, routers, network managers, etc., to divert the messages or corrupt the data or cause DOS	20.00%	This can be a major issue. The Hacker may bring down the entire cellular network.	2.00%	Assumed to be difficult for Hacker to be present inside cellular network	0.40%	Extremely Remote
Black Hat Hacker	Since cellular network is a commercial network it has access to internet. Hence any random hacker from internet anywhere may try to attack the gateways to ground side network.	2.00%	Estimate impact is 2% to AC communication. This is similar to enterprise network hacking.	5.00%	Similar to enterprise network	0.10%	Extremely Improbable

Table 5-5 Hazard Assessment for Loss of Data Integrity in Cellular Networks

Threat Vector	Description	Estimated Impact to Data Integrity		Access to Required Capabilities		Safety Hazard	
		Score	Remarks	Score	Remarks	Score	Level
Jamming	A strong noise transmitted to affect the legitimate signal to cause denial of service to aircraft in that region	0.01%	CRC checks at every layer are very robust against data corruption	90.00%	Cellular Jammers are commercially Available	0.0045%	Extremely Improbable
Scrambling	Selective jamming of a specific frames / parts of a frame Knowledge of the frame structure known to scrambler	0.01%	CRC checks at every layer is very robust against corrupted data	50.00%	May be difficult to build. But COTS HW can be used.	0.0025%	Extremely Improbable
Impersonating AC	Hacker uses a legal Mobile Device with AC credential to impersonate AC and gain illegal access to the network.	0.10%	Masqueraded AC may send wrong information but cannot modify critical NAS data. 20% of AC data within to a cell	10.00%	Difficult to get AC credentials	0.01%	Extremely Improbable
Rogue BS	The ground station or Base station faked by a Rogue Station. Rogue Station listens to BS ID and other credentials and uses them in its broadcast with higher power so that Mobiles Stations are attracted towards it.	0.50%	Masqueraded BS may send wrong information but may not be able to modify critical NAS data. 100% of AC data within a cell	1.00%	BS credentials difficult to get. Score for BS with credentials.	0.01%	Extremely Improbable
Key Mgmt issues	Loopholes in Key or credential management infrastructure leading to security breach on a large scale.	80.00%	Major issue. May impact entire NAS.	0.10%	Very difficult to manipulate credentials	0.08%	Extremely Improbable
Man in the middle	Hacker is inside the cellular network and attacks network element such as authenticators, routers, network managers, etc., to divert the messages, corrupt the data or cause denial of service to all Aircraft.	2.00%	May corrupt 10% of Cellular Network information (5 service providers assumed)	0.20%	Assumed to be difficult for Hacker to be present inside cellular network	0.0040%	Extremely Improbable
Black Hat Hacker	Since cellular network is a commercial network it has access to internet. Hence any random hacker from internet anywhere may try to attack the gateways to ground side network.	2.00%	10% of a network population	0.50%	Similar to enterprise network	0.01%	Extremely Improbable

Table 5-6 Risk Assessment for Loss of Communication in Cellular Network

Service Category	Loss of Communications	Jamming	Scrambling	Impersonating AC	Rogue BS	Key Mgmt issues	Man in the middle	Black Hat Hacker
	Hazard Level → Safety Objective	Extremely Remote	Extremely Remote	Extremely Improbable	Extremely Improbable	Extremely Remote	Extremely Improbable	Extremely Improbable
Data Communications Management Services (DCM)	Probable	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Clearance/Instruction Service (CIS)	Remote	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Flight Information Service (FIS)	Probable	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Advisory Services (AVS)	Remote	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Flight Position/Intent/ Preference Service (FPS)	Remote	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Emergency Information Service (EIS)	Probable	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Delegated Separation Service (DSS)	Remote	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Miscellaneous Services (MCS)	Extremely Improbable	Threat	Threat	No Threat	Threat	No Threat	No Threat	No Threat

Table 5-7 Risk Assessment for Loss of Data Integrity in Cellular Network

Service Category	Misleading Information	Jamming	Scrambling	Impersonating AC	Rogue BS	Key Mgmt issues	Man in the middle	Black Hat Hacker
	Hazard Level → Safety Objective	Extremely Improbable	Extremely Improbable	Extremely Improbable	Extremely Improbable	Extremely Improbable	Extremely Improbable	Extremely Improbable
Data Communications Management Services (DCM)	Remote	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact
Clearance/Instruction Service (CIS)	Extremely Remote	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact
Flight Information Service (FIS)	Extremely Remote	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact
Advisory Services (AVS)	Extremely Remote	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact
Flight Position/Intent/ Preference Service (FPS)	Extremely Remote	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact
Emergency Information Service (EIS)	Remote	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact
Delegated Separation Service (DSS)	Extremely Remote	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact
Miscellaneous Services (MCS)	Extremely Improbable	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact

Some of the conclusions of this assessment are given below.

- RF jamming and man-in-middle attacks are the major threats to cellular networks to cause loss of communication to critical datalink services. However the impact of jamming may not be severe owing to multi-carrier broad spectrum communication. The future cellular networks are expected to develop jamming proof mechanisms to minimize such vulnerabilities.
- The following services can be deployed over cellular networks without major issues.
    - Datalink Communication Management (DCM)
    - Flight Information Service (FIS)
    - Emergency Information services (EIS)
    - Clearance Instruction Service (CIS)
    - Advisory Service (AVS)
    - Flight Position/Intent/Preference Service (FPS)
    - Delegated Separation Service (DSS)
- MCS services like Autoexec applications that are used to control aircraft remotely from ground using datalinks, may require higher level of network robustness and hence they are vulnerable to most of the threat vectors identified for cellular networks. Hence, the cellular network alone may not be able to support such datalink services.

5.5. ARCHITECTURE OPTION 2 – SATELLITE NETWORK

The architecture option 2 based on satellite networks is shown in Figure 5-7. The major components of a satellite network are: 1) GEO satellites that orbit around the earth at an altitude of approximately 35,786 Km above the sea level, 2) earth feeder stations to provide connectivity between satellites and ground stations and 3) aircraft modems to provide communication between satellites and aircraft. Beyond Ground Earth Stations, the network may use telecom infrastructure or the Internet to connect to the ground side aeronautical network or any other enterprise network. The satellite network is expected to provide network connectivity to both safety critical datalink applications and passenger applications.

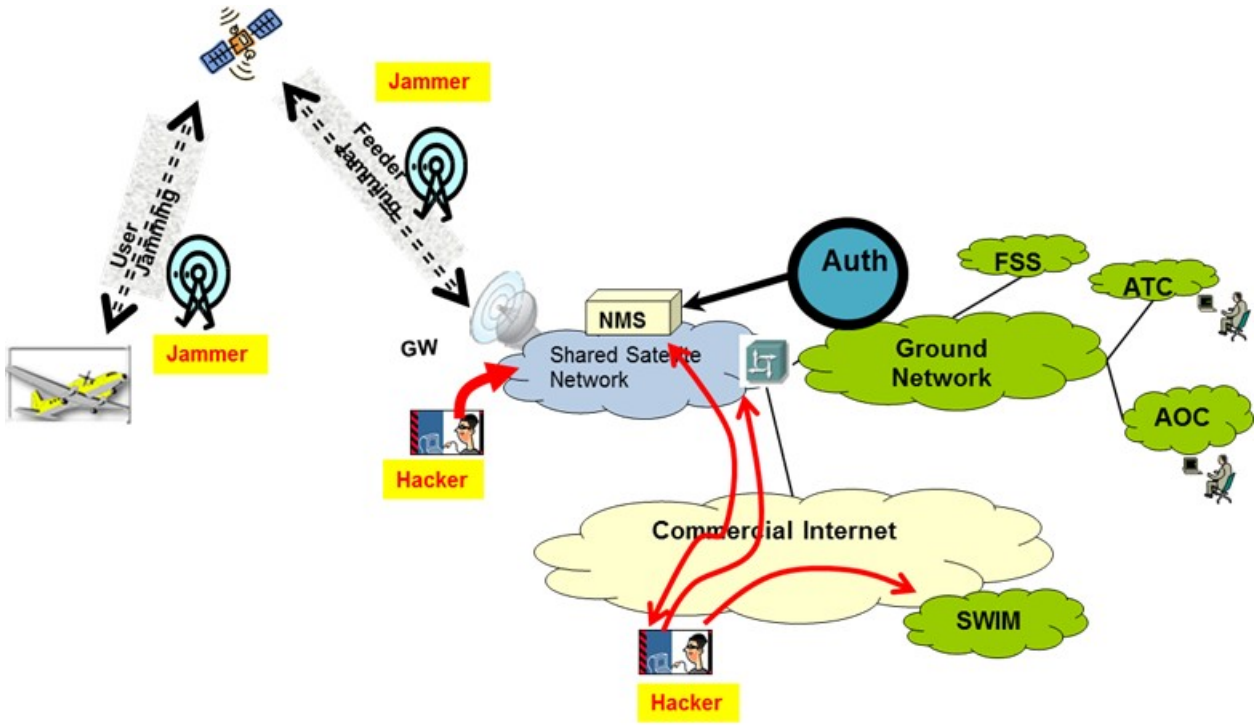


Figure 5-7 Security Threats to Satellite Network

Future GEO stationary satellites may use Ka band predominantly for both forward (satellite-to-aircraft) and return links (aircraft-to-satellite). The NAS region may have 75 to 100 spot beams spanning over an area of around 133,000 square kilometers. The US region may be supported by a pair of Ground Earth Stations for redundancy purposes, while the entire world may have three pairs of Earth Stations. Therefore, the entire aircraft data traffic over NAS region would be consolidated through a pair of feeder links towards the ground network. As the satellites are located at high altitudes, their communications would require phenomenal transmission power and focused directional beams. Such high power is required to compensate for the signal attenuation due to huge path loss over the long distance. Normally, the transmission power of feeder links will be at least ten times greater than that of spot beams. Typical path loss in Ka band for Geo satellite communication would be around 215 dB. Ka band also suffers from weather conditions that impact signal transmissions further.

5.5.1. Threat Analysis

Figure 5-7 shows possible major threats to satellite networks such as, signal jamming in feeder links and user links, man-in-middle attacks in the ground portion of satellite network and black hat hacker attacks from the Internet. Jamming threat is analyzed in detail in the following subsections, while man-in-middle and black hat hacker attacks are similar to the ones explained in section 5.4.

5.5.1.1. JAMMING

GEO satellites may be viewed as difficult systems to jam, as they are placed at very high altitudes. Simple ground based jammers with omni-directional antennas will never be able to interrupt the signals at GEO satellites, owing to tremendous path loss. Jammers would require millions of watts

of noise to reach the satellites, compensating path loss and other miscellaneous losses during their propagation. Practically, it is impossible to achieve such a high transmission power. However, satellites expose more wireless links to jammers such as, feeder uplinks/downlinks and user uplinks/downlinks, providing more vulnerable points for attacks. Moreover, technologies like, directional antennas, Unmanned Air Vehicles (UAVs) high power sources, etc., are expected to become commercially available in the 2060 timeframe and hence, the attackers would be capable of using such technologies in the future to develop sophisticated devices for jamming satellite systems. Some of the jamming techniques that could be deployed against satellite networks are explained below.

1. Full Barrage

   In this attack, random noise is generated across the entire transmission spectrum to degrade satellite link performances. These jamming devices can be easily implemented, but the power requirements of such devices would be extremely high.

2. Partial Jamming

   This technique uses power optimally to generate noise in a limited portion of the operational spectrum. Hence, partial jamming may cause more degradation to a communication link performance compared to full barrage jammers.

