NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**NETWORK-BASED MITIGATION OF ILLEGAL IMMIGRATION
IN AEGEAN SEA (GREECE)**

by

Dionysios Kotsifas

September 2010

Thesis Advisor:	Alex Bordetsky
Second Reader:	Eugene Bourakov

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Network-based Mitigation of Illegal Immigration in Aegean Sea (Greece)	**5. FUNDING NUMBERS**
6. AUTHOR(S) Dionysios Kotsifas	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ________________.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Illegal immigration is a serious concern of countries neighboring devastated parts of the modern world. Illegal migrants dreaming of a new life follow perilous routes, cooperating with smuggling networks. For a significant portion, their dream never comes true. Besides, smugglers are also responsible for other illegal activities, such as drugs and weapons trafficking.

Greece not only faces the problem of absorbing these immigrants from Africa and Greater Middle East countries, but it also has no chance to filter those migrants involved in dark networks. The Hellenic Coast Guard, lacking timely information on suspect vessels moving towards its territorial waters in the Eastern Aegean Sea, strives to be in the right place at the right time.

The need for an ever-present adaptive networking system able to provide reliable communication and sensor data to and from the areas of responsibility is more profound than ever.

This thesis examines the feasibility and constraints of applying modern networking technology, already successfully tested by NPS CENETIX TNT/test bed, on Aegean Sea islands as a concept of providing information to the Hellenic Coast Guard to enhance situational awareness and decision-making capability and thus increase overall effectiveness and efficiency while carrying out missions in that area.

14. SUBJECT TERMS Networks, Internet, Tactical Network Topology, Mesh, Situational Awareness Multi Agent System, Nodes, Wireless, Collaborative Environment, Point to Point Communications, Common Operating Picture	**15. NUMBER OF PAGES** 75
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

NETWORK-BASED MITIGATION OF ILLEGAL IMMIGRATION IN AEGEAN SEA (GREECE)

Dionysios Kotsifas
Major (P), Hellenic Air Force Academy, 1992

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2010

Author: Dionysios Kotsifas

Approved by: Alex Bordetsky
Thesis Advisor

Eugene Bourakov
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Illegal immigration is a serious concern of countries neighboring devastated parts of the modern world. Illegal migrants dreaming of a new life follow perilous routes, cooperating with smuggling networks. For a significant portion, their dream never comes true. Besides, smugglers are also responsible for other illegal activities, such as drugs and weapons trafficking.

Greece not only faces the problem of absorbing these immigrants from Africa and Greater Middle East countries, but it also has no chance to filter those migrants involved in dark networks. The Hellenic Coast Guard, lacking timely information on suspect vessels moving towards its territorial waters in the Eastern Aegean Sea, strives to be in the right place at the right time.

The need for an ever-present adaptive networking system able to provide reliable communication and sensor data to and from the areas of responsibility is more profound than ever.

This thesis examines the feasibility and constraints of applying modern networking technology, already successfully tested by NPS CENETIX TNT/test bed, on Aegean Sea islands as a concept of providing information to the Hellenic Coast Guard to enhance situational awareness and decision-making capability and thus increase overall effectiveness and efficiency while carrying out missions in that area.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION..1

A. BACKGROUND 1

B. VISION 4

C. OBJECTIVES 6

D. RESEARCH TASKS 7

E. SCOPE 7

F. METHODOLOGY 7

G. THESIS ORGANIZATION...7

II. NETWORK CONFIGURATION 9

A. NETWORKS OVERVIEW 9

1. Computer Networks...9

2. LAN 9

3. MAN 9

4. Mesh Network 10

5. Basic IEEE 802.11..11

6. Basic IEEE 802.16..11

7. OFDM 12

8. VPN Tunneling...12

B. WIRELESS SENSOR NETWORKS (WSN) 13

1. Key Terms and Definitions 13

2. WSN Concept 13

3. Sensor Node 14

4. Communication Link Node..14

5. NOC..14

6. Clustering in Sensor Networks 15

7. Real World Surveillance Sensor Networks Case Studies...............15

C. 80INPS/CENETIX/TNT TESTBED 19

1. The Backbone Network 19

2. The Stationary Network 20

3. Basic Collaborative Tools...22

4. TNT/MIO 10-02 Experimentation...24

III. CONCEPT OF NETWORK MODEL DESIGN.......................................27

A. SYSTEM REQUIREMENTS 27

B. OPERATIONAL REQUIREMENTS..29

1. Tactical Level 29

2. Operational Level..29

3. Strategic Level...30

C. SYSTEM ARCHITECTURE IN ACCORDANCE WITH OPERATIONAL DEMANDS...30

1. Single Cluster Mesh Sensor Network (Tactical Level)...................30

2. Grouped Cluster Mesh Sensor Networks (Operational Level)......32

D. NETWORKING....34
1. Communicating Through Nodes 34
2. Surveillance Via Sensors 37
3. Collaborating Through SA Tools 39
IV. ISLAND-BASED SURVEILLANCE NETWORK (CLUSTER) 41
A. NETWORK TOPOLOGY/TOPOGRAPHY 41
B. NETWORK'S COMMUNICATION SIMULATION TEST (SPEED)....45
C. SPEED'S APPLICATION FOR SIMULATION OF LESVOS NETWORK 48
D. RESULTS 49
V. CONCLUSIONS 53
A. CONCLUSIONS 53
B. OTHER APPLICATIONS....54
LIST OF REFERENCES 55
INITIAL DISTRIBUTION LIST 57

LIST OF FIGURES

Figure 1. Greek Aegean Sea Islands (From Google-Images) 1
Figure 2. The perilous trip (From Google-Images)..2
Figure 3. EU countries (From Google-Images)..3
Figure 4. Eastern Aegen Sea and territorial water line (From Google-Images)................4
Figure 5. Cross-border zone 5
Figure 6. Mesh network topology (From Wikipedia site)..10
Figure 7. Redline's video surveillance network topology in Kutahya City, Turkey (From Redline Communications site)..17
Figure 8. OFDM backbone of NPS Tactical Network Topology test bed (From CENETIX site)..20
Figure 9. NPS/CENETIX OFDM backbone (From CENETIX site).............................21
Figure 10. Bald Mountain, CA – CENETIX's OFDM station (From CENETIX site).....22
Figure 11. Cluster sensor network...28
Figure 12. Island-based cluster sensor network 31
Figure 13. Tactical-level network 32
Figure 14. Operational-level network 33
Figure 15. National-level network...34
Figure 16. Access Node AN-80i (From Redline Communications site)..........................36
Figure 17. Sensor node configuration 37
Figure 18. Nacimiento, CA-CENETIX's RN infrastructure-solar panels (From CENETIX site)..39
Figure 19. Head node configuration...40
Figure 20. Lesvos island cluster sensor network...41
Figure 21. Lesvos island topography 42
Figure 22. Lesvos cluster network AoR...42
Figure 23. Lesvos model network surveillance coverage 44
Figure 24. Sensor network of limited redundancy 45
Figure 25. Point-to-point analysis (From SPEED's Manual)...47
Figure 26. SPEED's application outcome..50
Figure 27. Basic and optional (mesh) extension of Lesvos network architecture............51