3. Single Tone:

   Single tone jamming can be very effective against systems that use single carrier frequency for their transmissions, but the advanced satellite systems are expected to be based on multiple carrier frequencies and use spread spectrum for their communications. Hence, the impact of such jammers to modern satellite systems would be very negligible.

4. Pulsed Multi-Tone

   In pulsed multi-tone jamming, random short pulses with high power and small duty cycle are generated across the entire operating spectrum to jam the signals in the communication link. This techniques uses power very optimally. Hence it can be one of the most effective techniques to cause large impact to satellite communications using less power.

5. Follower

   In this technique, the jammer understands signals, underlying communication technologies, frequency hopping, and other anti-jamming techniques implemented in the transmitter to jam its signals. Hence the follower can be very effective, even against devices that have anti-jamming techniques implemented. However, these kinds of systems would be very difficult to implement, as high technical capabilities are required to develop them.

A satellite network has at least three network devices that are exposed to jamming attacks. They are receivers at satellite, aircraft and ground earth stations. The following subsections explain the potential jamming attacks possible on these devices.

5.5.1.1.1. Threats to Receivers at Satellites

The footprint of a GEO satellite is very large, as it covers over 35% of total earth's surface. Therefore, geometrically, GEO satellites can be easily targeted by an attacker, as he would be able to jam the main lob of the transmitted signals even from a region located outside US boundaries. However, the power required to jam these signals at satellites would be immensely high due to the propagation loss of around 215 dB to the signal. Without directional antennas, even to create a noise power of -150 dBm/Hz at satellite receivers, the amount of transmission power required on ground level would be equivalent to 70dBm/Hz. If a bandwidth of 1 GHz is considered, the total power requirement would be 160 dBm (more than a billion kilowatt!!). Hence, it may not be possible to affect signals at satellites without using directional antennas.

As shown in Figure 5-8, a jammer may choose to attack a feeder link or a user link. To attack a feeder link, the jammer would require transmitters with very high power and large directional antennas, similar to the ones used in ground earth stations, to focus noise transmissions towards GEO satellites accurately. Hence, the required equipment capabilities are very high and unless funded by government agencies or huge organizations, acquiring such technical capabilities would be impossible. Hence it is concluded that jamming feeder uplink signals would be very difficult.

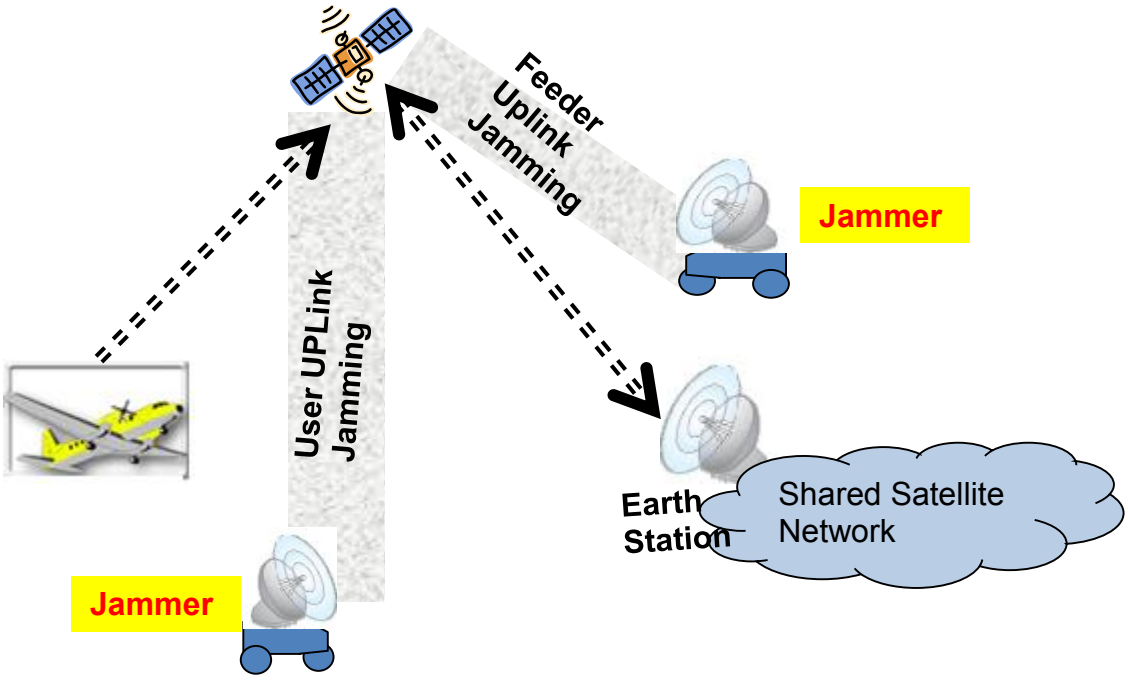


Figure 5-8 Jamming at Satellites

For user link jamming, equipment similar to aircraft modems could be deployed. Such equipment may be easier to acquire, but its impact to overall communications would be marginal.

Table 5-8 summarizes different jamming techniques and their impact to receivers at satellites.

Table 5-8 Impact of Jamming on Receivers at Satellites

Impact on Receivers at Satellites				
Jamming Technique	**Description**	**% of Loss of Bandwidth**	**% of Loss of Data Integrity**	**Remarks**
Full Barrage	Noise generated in the entire communication band to interrupt the signal receptions	0.01%	0.0001%	It is practically impossible to generate huge power to jam satellites, as they are located at very high altitude
Partial Spectrum	Attacker chooses a part of operational spectrum to jam.	0.50%	0.0001%	If directional antennas are used and feeder links are targeted, it may cause very minimal degradation to communications. Assumption 1% of the spectrum targeted and 50% effectiveness
Single Tone	A single carrier frequency is targeted and corrupted.	0.10%	0.0001%	Most of the satellite system would use multi carrier communication. Hence the impact is considered to be very less.
Pulsed Multi Tone	High strength pulses spread across the operational spectrum transmitted. Uses power in an effective way.	10%	0.0001%	May cause considerable amount of degradation if feeder link is affected. Assumption is based on the usage of directional antennas and high powered transmitters.
Follower	Equipage similar to ground stations used. Follower can understand the signal, technology, anti-jamming mechanism and follows transmitters and its frequency hops in order to spoil the reception	20%	0.0001%	Can be very effective, but, very complex to implement. 20% degradation assumed considering the usage of equipment levels similar to Ground Earth Stations.

5.5.1.1.2. Threats to aircraft receivers

The possible scenarios of jamming aircraft modems are provided in Figure 5-9. Aircraft receivers can be jammed either from ground or from UAVs.

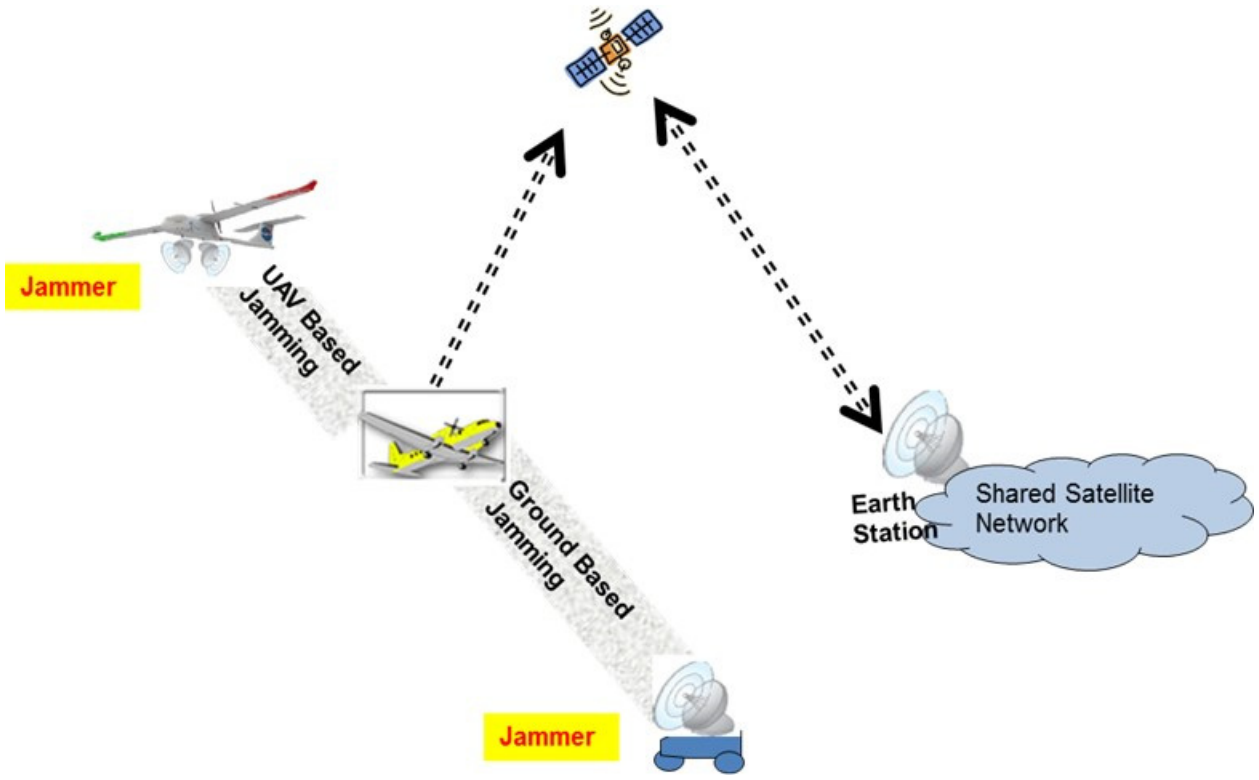


Figure 5-9 Jamming at Aircraft

In ground based jamming, a strong noise is sent from ground towards aircraft to impact the reception of downlink signal from satellites. Generally, the antennas of satellite modems are installed on the top of aircraft's fuselage and these antennas are directional and steered towards satellites. Hence, the aircraft body itself will act as a huge barrier for the ground based jammers. Therefore, the impact of ground based jammers on aircraft modems would be very minimal.

However, jammers hosted in UAVs flying at altitudes higher than that of aircraft will be able to affect satellite downlink signals at aircraft receivers. The strength of the transmitted signals from satellites would be weak at aircraft modems considering the huge path loss during their propagation from GEO orbits. Hence it would be possible to jam these signals from UAVs, even with considerably low noise power. For example, if a satellite transmitter's EIRP power is around 1000 watts (60dBm) at its transmitter antenna, considering the path loss of 213 dB and other miscellaneous losses amounting to 12 dB, the signal power at the receiver antenna of an aircraft will be around -165 dBm. UAVs flying at an altitude of 30 Km above the sea level would require only 1 dBm (1.25 milliwatts) transmit power to generate noise equal to the signal strength at aircraft receivers. The path loss from the UAV would be only 151 dB, considering UAV altitude of 30 to 40 Km above sea level. Hence an UAV, equipped with a jammer, even with 10 watts would be able to jam communications between satellites and aircraft phenomenally. UAV based jammers are estimated to impact aircraft in a region equivalent to 50% of a single spot beam footprint.

Table 5-9 summarizes different jamming techniques and their impact to receivers at aircraft.