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AATD – Aviation Applied Technology Division (US Army)

AIS – Automatic Identification System

AN – Access Node

AMRDEC – Aviation and Missile Research Development and Engineering Center

AoR – Area of Responsibility

CCTV – Closed Circuit TV

CENETIX – Center for Network Innovation and Experimentation

CG – Coast Guard

CMS – Central Monitoring Site

COTS – Commercial-off-the-shelf

C2 – Command and control

DHS – Department of Homeland Security

DNDO – Domestic Nuclear Detection Office

DTRA – Defense Threat Reduction Agency

DTED – Digital Terrain Elevation Data

EO – Electro-optical

EU – European Union

FDM – Frequency Division Multiplexing

GHz – Gigahertz

GIS – Geographic Information System

GPS – Global Positioning System

HCG – Hellenic Coast Guard

ID – Identification

IEEE – Institute of Electrical and Electronics Engineers

IP – Internet Protocol

IR – Infrared

IT – Information Technology

LAN – Local Area Network

LMCO – Lockheed Martin Corporation

LLNL – Lawrence Livermore National Laboratory

LOS – Line Of Sight

MAC – Medium Access Control

MAN – Metropolitan Area Network

Mbps – Megabits per second

MS – Microsoft

NATO – North Atlantic Treaty Organization

NLOS – Non Line of Site

NOC – Network Operations Center

NPS – Naval Postgraduate School

OFDM – Orthogonal Frequency Division Multiplexing

OPCEN – Operations Center

POE – Point of Entry

PTP – Point to Point

PTZ – Pan Tilt Zoom

RCS – Radar Cross Section

RN – Relaying Node

SA – Situational Awareness

SAR – Search and Rescue

SN – Sensor Node

SPEED – Systems Planning Engineering and Evaluation Device

TNT – Tactical Network Topology

TOC – Tactical Operations Center

TOI – Target of Interest

UAV – Unmanned Aerial Vehicle

USCG – United States Coast Guard

USEUCOM – United States Europe Command

USV – Unmanned Surface Vehicle

VPN – Virtual Private Network

WAN – Wide Area Network

WiFi – Wireless Fidelity

WiMAX – Worldwide Interoperability for Microwave Access

WLAN – Wireless LAN

WSN – Wireless Sensor Network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Dr. Alex Bordetsky and Eugene Bourakov for their kindness, support, and dedication throughout my academic journey, as well as for the great experience I had working with them during CENETIX’s experimentations.

I would like also to thank Maj. Mike Kutsor (USMC), another CENETIX’s group student, for his kind collaboration in my thesis project.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Associated Press: Athens, Greece, 27 October 2009—“A small boat loaded with Afghan families smashed onto the rocks and sank off an island in the Aegean Sea on Tuesday, causing three immigrant women and five children to drown…”

Quite often deadly accidents highlight the plight of thousands of migrants who risk their lives every year to reach the European Union. Greece, and particularly its islands in the Aegean Sea—due to their proximity to the Turkish shoreline, is considered to be a primary entry point for illegal immigrants coming from Africa and Greater Middle East (Figure 1).

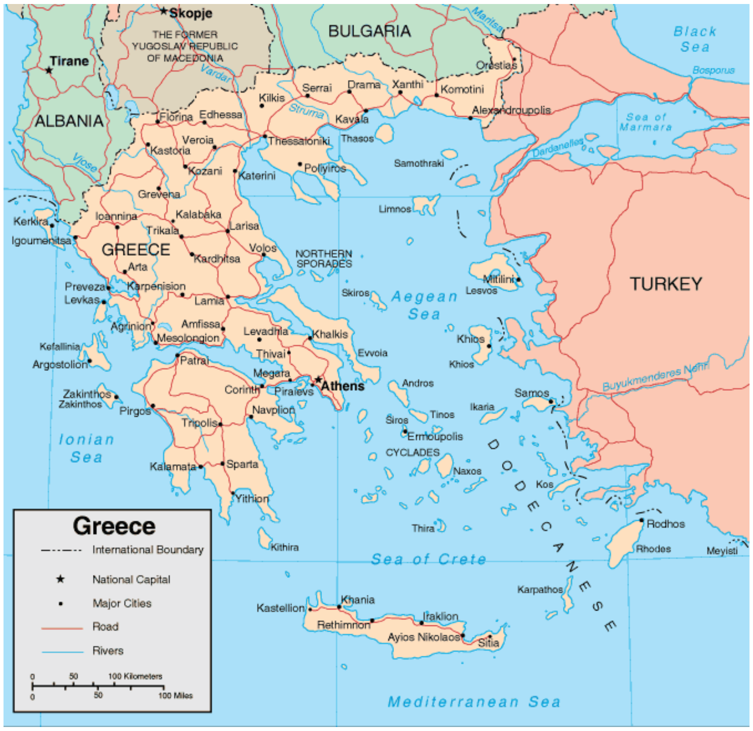


Figure 1. Greek Aegean Sea Islands (From Google-Images)

Illegal migrants, facilitated by smugglers aboard small, overcrowded, non-seaworthy vessels, cross into Greek territorial waters under perilous conditions (Figure 2). The tactic used by the smugglers is either to drag vessels with immigrants into Greek territorial waters and then abandon them as asylum seekers or to accompany them, pretending that they are also migrants. The Hellenic Coast Guard (HCG) is quite often one step behind in pursuing smugglers due to the lack of early warning for ongoing smuggling activities, which take place in short distances and timelines.

Figure 2. The perilous trip (From Google-Images)

In most cases, smugglers intend just to cross into Greek territorial waters because after that they are treated by the Greek Coast Guard as asylum seekers or, in extreme but frequent cases, as castaways according to international maritime law.

On the other hand, this continuous unfiltered flow of illegal migrants lacking identification documents has already caused a great impact on stability and security in Greece and other European Union (EU) countries (Figure 3).