Table 5-9 Impact of Jamming on Receivers at Aircraft

Impact on Receivers at Aircraft				
Jamming Technique	**Description**	**% of Loss of Bandwidth**	**% of Loss of Data Integrity**	**Remarks**
Full Barrage	Noise generated in the entire communication band to interrupt the signal receptions	0.2500%	0.0001%	Ground based jammers may not impact aircraft, as the antennas are isolated from jammers by the body of the aircraft.. UAVs deployed may be able to impact up to 50% of a spot beam area with 50% loss of BW to ACs. For airport region the number of AC impacted could be high.
Partial Spectrum	Attacker chooses a part of operational spectrum to jam.	0.2500%	0.0001%	Attacks based on UAVs possible. Impact would be similar to Full Barrage
Single Tone	A single carrier frequency is targeted and corrupted.	0.05%	0.0001%	Most of the satellite system would use multi carrier communication. Hence the impact is considered to be very less. 1% of one spot beam is assumed to be impacted
Pulsed Multi Tone	High strength pulses spread across the operational spectrum transmitted. Uses power in an effective way.	0.400%	0.0001%	UAV based jamming may have similar impact. 80% loss of BW to ACs within 50% of spot beam area assumed to be impacted in the Airport regions
Follower	Equipage similar to ground stations used. Follower can understand the signal technology, anti jamming mechanism and follows transmitters and its frequency hops in order to spoil the reception	0.4500%	0.0001%	Can be very effective, but, very complex to implement. Worst case scenario of 90% loss of communications to 50% of AC within a spot beam footprint assumed.

5.5.1.1.3. Threats to Earth Station

The earth stations have large dish antennas with high directionality. Hence it may not be possible to jam these antennas from a ground based jammers. The possibility of ground based jammers getting physically closer to the dish antenna and injecting noise within its solid angle of reception may be very difficult. However, UAVs flying at altitudes around 20 Km to 30 Km should be able to accomplish this without much of a geometrical problem.

Figure 5-10 shows a scenario of an UAV based jamming of an earth station. As discussed earlier UAVs with moderate jamming power and directional antennas should be capable of jamming earth stations. The feeder link contains the consolidated data traffic from all aircraft. The GEO satellite system may have a pair of Earth Stations working in redundant mode to handle the entire NAS region traffic. Hence the feeder link attack may cause serious impact to NAS operations.

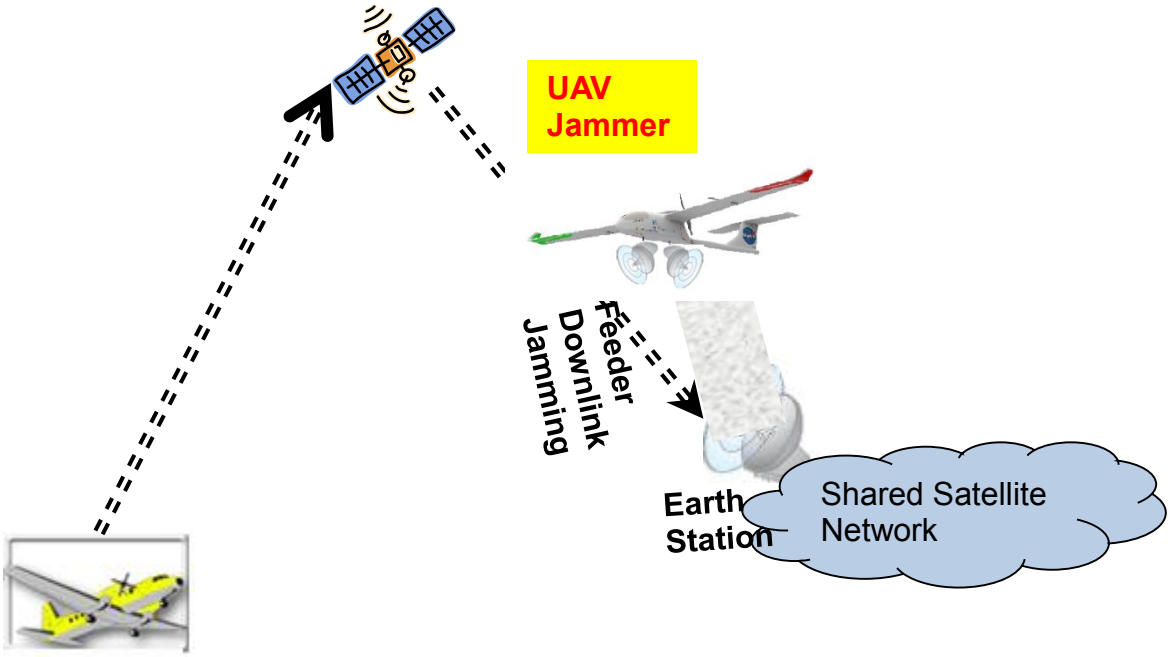


Figure 5-10 Jamming at Earth Station

Table 5-10 summarizes different jamming techniques at ground earth stations.

Table 5-10 Impact of Jamming on Receivers at Ground Earth Stations

Impact on Receivers at Ground Earth Stations				
Jamming Technique	**Description**	**% of Loss of Bandwidth**	**% of Loss of Data Integrity**	**Remarks**
Full Barrage	Noise generated in the entire communication band to interrupt the signal receptions	1.00%	0.0001%	Ground based Jammers may not be effective. UAVs equipped with jammers may cause damage. 1% impact to feeder link assumed
Partial Spectrum	Attacker chooses a part of operational spectrum to jam.	5.00%	0.0001%	Power can be utilized more optimally. Considering damage to 10% of the spectrum with 50% efficiency.
Single Tone	A single carrier frequency is targeted and corrupted.	0.10%	0.0001%	Most of the satellite system would use multi carrier communication. Hence the impact is considered to be very less.
Pulsed Multi Tone	High strength pulses spread across the operational spectrum transmitted. Uses power in an effective way.	50%	0.0001%	May cause considerable amount of degradation to feeder links. 50% damage to a feeder link assumed

Impact on Receivers at Ground Earth Stations				
Jamming Technique	**Description**	**% of Loss of Bandwidth**	**% of Loss of Data Integrity**	**Remarks**
Follower	Equipage similar to ground stations may be used. Follower can understand the signal , technology, anti jamming mechanism and follows transmitters and its frequency hops in order to spoil the reception	75%	0.0001%	Can be very effective, but, very complex to implement. 75% damage assumed

5.5.2. Capability Assessment for Jamming

UAV technologies are expected to mature over decades, acquiring capabilities to support long uninterrupted flight hours. Some of the internet companies show major interests to offer network access in remote areas of the world using cost effective UAV based solutions. Considerable amount of advancements are also happening in fuel cell technologies in increasing the capacity of fuel cells and reducing their form factors. Such fuel cells could power UAVs and onboard electronics in future. The technology advancements in metamaterials may yield lightweight, electronically steerable directional antenna that may not have moving parts or large dishes. These directional antennas could be easily hosted over UAVs. Hence considering the 2060 timeframe, jammers may not have difficulties in building jamming devices based on UAV platforms.

A rough estimate on the availability of technology capabilities for both UAV based and ground based jamming of satellite networks is provided in Table 5-11.

Table 5-11 Capability Assessment for Satellite Network Jamming

Electronics Availability		**Full Barrage**	**Partial**	**Single Tone**	**Pulsed Multi tone**	**Follower**
		20%	**80%**	**100%**	**75%**	**10%**
UAV Platform Availability	**30%**	6.00%	24.00%	30.00%	22.50%	3.00%
Ground Based Platform Availability	**50%**	10.00%	40.00%	50.00%	37.50%	5.00%
Platform Availability	**40%**	8.00%	32.00%	40.00%	30.00%	4.00%

5.5.3. Risk Assessment

This section consolidates safety hazard assessments for Loss of Communications and Loss of Data Integrity in Table 5-12 and Table 5-13 and overall risk assessments for supporting various datalink services in Table 5-14 and Table 5-15.

Table 5-12 Hazard Assessment for Loss of Communication in Satellite Networks

Jamming Techniques	Description	Access to Required Capabilities	% Loss of Bandwidth			Hazard	
			Satellite Receiver	AC Receiver	GES Receiver	Score	Level
Full Barrage	Noise generated in the entire communication band to interrupt the signal receptions	10%	0.01%	0.25%	1.00%	0.13%	Extremely Improbable
Partial Spectrum	Attacker chooses a part of operational spectrum to jam.	40%	0.50%	0.25%	5.00%	2.30%	Remote
Single Tone	A single carrier frequency is targeted and corrupted.	50%	0.10%	0.05%	0.10%	0.13%	Extremely Improbable
Pulsed Multi Tone	High strength pulses spread across the operational spectrum transmitted. Uses power in an effective way.	37%	10%	0.40%	50%	22.35%	Probable
Follower	Equipage similar to ground stations used. Follower can understand the signal , technology, anti jamming mechanism and follows transmitters and its frequency hops in order to spoil the reception	5%	20%	0.45%	75%	4.77%	Remote

Table 5-13 Hazard Assessment for Loss of Data Integrity in Satellite Networks

Jamming Techniques	Description	Access to Required Capabilities	Loss of Data Integrity	Hazard	
				Score	Level
Full Barrage	Noise generated in the entire communication band to interrupt the signal receptions	10%	0.00010%	0.00001%	Extremely Improbable
Partial Spectrum	Attacker chooses a part of operational spectrum to jam.	40%	0.00010%	0.00004%	Extremely Improbable
Single Tone	A single carrier frequency is targeted and corrupted.	50%	0.00010%	0.00005%	Extremely Improbable
Pulsed Multi Tone	High strength pulses spread across the operational spectrum transmitted. Uses power in an effective way.	37%	0.00010%	0.00004%	Extremely Improbable
Follower	Equipage similar to ground stations used. Follower can understand the signal , technology, anti jamming mechanism and follows transmitters and its frequency hops in order to spoil the reception	5%	0.00010%	0.00001%	Extremely Improbable

Table 5-14 Risk Assessment on Loss of Communications in satellite Networks

Service Category	Loss of Communications	Full Barrage	Partial Spectrum	Single Tone	Pulsed Multi Tone	Follower
	Safety Hazard→ Safety Target	Extremely Improbable	Remote	Extremely Improbable	Probable	Remote
Data Communications Management Services (DCM)	Probable	Ok	OK	OK	OK	OK
Clearance/Instruction Service (CIS)	Remote	OK	OK	OK	Threat	OK
Flight Information Service (FIS)	Probable	OK	OK	OK	OK	OK
Advisory Services (AVS)	Remote	OK	OK	OK	Threat	OK
Flight Position/Intent/ Preference Service (FPS)	Remote	OK	OK	OK	Threat	OK
Emergency Information Service (EIS)	Probable	OK	OK	OK	OK	OK
Delegated Separation Service(DSS)	Remote	OK	OK	OK	Threat	OK
Miscellaneous Services(MCS)	Extremely Improbable	OK	Threat	OK	Threat	Threat

Table 5-15 Risk Assessment on Loss of Data Integrity in satellite Networks

Service Category	Loss of Communications	Full Barrage	Partial Spectrum	Single Tone	Pulsed Multi Tone	Follower
	Safety Hazard → Safety Target	Extremely Improbable	Extremely Improbable	Extremely Improbable	Extremely Improbable	Extremely Improbable
Data Communications Management Services (DCM)	Probable	Ok	Ok	Ok	Ok	Ok
Clearance/Instruction Service (CIS)	Remote	OK	OK	OK	OK	OK
Flight Information Service (FIS)	Probable	OK	OK	OK	OK	OK
Advisory Services (AVS)	Remote	OK	OK	OK	OK	OK
Flight Position/Intent/ Preference Service (FPS)	Remote	OK	OK	OK	OK	OK
Emergency Information Service (EIS)	Probable	OK	OK	OK	OK	OK
Delegated Separation Service(DSS)	Remote	OK	OK	OK	OK	OK
Miscellaneous Services(MCS)	Extremely Improbable	OK	OK	OK	OK	OK

Some of the conclusions of the assessments are given below.

- By design, the entire air-ground data is consolidated through feeder links to reach ground stations in satellite and downstream networks. Hence any impact to feeder links may cause severe performance degradation over a wide area.
- The advancements in technologies such as UAVs, fuel cells and lightweight directional antennas may help miscreants to design airborne jammers that can cause serious damage to feeder link performances.
- Hence, the assessment concludes that, unless the feeder link is safeguarded from UAV based jamming attacks, the satellite network may not be safe for datalink services such as Clearance/Instruction Service (CIS), Advisory Services (AVS), Flight Position/Intent/ Preference Service (FPS), Delegated Separation Service (DSS) and Miscellaneous Services (MCS).

5.6. ARCHITECTURE OPTION 3 – SO-OFDMA NETWORK

As per the concept definition of SO-OFDMA network in Phase 1 of the project, the network does not have its own security framework at the Physical (PHY) and Link layers. The packets are broadcasted in clear text at the SO-OFDMA level. As per the model, if the data messages are to be secured, they have to be protected by the higher layers, either at higher MAC level or at network layer level. Hence, this architecture exposes SO-OFDMA link control messages and the broadcast messages that originate at SO-OFDMA level to cyber attacks. Figure 5-11 shows SO-OFDMA network architecture and its vulnerabilities to various attacks.

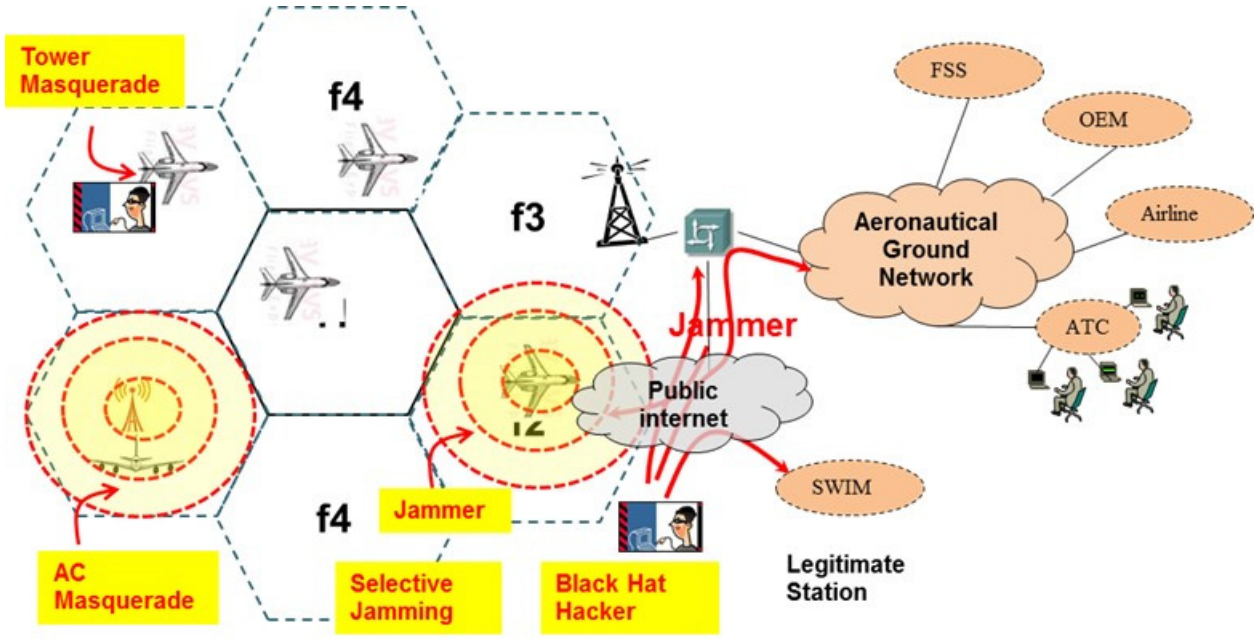


Figure 5-11 Security Threats to SO-OFDMA network

In the SO-OFDMA architecture the base stations do not control or coordinate network functions, but act as mere data nodes connecting aircraft to the ground network. The ground node may be connected to aeronautical ground network as well as to the internet for accessing SWIM services. Hence this architecture exposes the network to a host of attacks similar to the ones explained in section 5.4 for cellular networks.

5.6.1. Threat Analysis

The types of threats possible in an SO-OFDMA network are:

- Jamming
- Scrambling (Selective Jamming)
- Impersonating AC
- Impersonating Ground Node
- Key Management Issue
- Black Hat Hacker Attack

Please refer Section 5.4 for details about these threats as these attacks are similar to the ones explained there.

5.6.2. Risk Assessment

Safety hazard assessments for SO-OFDMA network is provided in Table 5-16 and Table 5-17 and the overall risk assessments of Loss of Communications and Loss of Data Integrity in supporting various datalink services are provided in Table 5-18 and Table 5-19.

Table 5-16 Hazard Assessment on Loss of communications in SO-OFDMA Networks

Threat Vector	Description	Estimated Loss of Communication		Access to Required Capabilities		Safety Hazard	
		Score	Remarks	Score	Remarks	Loss of Communications	
Jamming	A strong noise transmitted to affect the legitimate signal to cause denial of service to aircraft in that region	0.25%	Assuming 20% of the pseudo cell communication impacted by continuous jamming. Creating continuous jamming noise will require high amount power. The cell range is larger than commercial mobile towers.	90.00%	Generic commercial cell phone jammers may be deployed	0.23%	Extremely Improbable
Scrambling	Selective jamming of a specific frames / parts of a frame Knowledge of the frame structure known to scrambler	0.50%	The entire cell operations can be brought down by selectively knocking off control part of the frame	50.00%	May require additional engineering efforts.	0.25%	Extremely Remote
Impersonating AC	Hacker uses a SO-OFDMA modem with AC Id to impersonate AC and broadcast wrong AC positions and IDs to confuse the network.	0.40%	Broadcast traffic may be severely impacted. Flooding AC Ids and positions may confuse the network	50.00%	SO-OFDMA modem can be modified to send wrong information	0.20%	Extremely Improbable
Impersonating BS	The ground station or Base station faked by a Rogue Station/Aircraft. Rogue Station uses legitimate Base station ID in its routing broadcast so that all aircraft in the pseudo cell and adjacent pseudo cells are attracted towards it.	12.00%	The entire routing information may be modified in the region covering multiple cells. (Assuming 30 cells impacted by wrong info. The impact is on Air Ground communications. Air to Air may remain unaffected)	50.00%	BS credentials difficult to get. Score for BS with credentials.	6.00%	Remote
Key Mgmt issues	Loopholes in Key or credential management infrastructure leading to security breach on a large scale.	50.00%	Major issue. May impact entire NAS.	0.10%	Very difficult to manipulate credentials	0.05%	Extremely Improbable
Black Hat Hacker	SO-OFDMA may use cellular network for ground connectivity. Since cellular network is a public network any random hacker from internet anywhere may try to attack the gateways to ground side network.	2.00%	10% of a network population	0.50%	Similar to enterprise network	0.01%	Extremely Improbable

Table 5-17 Hazard Assessment on Loss of Data Integrity in SO-OFDMA Networks

Threat Vector	Description	Estimated Loss of Data Integrity		Access to Required Capabilities		Safety Hazard	
		Score	Remarks	Score	Remarks	Loss of Data Integrity	
Jamming	A strong noise transmitted to affect the legitimate signal to cause denial of service to aircraft in that region	0.01%	Jamming may not impact data integrity owing to integrity algorithms	90.00%	Generic commercial cell phone jammers may be deployed	0.00%	Extremely Improbable
Scrambling	Selective jamming of a specific frames / parts of a frame Knowledge of the frame structure known to scrambler	0.01%	Same as Jamming. May not impact integrity much	50.00%	SO-OFDMA modem can be modified to impact the control frames May require additional engineering efforts.	0.00%	Extremely Improbable
Impersonating AC	Hacker uses a SO-OFDMA modem with AC Id to impersonate AC and broadcast wrong AC positions and IDs to confuse the network.	0.50%	As the broadcasts are sent as clear text, Surveillance information may get severely impacted in the cell range. (1 cell out of 20 cells assumed)	50.00%	SO-OFDMA modem can be modified to send wrong information	0.25%	Extremely Remote
Impersonating BS	The ground station or Base station faked by a Rogue Station/Aircraft. Rogue Station uses legitimate Base station ID in its routing broadcast so that all aircraft in the pseudo cell and adjacent pseudo cells are attracted towards it.	12.00%	Surveillance information in multiple cells may be impacted causing confusion in the region. (8-% of 30 cells out of 200 cells impacted)	50.00%	SO-OFDMA modem can be modified to send wrong information	6.00%	Remote
Key Mgmt issues	Loopholes in Key or credential management infrastructure leading to security breach on a large scale.	50.00%	Major issue. May impact entire NAS.	0.10%	Very difficult to manipulate credentials	0.05%	Extremely Improbable
Black Hat Hacker	SO-OFDMA may use cellular network for ground connectivity. Since cellular network is a commercial network it has access to internet. Hence any random hacker from internet anywhere may try to attack the gateways to ground side network.	2.00%	10% of a network population	0.50%	Similar to enterprise network	0.01%	Extremely Improbable

Table 5-18 Risk Assessment on Loss of communications in SO-OFDMA Networks

Service Category	Loss of Communications	Jamming	Scrambling	Impersonating AC	Impersonating Ground Node	Key Mgmt issues	Black Hat Hacker
	Safety Hazard→ Safety Objective	Extremely Improbable	Extremely Remote	Extremely Improbable	Remote	Extremely Improbable	Extremely Improbable
Data Communications Management Services (DCM)	Probable	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Clearance/Instruction Service (CIS)	Remote	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Flight Information Service (FIS)	Probable	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Advisory Services (AVS)	Remote	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Flight Position/Intent/ Preference Service (FPS)	Remote	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Emergency Information Service (EIS)	Probable	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Delegated Separation Service (DSS)	Remote	No Threat	No Threat	No Threat	No Threat	No Threat	No Threat
Miscellaneous Services (MCS)	Extremely Improbable	No Threat	Threat	No Threat	Threat	No Threat	No Threat

Table 5-19 Risk Assessment on Loss of Data Integrity in SO-OFDMA Networks

Service Category	Loss of Data integrity	Jamming	Scrambling	Impersonating AC	Ground Node Impersonating	Key Mgmt issues	Black Hat Hacker
	Safety Hazard→ Safety Objective	Extremely Improbable	Extremely Improbable	Extremely Remote	Remote	Extremely Improbable	Extremely Improbable
Data Communications Management Services (DCM)	Remote	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact
Clearance/Instruction Service (CIS)	Extremely Remote	No Impact	No Impact	No Impact	Threat	No Impact	No Impact
Flight Information Service (FIS)	Extremely Remote	No Impact	No Impact	No Impact	Threat	No Impact	No Impact
Advisory Services (AVS)	Extremely Remote	No Impact	No Impact	No Impact	Threat	No Impact	No Impact
Flight Position/Intent/ Preference Service (FPS)	Extremely Remote	No Impact	No Impact	No Impact	Threat	No Impact	No Impact
Emergency Information Service (EIS)	Remote	No Impact	No Impact	No Impact	No Impact	No Impact	No Impact
Delegated Separation Service (DSS)	Extremely Remote	No Impact	No Impact	No Impact	Threat	No Impact	No Impact

Miscellaneous Services (MCS)	Extremely Improbable	No Impact	No Impact	Threat	Threat	No Impact	No Impact

The conclusions of the SO-OFDMA security assessment are listed below:

- At the current level of definition, SO-OFDMA network may be able to satisfy the requirements of Data Communication Management Service (DCM) and Emergency Information Service (EIS) only. All other datalink services demand higher level of robustness from the network.
- Lack of security features at link and physical layer is a major concern for SO-OFDMA network to support safety critical datalink applications.
- Link layer broadcast in clear text communication makes the network vulnerable to masquerading attacks that may impact data integrity. It may not be possible to support surveillance applications requiring air-to-air broadcast such as ADS-B, if there are integrity issues.
- SO-OFDMA being defined as an ad hoc network that works without a central network control node, the network is immune to single point failures, as experienced by the centrally controlled networks. However, the addition of security features at physical and link layers would be required to improve the robustness of the network comprehensively.