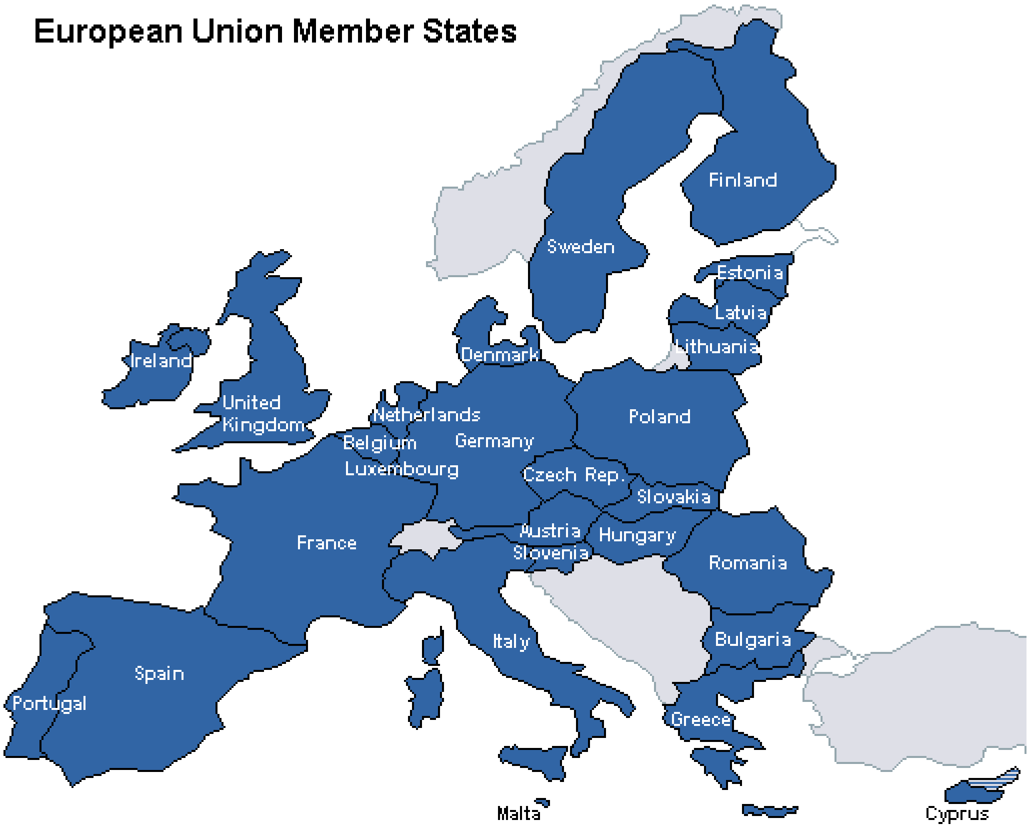


Figure 3. EU countries (From Google-Images)

Even if illegal immigration is an issue of primary concern for the Greek state, the particularities of the Aegean Sea, and especially the lack of timely information and the extremely short time available for response, makes the mitigation of potential smugglers a very tough issue. Apart from possible bilateral or multilateral diplomatic resolutions on this illegal activity, at the operational/tactical level, we can focus from the very beginning on the key word, "information." A kind of network-based coastal surveillance system could be the source of the required information for the efficient prevention of such illegal activities.

Rapid advancements in network components, and especially in wireless communications and mobile data devices, have lately made possible the practical use of wireless networks in many current military and law enforcement applications in a variety of environments, even in that of the archipelagic Aegean Sea. The research performed at the Center for Network Innovation and Experimentation (CENETIX) program within the

Naval Postgraduate School (NPS) and the extended experimentation under the framework of the Maritime Interdiction Operations (MIO)/Tactical Network Topology (TNT) test bed can contribute decisively to the design and development of such a network-based maritime surveillance system.

B. VISION

My vision involves placing a border surveillance system on the most critical islands in the Eastern Aegean Sea (Lesvos-Chios-Samos-Cos-Rhodes in Figure 4), based on the network technology already developed and applied by the CENETIX/TNT test bed.

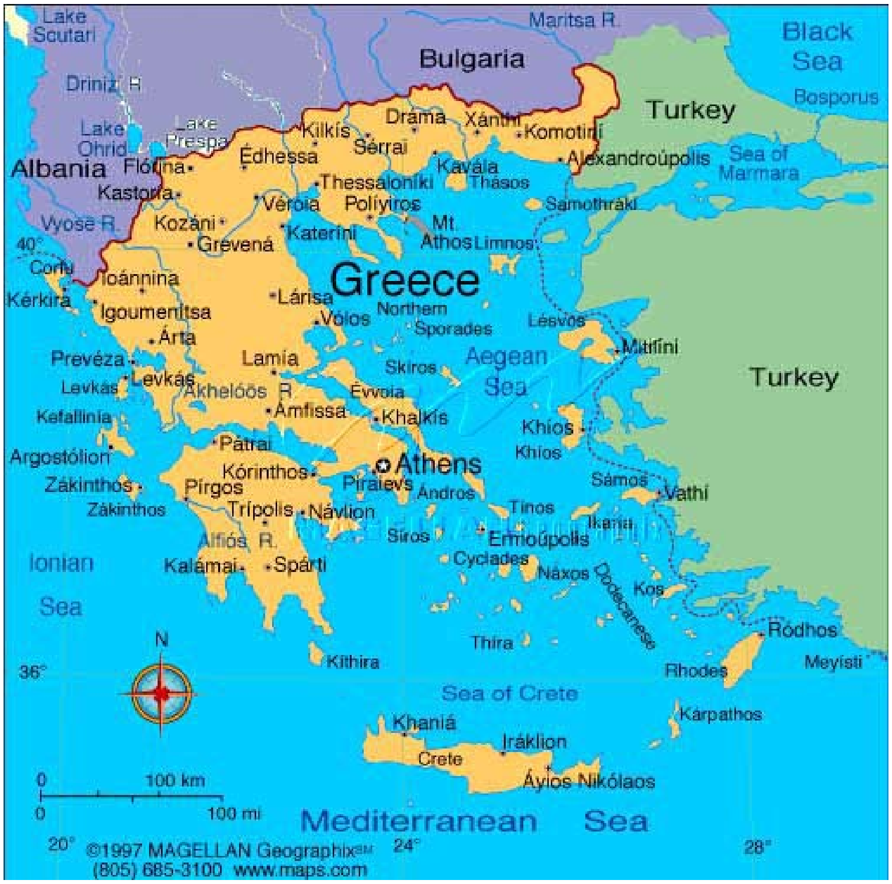


Figure 4. Eastern Aegen Sea and territorial water line (From Google-Images)

This synthesized system should be able to enhance maritime situational awareness, thus preventing unauthorized border crossings, reducing the number of illegal immigrants losing their lives in the Aegean Sea, reducing cross-border crime, and generally making law enforcement forces more efficient and productive in conducting their missions.

To this end, I imagine a system capable of providing 24/7/365 early warning of suspect vessels in the cross-border zone (Figure 5) for use by the Coast Guard in order to achieve perpetual vigilance and leading at least to a visible deterrent to potential perpetrators.

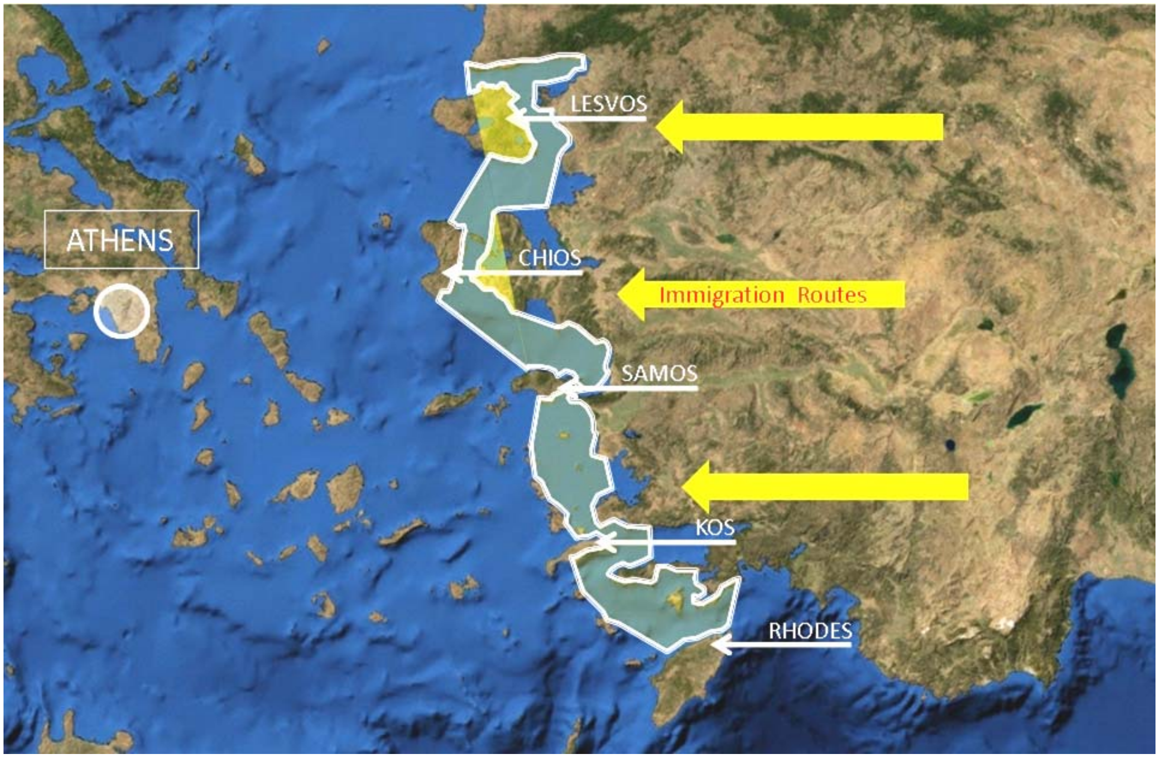


Figure 5. Cross-border zone

In parallel, such a system should be suitable not only for autonomous local use, but also to share a common real-time surface picture through an Aegean islands mesh network developed around the central node of the Hellenic Coast Guard Command and Control (C2) Coordination Center in Athens.

Taking into account the specific environment of the Aegean Sea and regarding the synthesis of such a system, I consider that the network would be comprised of subsystems able to provide electronic early warning of small vessels by maritime surveillance radar sensors and identification capabilities by electro-optical (EO) sensors for all weather conditions during both night and day. Regarding the mesh network, I find that it should be capable of circulating a live data stream (video, voice, etc.) in real-time or near-real-time.

Going further, such a system could be used as the core infrastructure for enhancing law enforcement and expanding maritime operational capabilities in cases such as search-and-rescue (SAR) operation, interdiction of drugs and weapons smuggling, natural and man-made disasters, port security, legal fishery enforcement, cleanup of dumping and accidental spills, and information collection for databases about illegal actions and their actors, etc.

Moreover, the value added by expanding such a mesh network to mobile nodes (aboard Coast Guard vessels) could greatly enhance the capability of an on-scene commander for any maritime incident in the region. At the end of the day, I consider that such an integrated system presents a challenging prospect, since it can serve as a potential force multiplier with time and cost savings in manpower and tasking.

C. OBJECTIVES

This research is being conducted to aid in the creation of a network-centric system sited on the Aegean Sea islands, intending to provide early warning capabilities and real-time maritime domain awareness to the Hellenic Coast Guard, for the timely interdiction of smuggling activities.

The ultimate goal is to identify a viable application and network configuration made by low-cost commercial-off-the-shelf (COTS) elements that will suit the Hellenic Coast Guard’s organizational needs in the maritime environment for use during law enforcement missions.

This research will also have the added benefit of being the base for any further similar applications on countering illegal activities and/or developments for all kinds of exploitation in the area of the Aegean Sea.

D. RESEARCH TASKS

The first task is to design the architecture of a tactical network-centric system for early warning, situational awareness, and timely interdiction of smuggling activities in the Eastern Aegean Sea. The second task involves identifying the feasibility of and major constraints associated with the operational usage of such a network-based early warning system.

E. SCOPE

The overall scope of this thesis is to design the architecture of a tactical network-based early warning system capable of enhancing situational awareness within maritime smuggling routes between the islands of the Eastern Aegean Sea and the Turkish shoreline.

F. METHODOLOGY

1. Studying the results of applying networks and sensors to MIO in previous experiments and recorded case studies.
2. Analyzing the requirements for a network-based early warning system for countering illegal immigration in the Aegean Sea.
3. Setting the requirements and specifications.
4. Designing the system's architecture.
5. Conducting the application's simulation test.
6. Analyzing results and presenting conclusions.

G. THESIS ORGANIZATION

This thesis is organized as follows: Chapter I includes all the introductory material regarding the motivation, scope and methodology behind the thesis field experimentation. Chapter II summarizes the theoretical background on basic terms and concepts regarding networking in the realm of surveillance and the relevant experimentation conducted by the NPS/CENETIX. It also includes a brief presentation of networked surveillance systems applied in the real world. Chapter III analyzes the system's requirements, specifications and architecture design. Chapter IV describes the network model architecture and a simulation test of its applicability. Chapter V presents the conclusions as well as the use and exploitation of such a network for further purposes.