5.7. MITIGATION TECHNIQUES

The security assessments done so far, on the three network architecture options, reveal that none of the networks would be able to support all requirements of future safety critical datalink services completely. The services like A-Exec involve controlling aircraft from ground remotely and hence they require a very high robust network. Some of the concerns about the network architectures are listed below.

- Most of the traditional networks are based on the architectures that have central node to control network operations. Hence jamming these control nodes may cause network outages in the regions serviced by those nodes.
- Generally in communication networks, the initial control messages for link establishment, ranging, etc., are sent in clear text which is vulnerable to attacks.
- Absence of a common security framework across networks in NAS environment to implement common policies, cryptographies and keys, required by NextGen safety critical applications, may be viewed as a serious limitation over a period of time.
- NextGen Datalink applications may become more sensitive even to loss of communications in the future.

Considering the above limitations, some mitigations techniques are identified in the following sections and the approach to incorporate them in NAS environment is also explained.

5.7.1. Decentralized network

The main purpose of a decentralized network is to remove the dependency on ground stations to control network operations and thereby avoiding single point failures in the network. Aircraft flying over a region should be able to form a network in an ad hoc manner and support both air-

to-air and air/ground communications without the need of a control node. Figure 5-12 illustrates a concept to implement ad hoc network over the NAS region. This proposal extends some of the concepts from the SO-OFDMA architecture.

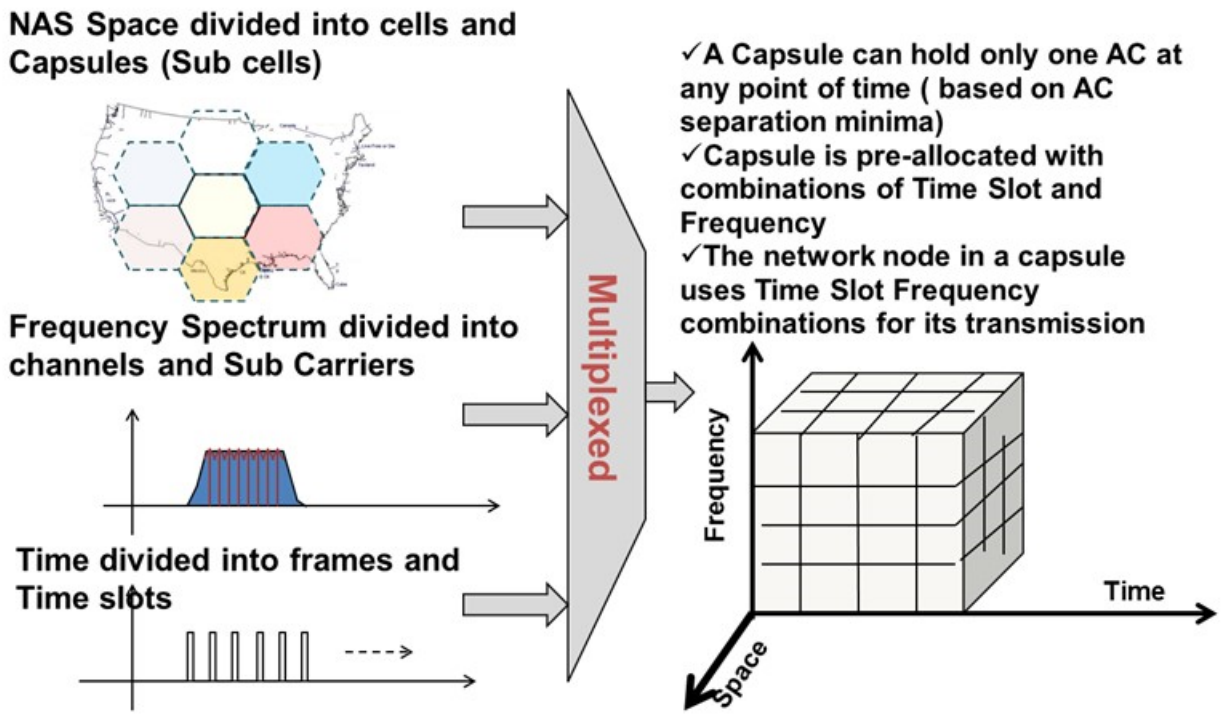


Figure 5-12 Space Time Frequency Resource Allocation Scheme

The overall NAS space is be divided into cells and capsules. Capsule size is determined based on separation minima definition for aircraft in a region so that a capsule can hold only one aircraft at any point of time. The frequency spectrum is divided into multiple carrier frequencies. Space Time Frequency multiplexing scheme can be followed to allocate resources to a capsule for various timeslots. Every capsule is allocated with a schedule of carrier frequency and time slot combination that varies dynamically with time. Such resource allocation plan is standardized and loaded into aircraft modems. Depending upon the aircraft position, corresponding capsule can be identified by the modem and the allocated carrier frequencies for various time slots can be derived from the resource plan and utilized accordingly for its transmissions. Thus, the need for a central network node to coordinate resource allocations can be eliminated.

5.7.2. Allocation of Network resources

The ad hoc network environment for NAS explained in section 5.7.1 would require a mechanism to configure aircraft with the pre-allocated network resource plan. Figure 5-13 shows such a mechanism for providing resource allocation plans to aircraft.

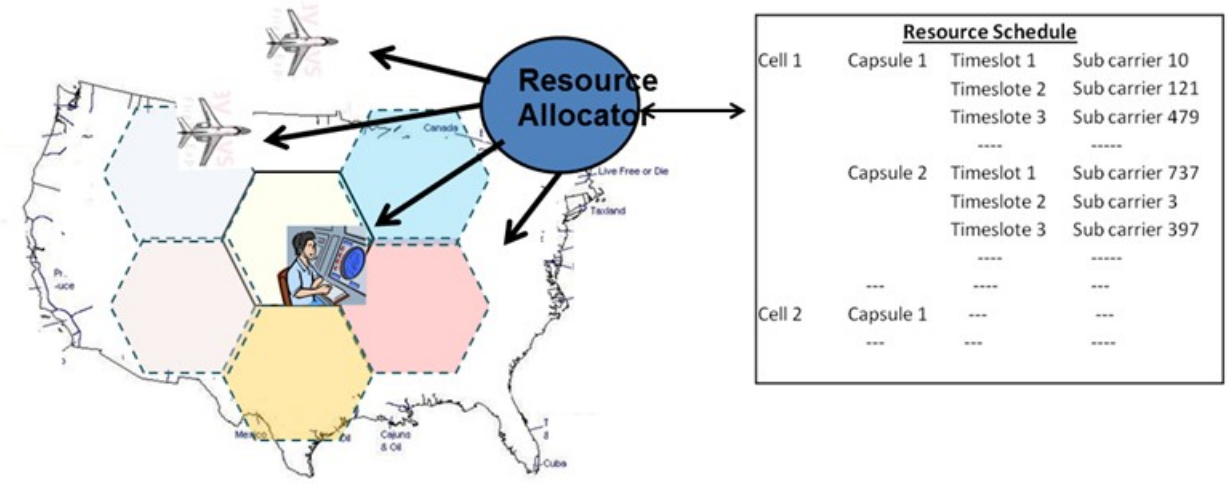


Figure 5-13 AC Resource Allocation Mechanism

A common resource allocator manages the overall resource schedule for the NAS region. The resource schedule has a mapping of capsules to timeslots and carrier frequencies. The resource allocator will periodically configure all ground systems with this information through a secured communication link. Aircraft will receive NAS resource allocation plan, only if they are cleared for flying. When an aircraft files a flight plan with ATC, the network resource plan corresponding to its time window of flight can be configured into the aircraft on its flight plan approval. Thus the system ensures that only the authorized nodes get the resource allocation information of NAS. The resource allocator can periodically change the resource allocation schedule for the NAS region to improve security. The network configurations are transferred to aircraft securely as per the mechanism defined in section 5.7.5.

5.7.3. Configurations of Security Parameters

In addition to the resource allocations, security plan can also be configured to the aircraft during flight plan filing phase as shown Figure 5-14.

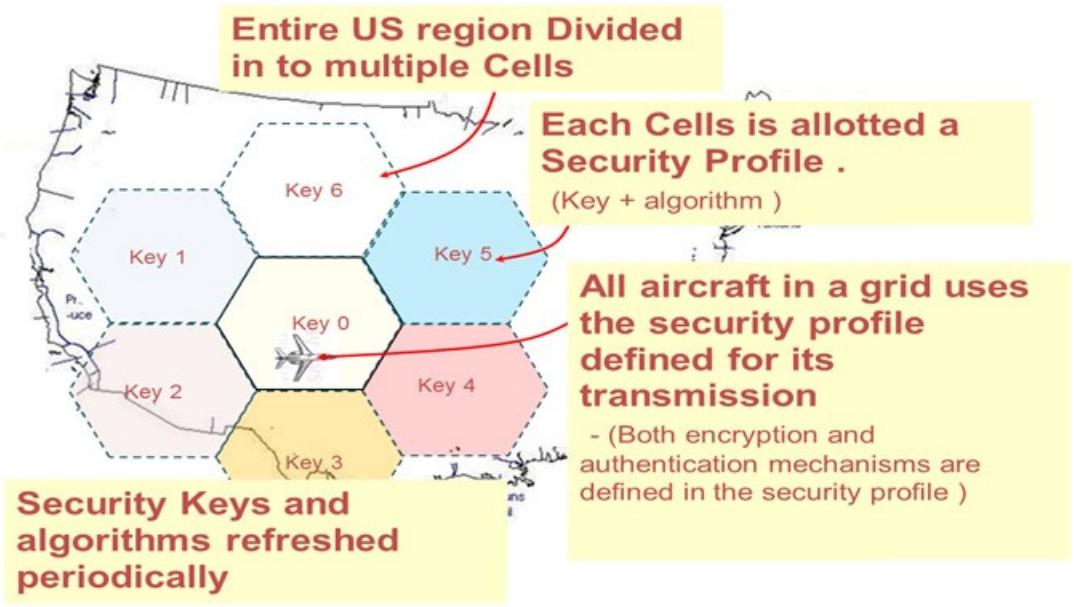


Figure 5-14 Security Plan configuration

The security plan may include cryptographic algorithms and keys that are to be used in each cell (if not capsule) for various traffic like broadcasts, unicasts, network packets, Layer 2 packets, etc., depending upon the security policies in place. Aircraft can use the appropriate security policy for its transmission or reception. Aircraft and other network nodes are expected to support a set of pre-approved security algorithms and the security plan is arrived by selecting a combination of security algorithm from the pre-approved list for various traffics. The security plan for a region will be refreshed periodically.

5.7.4. Configurable Radios

Considering 2060 time frame, the availability of software defined radios and capabilities to support multiple waveforms in a single radio box would be common, as illustrated in Figure 5-15.

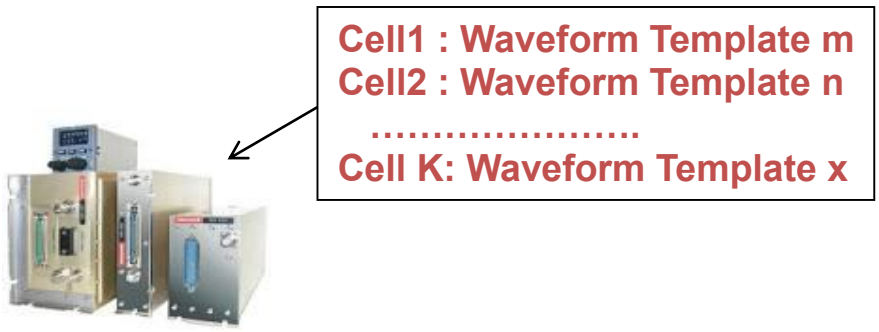


Figure 5-15 Radio Parameter Configuration

Hence the radio parameters can also be defined for every cell and configured into the aircraft and other network nodes using the same or similar framework explained in section 5.7.3.

5.7.5. Network Configuration Management

Since the entire network operations depend upon the network configurations, a robust configuration management procedure is required to transfer network parameters to aircraft. Figure 5-16 illustrates the network configuration management scheme.

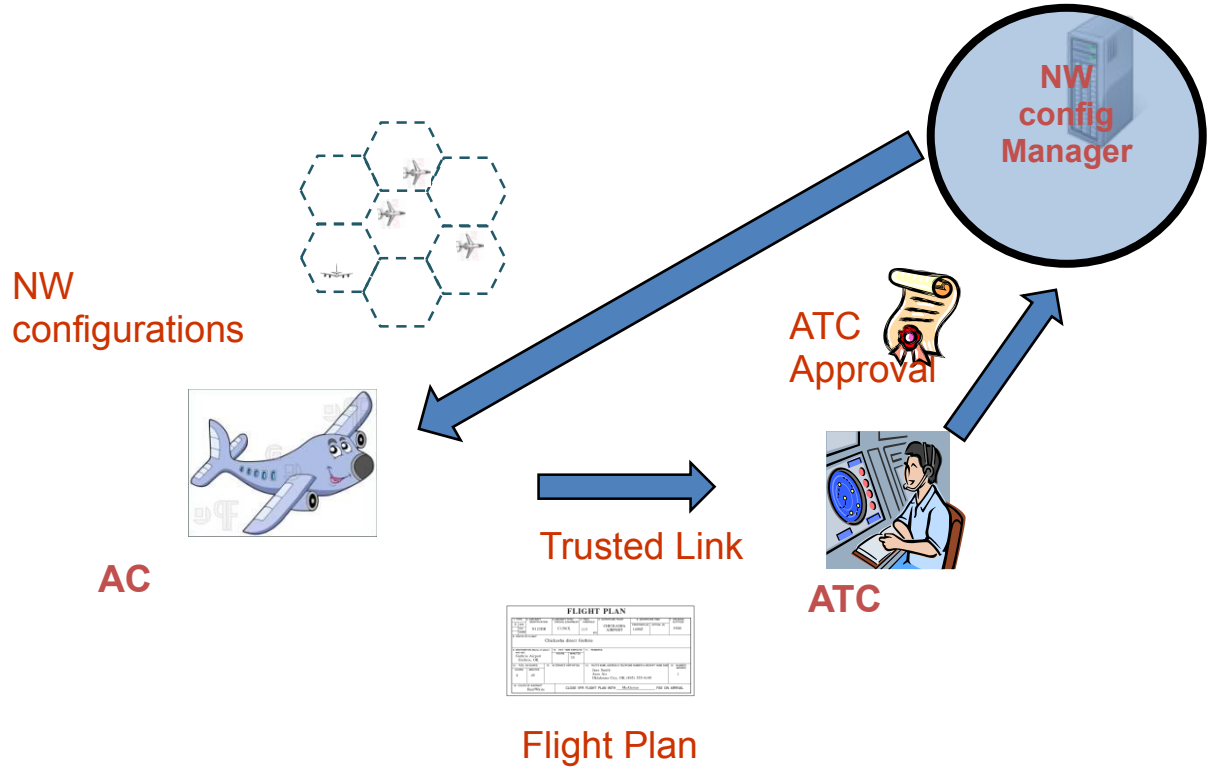


Figure 5-16 Network Configuration Management

As per this mechanism, an aircraft files the flight plan with the ATC. ATC on approving the flight plan passes the flight information to the Network Resource Manager. The Network Resource Manager maintains complete information about resource allocation plan, security plan and radio

configuration plan for the NAS region. These details are configured into the aircraft as indicated in the flight plan. The information exchanges between aircraft, ATC and Network Resource Manager would happen through secured datalinks. The trust between the three parties could be established by digital certificates signed by common certificate authority servicing the NAS region for other datalink services. The network manager periodically refreshes the resource allocation and configuration plans. In addition to updating aircraft, the ground nodes also have similar mechanism to acquire the network configuration information from the network manager. FAA or any other agency appointed by FAA may provide such service in NAS region.

5.7.6. Safety Considerations

Figure 5-17 shows the extent of safety considerations addressed in approach discussed so far.

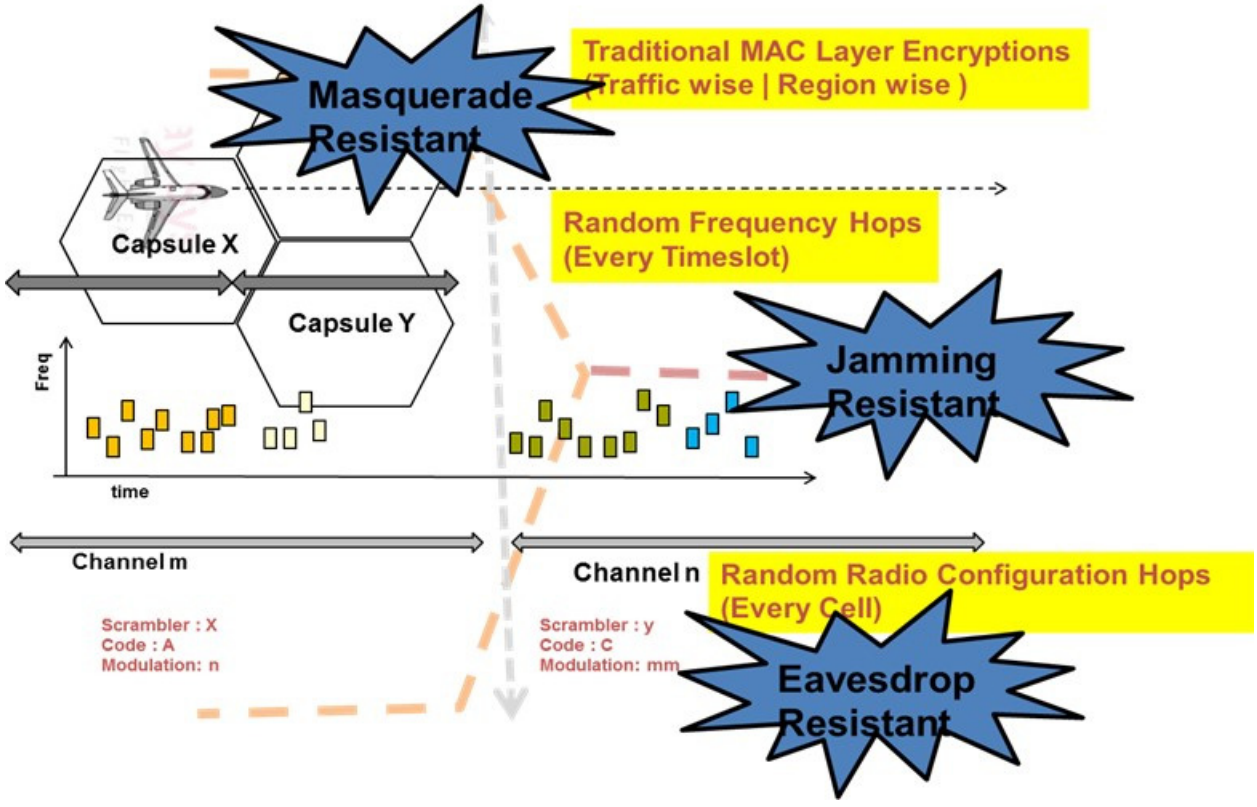


Figure 5-17 Safety Considerations

- Waveform designs are configured for every cell. Unless this information is known to the intruder, he will never be able to decode the waveforms and extract data out of it. Hence the network becomes resistant to eavesdrops at physical layer.
- The carrier frequencies are allocated for every capsule–timeslot combination. The carrier frequencies are spread across the entire aeronautical spectrum used for communication. Unless such allocation scheme is available to the jammer, the jammer will not be able to

follow the carrier signals to jam it or decode control information. Hence selective jamming techniques may not be effective in such networks.

- The security framework ensures that the messages are protected at MAC and higher layers.
- In absence of a centralized network control, every node in the network operates independently of each of each other. Hence the network is immune to single point failures.

Hence such a network would be very robust and immune to most of the threats.

5.7.7. Strategy for Cellular Network

As discussed earlier, some minor modifications would be required in cellular networks to support air-ground communications. Increased transmission power to support long range communications, strategies to handle higher Doppler shifts because of higher aircraft speeds, antenna designs to support emission towards aircraft, etc., are some of the changes anticipated in the cellular network designs. Therefore, the base stations are expected to be modified to support air-ground communications as shown in Figure 5-18.

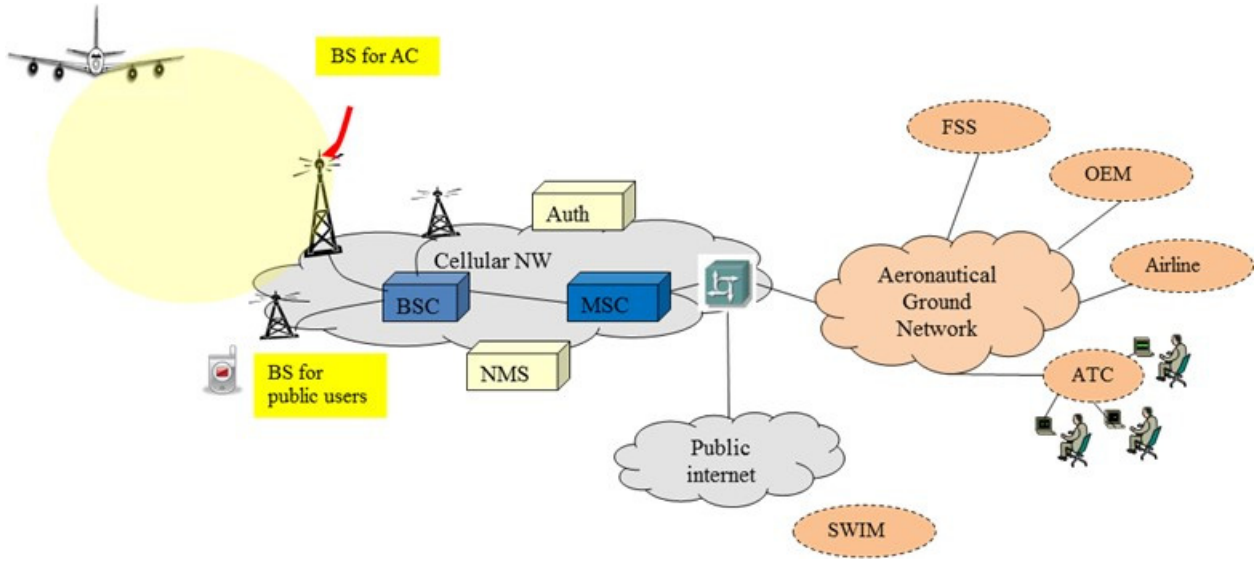


Figure 5-18 Cellular Network

Hence, while redesigning the base stations for aeronautical purposes, the security risk mitigation techniques identified in the sections above could be implemented at the same time. Beyond base stations, the network would be common for both commercial and aeronautical data traffic. There are no changes expected in the network nodes such as message switches or gateways that are present in the cellular network beyond base stations.