II. NETWORK CONFIGURATION

A. NETWORKS OVERVIEW

1. Computer Networks

A computer network is a group of computers, servers, switches, routers, printers, scanners, and other devices that can communicate with each other and share information over some transmission medium. When the medium is radio waves or infrared signals instead of wires, it is called a wireless network.

2. LAN

A local area network (LAN) is a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide area network (WAN).
The following characteristics differentiate one LAN from another:

➢ Topology refers to the geometric arrangement of devices on the network. For example, devices can be arranged in a ring or in a straight line.

➢ Protocols are the rules and encoding specifications for sending data. The protocols also determine whether the network uses a peer-to-peer or client/server architecture.

➢ Media refers to how the devices are connected. Devices can be connected by twisted-pair wire, coaxial cables, or fiber-optic cables. Some networks do without connecting media altogether, communicating instead via radio waves.

LANs are capable of transmitting data at very fast rates—much faster than data can be transmitted over a telephone line—but the distances are limited and there is also a limit on the number of computers that can be attached to a single LAN. (LAN, n.d.)

3. MAN

A metropolitan area network (MAN) is a data network designed for a town or city. In terms of geographic breadth, MANs are larger than LANs but smaller than

WANs. MANs are usually characterized by very high-speed connections using fiber-optic cable or other digital media. (MAN, n.d.)

4. Mesh Network

Also called mesh topology, mesh is a network topology in which devices are connected with many redundant interconnections between network nodes. In a true mesh topology, every node has a connection to every other node in the network (Figure 6).

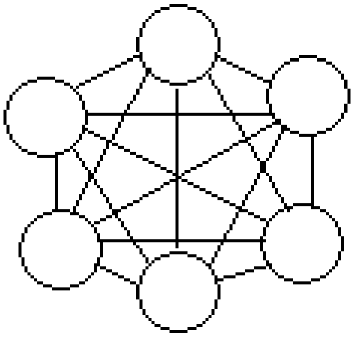


Figure 6. Mesh network topology (From Wikipedia site)

There are two types of mesh topologies: full mesh and partial mesh. Full mesh topology occurs when every node has a circuit connecting it to every other node in a network. Full mesh is very expensive to implement but yields the greatest amount of redundancy, so in the event that one of those nodes fails, network traffic can be directed to any of the other nodes. Full mesh is usually reserved for backbone networks. Partial mesh topology is less expensive to implement but yields less redundancy than full mesh topology. With partial mesh, some nodes are organized in a full mesh scheme but others are only connected to one or two other nodes in the network. Partial mesh topology is commonly found in peripheral networks connected to a full meshed backbone. (Mesh, n.d.)

NPS students J. Klopson and S. Burdian summarize in their thesis (Klopson & Burdian, 2005) the following regarding wireless mesh networking: “The biggest advantage of mesh networking is that it decentralizes the network infrastructure. In a client-server configuration, every node on the network must access a common server.

With a standard wireless access point, every node accessing the system must share the bandwidth provided by that single access point. The great benefit of a mesh topology is that the nodes communicate with each other instead of having to reach all the way to the access point itself. This has several advantages. First, the network can grow exponentially larger than a single access point network since nodes that are too far away from the access point can still remain connected to the network by "hopping" through nearby peers. Second, nodes are generally not limited by a single point of failure; they must be within range of several other nodes, so if one goes down, they can simply route through one of the other nearby nodes. Third, limited bandwidth improves as more nodes are added since the additional nodes each take on a share of the work, the opposite of a standard single access point network in which each computer added further subdivides the shared bandwidth."

5. Basic IEEE 802.11

The terms "802.11" and "802.11x" refer to a family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless LAN (WLAN) technology. The 802.11 type specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted these specifications in 1997.

There are several specifications within the 802.11 family. For example 802.11g applies to wireless LANs and is used for transmission over short distances at up to 54 megabits per second (Mbps) in the 2.4 gigahertz (GHz) bands but, in general, provides moderate throughput at moderate ranges. (802.11, n.d.)

6. Basic IEEE 802.16

Commonly referred to as WiMAX, 802.16 is a specification for fixed broadband wireless MANs that use a point-to-multipoint architecture. Published in April 2002, the standard defines the use of bandwidth between the licensed 10 GHz and 66 GHz frequency ranges and between the unlicensed 2 GHz and 11 GHz frequency ranges and defines a media access control (MAC) layer that supports multiple physical layer specifications customized for the frequency band of use and their associated regulations.

The 802.16 specification supports very high bit rates in both uploading to and downloading from a base station for distances up to 30 miles to handle such services as Internet Protocol (IP) connectivity, Voice over IP (VoIP), and time-division multiplexing (TDM) voice and data. (802.16, n.d.)

7. OFDM

Orthogonal Frequency Division Multiplexing (OFDM) is a frequency division multiplexing (FDM) modulation technique for transmitting large amounts of digital data over a radio wave. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of crosstalk in signal transmissions. OFDM technology is used in 802.11a WLAN, 802.16 and WiMAX. (OFDM, n.d.)

8. VPN Tunneling

A virtual private network (VPN) is a data network having connections that make use of public networking facilities. The VPN part of a public network is set up “virtually” by a private-sector entity to provide public networking services to small entities. With the globalization of businesses, many companies have facilities across the world and use VPNs to maintain fast, secure, and reliable communications across their branches.

VPNs are deployed with privacy through the use of a tunneling protocol and security procedures. A tunnel is a connection that forms a virtual network on top of a physical network. In computer networking, a tunnel resembles a telephone line in a public switced telephone network. VPNs typically rely on tunelling to create a private network that reaches across a public network. Tunneling is the process of encapsulating packets and sending them over the public network. (Mir, 2007)

B. WIRELESS SENSOR NETWORKS (WSN)

1. Key Terms and Definitions

- A sensor is a transducer that converts a physical phenomenon, such as heat, light, sound or motion, into electrical or other signals that may be further manipulated by other apparatus.
- Network topology is a connectivity graph where nodes are sensor nodes and edges are communication links. In a wireless network, the link represents a one-hop connection, and the neighbors of a node are those within the radio range of the node.
- Routing is the process of determining a network path from a packet source node to its destination.
- Geographic routing is the routing of data based on geographical attributes such as locations or regions.
- Collaborative processing involves sensors cooperatively processing data from multiple sources in order to serve a high-level task. This typically requires communication among a set of nodes.
- Task may refer to either high-level system tasks, which may include sensing, communication, processing, and resource allocation, or application tasks, which may include detection, classification, localization, or tracking.
- Detection is the process of discovering the existence of a physical phenomenon. A threshold-based detector may flag a detection whenever the signature of a physical phenomenon is determined to be significant enough compared with the threshold. (Dahlman, Parkvall, Bovik & Beming, 2009)

2. WSN Concept

The concept of wireless sensor networks (WSNs) is based on the combination of radio communication, processing and sensing, which raises the possibility of thousands of potential technological applications. The key advantage of WSNs in general is their ability to match the difference between the remote physical world and the virtual domain by gathering useful data from the first and sending them to the other for processing and analysis. The scope of networked sensors is to enhance sensing capability.

One of the major categories of such applications is that of surveillance and security sensor networks. This kind of network is comprised of a number of wireless linked nodes placed at fixed sites in a specified geographical area responsible for continuously monitoring for any intrusion or abnormality.

3. Sensor Node

A typical sensor node consists mainly of a sensing unit, a processor with memory, a power unit and a wireless transceiver component. All the processes within the sensor node are synchronized by a local clocking and synchronizing system. The analog signals produced by the sensors, based on the observed event, are converted to digital signals by the converter and then fed into the processing unit. The processor performs certain computations on the data and, depending on how it is programmed, may send the resulting information out to the network.

4. Communication Link Node

A communication node has the ability for bidirectional or multidirectional (mesh) linkage with any other node within a specific distance from it. The link breaks if the node moves to a distance greater than that.

5. NOC

A network operations center (NOC) is the physical space from which a typically large telecommunications network is managed, monitored and supervised. The NOC coordinates network trouble reporting; provides problem management and router configuration services; manages network changes; allocates and manages domain names and IP addresses; monitors routers, switches, hubs and uninterruptible power supply (UPS) systems that keep the network operating smoothly; manages the distribution and updating of software; and coordinates with affiliated networks. NOCs also provide network accessibility to users connecting to the network from outside of the physical office space or campus. (NOC, n.d.)

6. Clustering in Sensor Networks

The term clustering in sensor networks is used to describe the partitioning of a region being sensed into equally loaded clusters of sensor nodes. A cluster in a network resembles a domain in a computer network. Different types of sensors can also be deployed in a region forming a cluster network with irregular topology. Communicating nodes are normally linked by a wireless medium, such as radio. Several clusters can be interconnected to the base station; each cluster contains a cluster head responsible for routing data from its corresponding cluster to a base station. (Mir, 2007)

7. Real World Surveillance Sensor Networks Case Studies

a) City-Wide Video Surveillance and Remote Monitoring for City in Mexico

Challenge: To monitor traffic flow and improve security for a large tourist population, a state in Mexico installed 350 traffic cameras in select locations throughout the capital city. Laws protecting Mexico's historic buildings prohibit even the government from disrupting the surrounding soil or attaching equipment to the exterior of the city's historic architecture, necessitating a wireless closed-circuit TV (CCTV) network. This would require the highest modulation and lowest latency possible in a single sector to keep the maximum throughput available for a clear video image. Any delays in the transfer of data can make a catastrophic difference in a police investigation.

Solution: A broadband wireless CCTV network infrastructure was recommended with connection speeds up to 108 Mbps using Redline's AN-80i, mounted on utility poles already in place throughout the city. The coverage radius was defined according to a propagation study that enabled complete coverage of every phase of the project and compensated for line-of-sight (LOS) issues that are common in urban areas.

Result: The surveillance network provides greater safety for the city's citizens and visiting tourists. Real-time video makes a real difference. The network gives public safety officials a constant, live bird’s-eye view of activity in bus stops, on street corners and in traffic to provide early detection of suspect activity and emergency scenarios. (Redline Communications, 2010a)

b) Turkish National Police with City-Wide Video Surveillance

Challenge: The police in Kutahya City, Turkey, required a reliable, secure, low-cost and high-bandwidth network for their 24-hour city-wide video surveillance project. The project entailed the deployment of multiple video surveillance cameras throughout the city of Kutahya. Deploying the high-capacity surveillance network posed a challenge due to interference of urban obstacles, which necessitated the use of many non-line-of-site (NLOS) network links.

Solution: The Redline Company recommended the installation of a broadband wireless communication system (RedMAX™ WiMAX) able to provide secure and reliable high-speed connections in NLOS conditions.

RedMAX base stations were deployed throughout the city along with RedMAX SU-Os (Outdoor Subscriber Units). Redline’s AN-80i products were used to backhaul the connection to police headquarters (Figure 7).

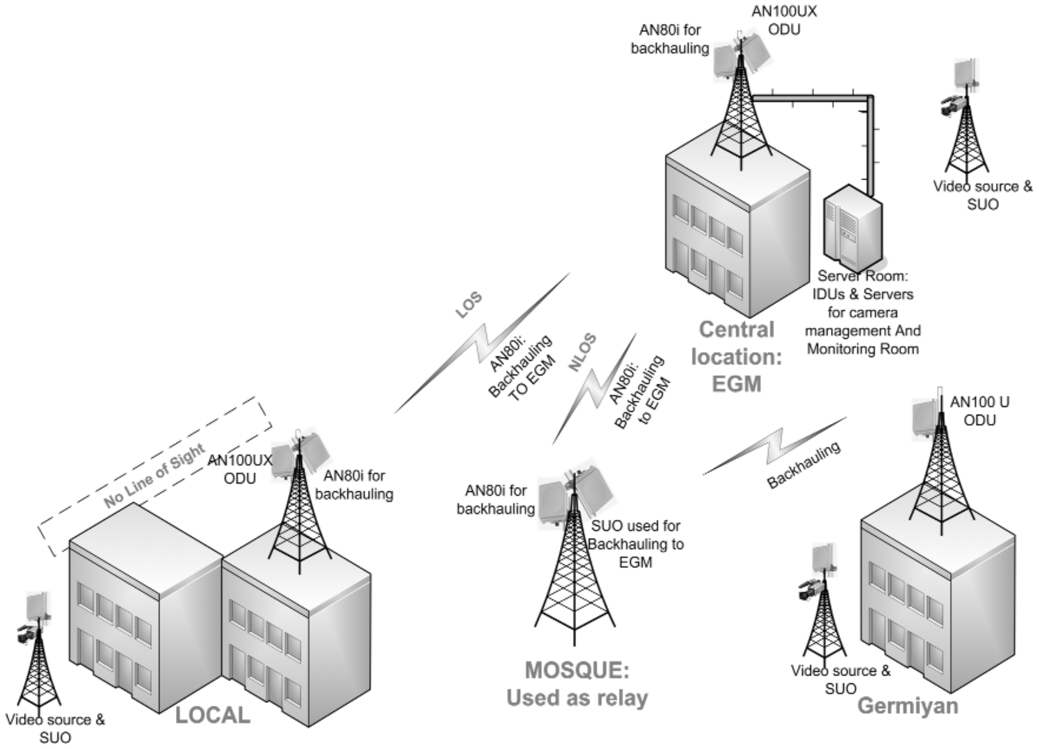


Figure 7. Redline's video surveillance network topology in Kutahya City, Turkey (From Redline Communications site)