5.7.8. Strategy for Satellite Network

As per the assessment, the major concern for the satellite network is the attack on its feeder links using airborne platforms. UAV based jammers with nominal noise power would be able to jam the feeder links at ground earth stations. Hence the strategy for the satellite network is to eliminate the feeder links completely for the satellite networks. See Figure 5-19.

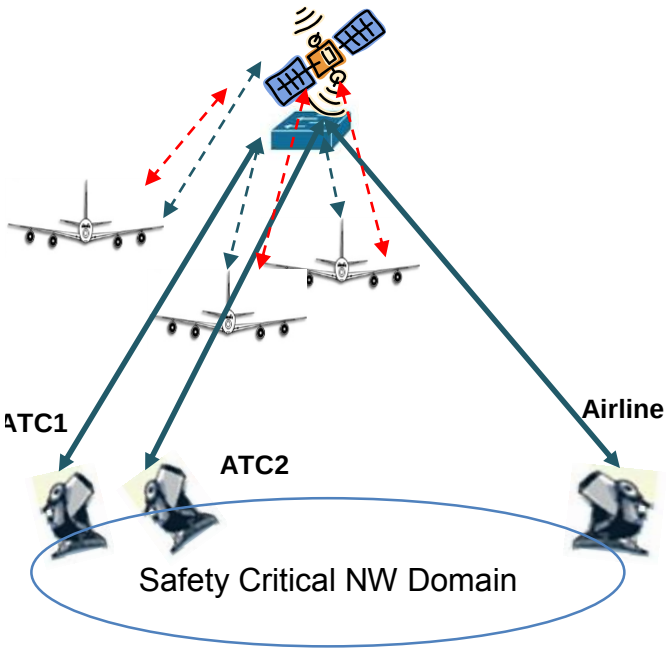


Figure 5-19 Satellite Network without Feeder Links

In this proposal, the satellites have only user links for both aircraft and ground systems. ATC centers and airline operations centers may have the user terminals similar to aircraft modems installed in their premises. The satellites have onboard routing/switching capability. Satellites will establish direct point to point connections between the user terminals for their communications based on their requests. Bandwidth allocations will depend upon the number connections established by the terminals. For example: Aircraft may require one or more connections to communicate with ATC or airline centers, while ATC centers might require multiple connections to communicate with all aircraft within its control. The satellite network should be capable of supporting such dynamic bandwidth aggregation depending upon the connection requirements. The satellite control link may make use of user terminal connections for communicating with satellite control systems. Thus the feeder link can be completely eliminated in this design and the satellite network becomes almost immune to all types of attacks discussed so far.

5.7.9. Jammer Localization

By implementing the strategies discussed above, the networks may become more robust and immune to attacks that would cause network outages. But still jammers would be able to cause minor disturbances to the network causing marginal degradation in network performances. Hence, it is also important to identify the jamming incidents, locate jammers and stop them to limit the duration of disturbances to the network. Figure 5-20 illustrates such a technique to locate jammers.

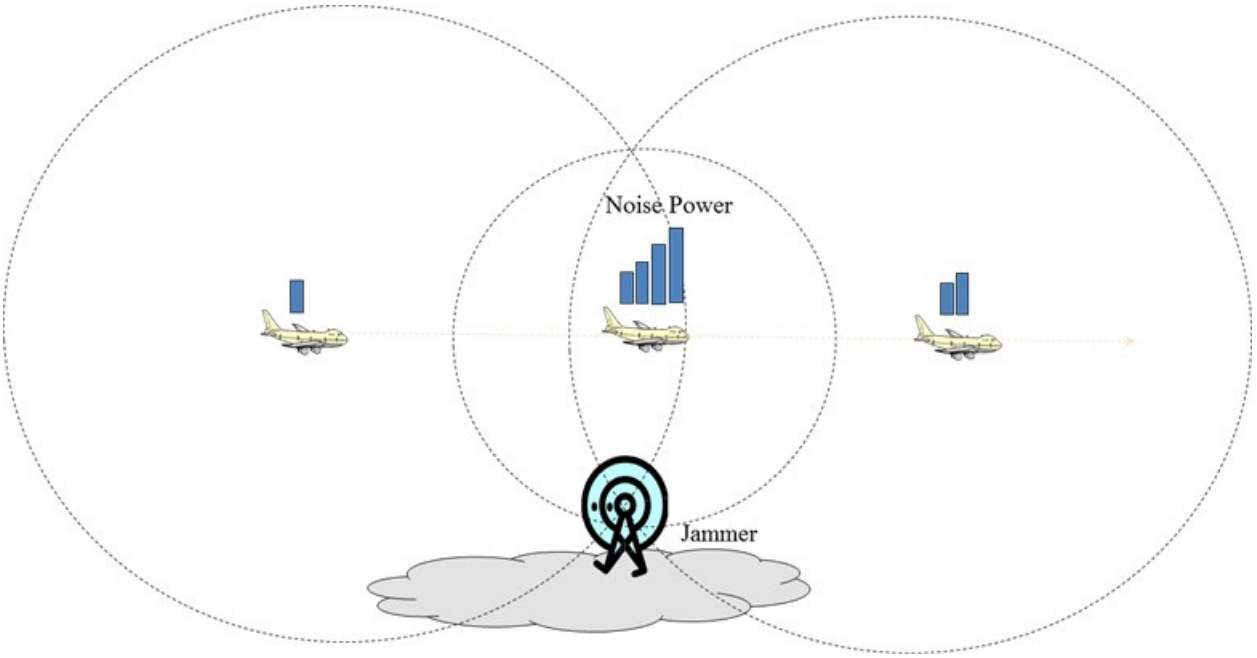


Figure 5-20 Multilateration Technique to Locate Jammers

It should be possible to locate the jammers roughly by tracking the noise power continuously along the aircraft flight trajectory and applying multilateration technique to determine the approximate location of the jammer. Analysis of the jammer localization technique was not within scope of this project, but a further study on this area is highly recommended.

5.7.10. Hacker monitoring

Generally, the networks would be connected to the Internet for accessing some services or to provide website/email connectivity to passengers. Hence the network becomes exposed to black hat hacker attacks. It should be noted that black hat hacker attacks from the Internet can never be avoided completely, but it should be possible to locate the hacker threats and alert network administrators for corrective actions. The corrective actions may include shutting down certain interfaces, blocking some traffic, masking some network domains, etc.

As shown in Figure 5-21, traffic monitors can be included in the networks in strategic locations to look for patterns of hacker attacks in the network. In case of a hacker attack, the hacker would be generating data traffic in a particular pattern, such as continuous login messages, etc. Traffic monitors would look for such patterns and identify the potential threats to the network and alert the centrally located NAS network monitor. Such a network monitoring framework and tools could be considered for deployment in the NAS network.

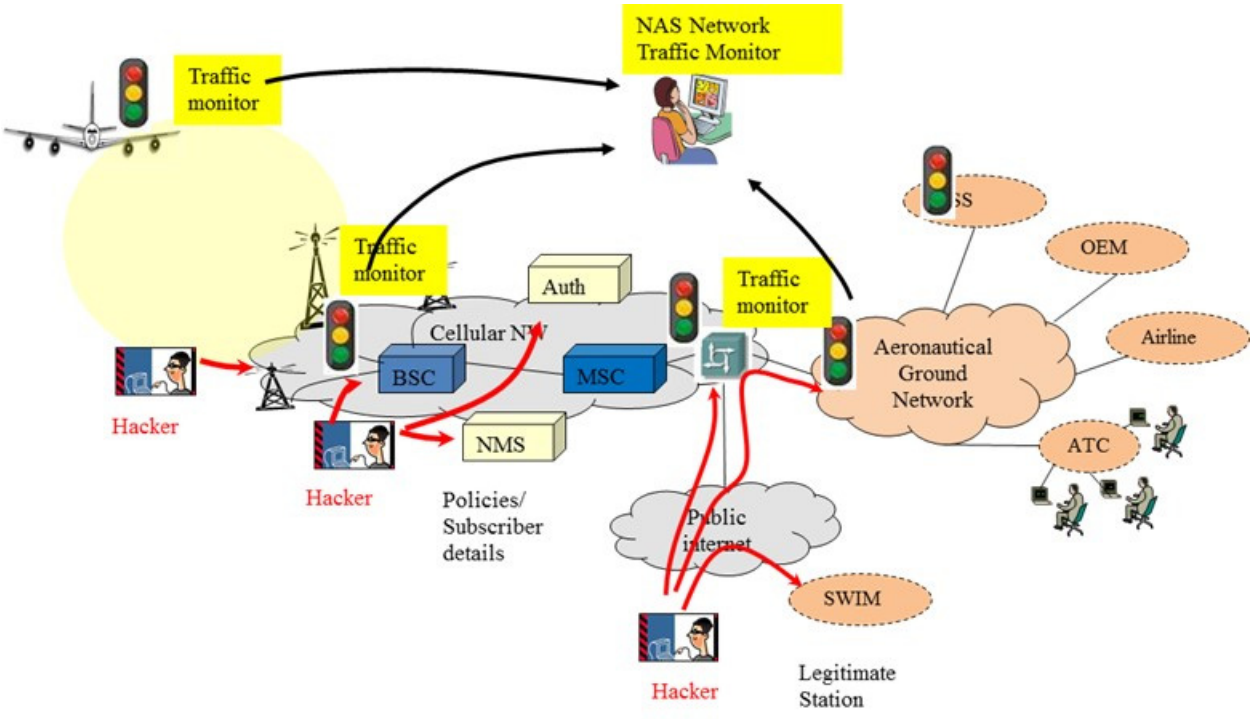


Figure 5-21 Hacker Monitoring

5.8. SUMMARY OF SECURITY ASSESSMENT

Security assessments were carried out with the objective of identifying the vulnerabilities of candidate technologies and architectures to intentional safety threats, assessing safety hazards to datalink services and recommending mitigation strategies to improve overall safety aspects of the NAS environment. The candidate technologies down-selected from phase 1 tasks were considered for the assessment. Future Cellular, GEO Satellite and SO-OFDMA technologies were considered for the assessment. The assessment was carried out in three stages, namely, Threat Identification, Hazard Estimation and Risk Assessment. Finally, mitigation techniques were identified and the strategies to implement them in NAS environment were recommended.

Some of the observations of this assessment are listed below:

- Cellular networks should be able to handle most of the data link services except the applications like Autoexec that would be used to control aircraft remotely from ground using datalinks. Such services may require very high network robustness. The architectures with base stations controlling network operations are vulnerable to network outages when the base stations are targeted by the attackers. RF jamming and man-in-middle attacks are the major concerns for Cellular Networks.
- Satellite networks are generally immune to most of the attacks, but in the 2060 timeframe, the attacks based on UAV platforms may become more common and such attacks on feeder links at ground earth stations may cause a serious impact in the NAS region. Unless protected from such feeder link attacks, the satellite network may not be safe for datalink

services such as Clearance/Instruction Service (CIS), Advisory Services (AVS), Flight Position/Intent/ Preference Service (FPS), Delegated Separation Service (DSS) and Miscellaneous Services (MCS).