Result: The Turkish police can now depend on a reliable high-speed network for improved video surveillance and enhanced public protection. Three RedMAX base stations were installed to achieve city-wide wireless coverage to connect the police department's video surveillance system. Coverage of 17 km x 7 km has been created and achieved through the installation of base stations in Kutahya. Within this area, 35 surveillance cameras, both pan-tilt-zoom (PTZ) and fixed, and three license plate recognition systems on three separate highways with 12 fixed cameras have been deployed. The central monitoring system for the network is situated at the local police station (EGM). Each RedMAX base station is connected by an AN-80i backhaul link. The EGM base station location consists of one RedMAX AN-100UX sector controller connected to two 60degree antennas. Four movable cameras (2.5 Mbps/camera) are then connected to this sector controller at EGM through four SU-Os located at an average distance of 2.5 km (1 LOS and 3 NLOS). The second site, Local, houses a base station that consists of three AN-100UXs, two with one 60-degree antenna each, and the third with two 60-degree antennas. Fixed and nomadic cameras are connected through 13 SU-Os (most of them NLOS) and once again backhauled to EGM via Redline's AN-80i. The third site, Germiyan, is connected to EGM via a relay site. The base station at Germiyan transmits to a RedMAX SU-O on the relay site, which, in turn, is connected to EGM via an AN-80i backhaul unit. (Redline Communications, 2010a)

c) Homeland Security Network-Enabled, Great Lakes Wide-Area Radar Surveillance

Sicom Systems, Ltd. develops low-cost radar surveillance solutions, which are well-suited for addressing international border security (IBS) missions and critical infrastructure protection (CIP) missions. They provide all-weather, day-night, situational awareness with automated, advance warning of possible terrorist or smuggling threats. As a result of post-9/11 security threats, these capabilities are particularly needed along the extensive waterways bordering Canada and the United States.

Sicom's Accipiter Radar is a low-cost, network-enabled, digital radar solution that can provide effective, wide-area radar surveillance in and around large bodies of water. Shore-mounted radar has a visual LOS that can survey thousands of square kilometers of lake surface. The entire western half of Lake Ontario is within radar coverage. Alerts and situational awareness information can be communicated to a central monitoring site (CMS), where they can be integrated using data fusion software to create an overall picture for use by authorities. Alerts can be designed to provide warning of potential asymmetric threats directed towards large vessels on the water, suspicious activity, or perimeter breaches associated with shoreline critical infrastructure.

Several advantages using Accipiter technology are apparent. Automated detection and tracking advantages result from the use of Sicom's proprietary radar signal processing and tracking algorithms. The Accipiter display provides real-time situational awareness through the use of specially designed overlays of processed radar and map information. A geographic map shown on the bottom layer with processed radar plan position indicator (PPI) imagery overlaid in such a way that returns from the surrounding shorelines are clearly visible in yellow color. Radar detections (plots) from the current scan are shown as green circles on the water. Several track symbols are shown along with track labels. Plots and tracks are uniquely time-stamped and maintained in a track database so they can be archived indefinitely as well as communicated in real-time to the CMS. Plots and tracks are also geo-located in real-time so that target coordinates are readily available. Target positions in local radar coordinates, map latitude and longitude, as well as Universal Transverse Mercator (UTM) coordinates are provided. Playback and reprocessing of plots and tracks at rates many times faster than real-time allow archives to be used for intelligence gathering, distribution, and prosecution. Additional information can be obtained by contacting ACCIPITER Radar Technologies, Inc. (Sicom Systems, 2004)

C. NPS/CENETIX/TNT TESTBED

1. The Backbone Network

The current CENETIX/TNT-MIO experimentation network uses OFDM 802.16 technology to provide a long-haul link, enabling high-bandwidth connectivity up to 54 Mbps. The test bed, as shown in Figure 8, enables a multiplatform plug-and-play environment for emerging sensor, unmanned vehicles, and decision maker networks, in which a terrestrial long-haul wireless network is deployed by the OFDM backbone, and further extended by unmanned aerial vehicles (UAVs), air balloons, light reconnaissance vehicles (LRVs) on the ground, unattended sensors, and mobile operations centers. It utilizes Redline Communications technology a manufacturer of wide range OFDM equipment.