- SO-OFDMA concept in its current level definition does not support security mechanism at the PHY and Link levels. This makes SO-OFDMA network highly vulnerable to many attacks. The network is susceptible to data integrity issues because of the absence of protection for broadcast messages. Unless security features are incorporated in the network, the network may not be able to support most of the datalink applications. Assessment revealed that SO-OFDMA network may be able to satisfy the requirements of Data Communication Management Service (DCM) and Emergency Information Service (EIS) only. Hence additional security features is highly recommended.

Satellite and Cellular networks suffer from the central node based architecture that controls network operations, while SO-OFDMA network is immune to such single point failures, but, it lacks other security features that are available in other networks. Hence, mitigation objectives were identified by combining the merits of all networks. Some of the mitigation strategies recommended are decentralizing network, pre-allocated network resources, configurable radios, configurable security parameters, position based resource allocation scheme and Jammer/Hacker location strategies.

6. CONCLUSIONS

This section summarizes the results of the operational and security assessments of the best alternative technologies. It provides recommendations for future work beyond this project to further analyze and develop the technologies and architectures with the goal of defining requirements and approach for proof-of-concept activities.

6.1. SUMMARY

This report provided the results of operational and security assessments of the best technology alternatives. The best alternative technologies were selected based on analyses performed in previous analysis and assessment tasks in the project. The best alternative technologies selected include next generation 5G+ cellular, Ku/Ka band SATCOM and SO-OFDMA. FSO was identified as a supplementary technology for high throughput point-to-point links. In this Task 6, the subject of this report, the best alternative technologies and architectures are analyzed in operational and security assessments in providing air/ground and air-to-air communications for ATM applications in the 2060 timeframe.

The results of the best alternatives assessment reinforce the conclusion of the previous project analysis tasks that the three remaining technology and architecture candidates together provide a suitable hybrid solution. They generally meet latency and data throughput performance requirements of ATM applications in the 2060 timeframe. Security was analyzed in terms of the susceptibilities inherent in the nature of the technologies. Potential security protections were analyzed for mitigation of the security risks presented by the threats. Security measures can be put in place to mitigate the risks but not completely eliminate the risks. A defense in depth will be a good approach to mitigate risks. Summaries of the operational and security assessments are provided below.

Summary of Operational Assessment

The operational assessment consisted of an operational view analysis and simulation modeling analysis. In the operational view analysis, a concept of operations of communication services supporting ATM application services was developed. It identified information flows of the communication services for the following types of data traffic: critical safety services - ATS and AOC; non-critical services - AAC and SWIM; and passenger traffic - APC. The concept of operations assumed that these data traffic types, including APC, will share common links in future broadband air/ground communication systems in the 2060 timeframe. Air-to-air communication systems were assumed to be dedicated to ATS, AOC and AAC traffic only.

Communication scenarios were analyzed in context of the architectures using the best alternative technologies for air/ground and air-to-air communications. The architectures included ground-based and HAP-based 5G+ cellular architecture (architecture option 1), Ku/Ka SATCOM architecture (architecture option 2) and SO-OFDMA architecture (architecture option 3). The hybrid architecture is a combination of the three architectures and thus an analysis of the hybrid architecture was covered by the analyses of the three architectures.

The operational view analysis results included the data traffic throughputs or bandwidth predicted for the 2060 timeframe for the data traffic types (ATS, AOC, AAC, SWIM and APC) in each airspace domain and flight phase (pre-departure, arrival and taxi in APT domain; departure and arrival in TMA; operations in ENR, OPR and AOA). The data traffic was analyzed across various aircraft types, including ATR, microjets, BGA, UAS and military aircraft flying civilian routes under CAA rules. The single-aircraft data flow results for each of these aircraft types were used for input to the simulation modeling analysis.

The next phase of the operational assessment used modeling and simulation to further assess the best alternative technologies. Starting with the latency, data bandwidth (per-aircraft data traffic estimates provided by the operational view analysis) and priority requirements of the data traffic types, the architectures were modeled and analyzed, which included computer-based modeling. Data packet loss and scalability performance were also analyzed. Aircraft traffic information was taken from current ADSI data and extrapolated for the 2060 timeframe. The simulation and analysis produced performance results to assess if and how well the technologies met the requirements. The technologies were modeled and analyzed in context of the three architectures.

The modeling and simulation part of the operational assessment utilized a combination of modeling of the single-system architectures, which included computer-based modeling of the systems, and a traffic and network simulation covering the CONUS. The traffic and network simulation, the Air Traffic Simulation Model Tool, applied the models of the three best alternative architectures to a planned CONUS-wide network for air/ground and air-to-air communications. The Microsoft Windows® based tool is a NAS network simulation and visualization tool to generate performance statistics for analysis and evaluation. It is a highly configurable tool and provides a GUI for setup, operation and report generation.

A summary of the modeling and simulation results are provided below.

- Ground-based Cellular Network Results

Latency requirements of ATS, AOC, AAC, SWIM and APC data types were met for high-density aircraft traffic (up to 400 aircraft per 2 degree by 2 degree cell). However, APC, having the lowest priority for transmission and much greater traffic volume, experienced significantly more latency at 400 aircraft per cell and significant packet loss starting at 50 aircraft per cell. There was no packet loss experienced by ATS, AOC, AAC and SWIM up to 400 aircraft per cell. To cover the CONUS, 360 cells (ground base stations) were needed.

- HAP-based Cellular Network Results

Results were similar to the results of the ground-based cellular network. A single HAP cell is able to support a greater number of aircraft and thus fewer HAP cells are needed to cover the CONUS in comparison to the coverage of ground-based cells. However, a higher link capacity is required for the aircraft-to-HAP link to support the greater number of aircraft in the cell (4 degree by 4 degree cell). This link represents a potential bottleneck in traffic flow. To cover the CONUS, 100 cells (HAP base stations) were needed.

- Satellite Network Results

Latency was significantly higher due to the inherent propagation delays in satellite communications. SATCOM is not suitable for latency critical real-time applications. SATCOM supported ATS, AOC and AAC with up to 300 aircraft per spot beam (4 degree by 4 degree spot beam). Packet loss was experienced by SWIM and APC starting at 5 aircraft per spot beam. The potential bottleneck in the SATCOM system is the satellite-to-ground gateway link. To cover the CONUS, 100 spot beams from a satellite were needed.

- Aircraft-to-Aircraft Communications Network Results

The simulation results showed generally good air-to-air and air/ground coverage across the CONUS, based on the aircraft flight schedules, routes and aircraft density represented by the ASDI data used in the simulation. There were instances of disconnected aircraft (from the ground) during times when the aircraft did not have a complete path to a ground station. This occurs in sections of lightly traveled routes such as routes between the east and the northwest over areas such as Montana. A disconnected occurrence was also indicated as such when the number of hops between an aircraft to a ground station exceeded a maximum number of hops, which was configurable in the simulation. An aircraft RF range of 120 nm was represented as a mobile node with a range circle with 2 degree radius. The ground stations were placed at major airports and 21 selected airports provided the coverage for the CONUS.

Summary of Security Assessment

The security assessment considered security in context of the architectures and defined a security perimeter boundary to properly set the context of the security analysis of the technologies. The security perimeter included the physical and link layers and the access network layer. However, potential hackers (black hat hackers) operating on the ground-based networks further back from the aircraft/ground network in the overall end-to-end network topology were also considered as potential threats in the analysis. The following threats were identified and analyzed: jamming, scrambling, aircraft impersonation, rogue (fake) base station, key management breaches, attacks from man-in-the-middle hackers and attacks from black hat hackers. These threats were numerically analyzed on the extent of impact they would have on data integrity and loss of communications (percentage of system degraded or disrupted by the attack) and the required capabilities to effect the attacks (percentage estimate of likelihood the attack can be done given cost and complexity to do it). The product of the impact and likelihood of each threat to data integrity and communications was assigned a hazard level classification. The hazard level of each threat was compared against the safety objective of each ATM service to determine the level of security risk. A hazard level that is greater than the safety objective indicates a security risk. The safety objectives of the ATM application services were defined using the same set of classifications and were based on COCR requirements. Technical mitigations of the security risks were identified and analyzed.

A summary of the security assessment results are provided below.

- Cellular Network Results

The assessment of cellular networks showed that all data communication services can be supported without major security issues with the exception of very safety critical, future services such as the Autoexec service, which will require more robust security to protect it against threats. A service such as Autoexec is susceptible to jamming, scrambling and rogue base station threats.

- Satellite Network Results

Feeder links (satellite-to-ground station) were found to be susceptible to attack. Emerging and more prevalent UAVs were found to be a good platform from which to jam the downlinks in the feeder link. To mitigate this risk, the feeder link could be eliminated in lieu of user links between satellite and user terminals on the premises of ground-based users.

- Aircraft-to-Aircraft Communication Network Results

The self-organized aircraft-to-aircraft network, which is in the conceptual phase of development, was recognized as lacking security mechanisms at this point in its development. Without security mechanisms, it is susceptible to attacks such as jamming and impersonation. An aircraft-to-aircraft network uses non-centralized control as an ad hoc network, which provides some immunity to single point failures that can be experienced by centrally controlled networks.

Application of the self-organized cell concept and the concept of the decentralized network with appropriate security measures and key management were proposed to mitigate risks. Aircraft would form an ad hoc network to use space, time and frequency domain separation to allocate resources and provide security in a way to avoid the impact of attacks on single control points.

Other mitigation strategies include jammer localization and hacker monitoring, which is based on the observation that jammers and hackers are typically localized. By localizing the jammer and hackers through monitoring preventive measures can be implemented effectively.

6.2. RECOMMENDATIONS

Recommendations for further work are provided below. Further analysis, modeling and simulation are needed to define the requirements and approach for proof-of-concept activities to build and test systems to validate the requirements. Validated requirements can subsequently be used to help develop standards needed for implementations. The essential recommendations for future study are:

- Detailed analysis of the impact of low-altitude UAS, specifically in urban areas, on future NAS communications. The analysis should include harmonization strategies for UAS command and control links with traditional ATC communications as well as general integration of UAS information for situational awareness of the pilots and controllers.
- Develop high fidelity simulation models of the proposed architectures to perform tradeoff analyses and operational scenario-based simulations. In addition, by integrating these simulation models with other pre-existing NASA models, higher fidelity system models can be developed to aid future system design.

- One of the key challenges for applying FSO to aeronautical communications is the acquisition and tracking of aircraft moving at very high relative speeds. Therefore, a future study should undertake this challenge to develop technical approach and system design for aircraft acquisition and tracking to support FSO communications.
- Security analysis presented in this paper provides a high level assessment of the security threats, risks and their potential mitigation approaches. A future study should specifically expand this analysis to fully address the security vulnerabilities of the proposed architectures and develop mitigation approaches.
- RF spectrum is a very limited resource and its demand is increasing exponentially with time. Therefore, a future study should analyze the availability of effective spectrum for aeronautical communications and develop a technical approach for reuse and dynamic, on demand, allocation of spectrum.
- The aviation network of the future needs to be very dynamic with multiple air/ground connectivity options supporting simultaneous traffic flows with varied quality of service requirements and ad-hoc, self-configuring air-to-air networks. To maintain robust data flows and to assure low latency and jitter, future aeronautical networks must support sophisticated routing algorithms that can converge very quickly and impose very little system overhead. It is essential to research and design this routing algorithm soon such that it would be ready for standardization within the next ten years. This research should include management of multiple links for seamless inter-technology handovers and leverage currently evolving IP mobility standards.
- Similar to the routing challenges, aircraft architecture may also need to be investigated to facilitate such a dynamic network operation while ensuring security of the flight critical services and safety of flight.