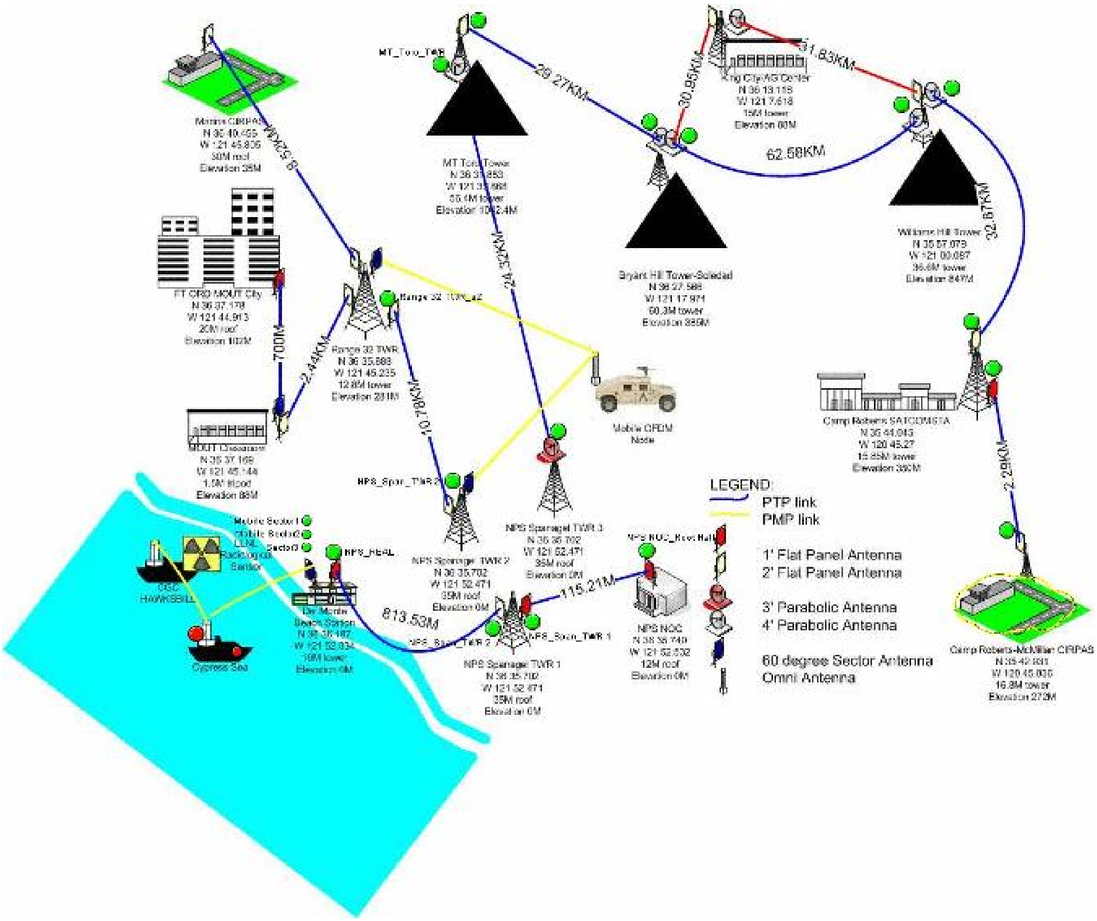


Figure 8. **OFDM backbone of NPS Tactical Network Topology test bed (From CENETIX site)**

2. The Stationary Network

For the creation of the stationary part of the existing 802.16 wireless TNT network, several pairs of Redline Access Nodes-50 (AN-50e) were used. The AN-50e consists of an IP-enabled high-frequency radio and outdoor transceiver capable of providing a long-haul 802.16 wireless link between stationary nodes. Thus, the extension of a terrestrial network from NPS (Monterey) to Nacimiento Lake for the needs of CENETIX and its collaborative centers became feasible, as shown in Figure 9.

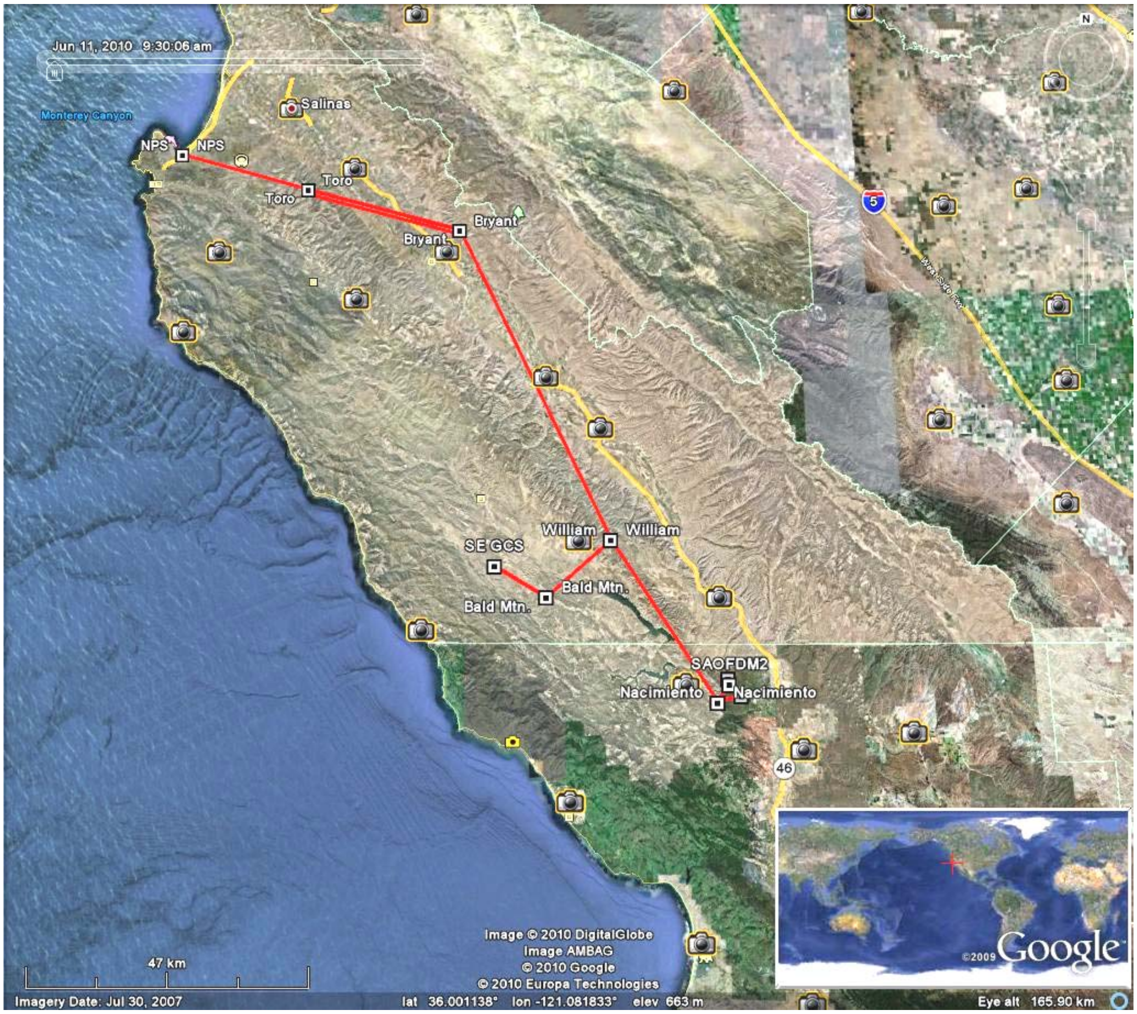


Figure 9. NPS/CENETIX OFDM backbone (From CENETIX site)

Each radio is mounted on permanent communication towers in LOS distances which provide the point-to-point signals transmission (Figure 10). Further extension of the network is accomplished through the use of the Internet, which bridges the San Francisco Bay Area with the above-mentioned 802.16 backbone. At the end of the northern part, a video camera provides live video streaming from the Golden Gate area via the communication transceiving installations directly to the NPS/CENETIX NOC. Then the NOC serves as a network bridge between the NPS Intranet and the Internet. (Naval Postgraduate School, 2010)

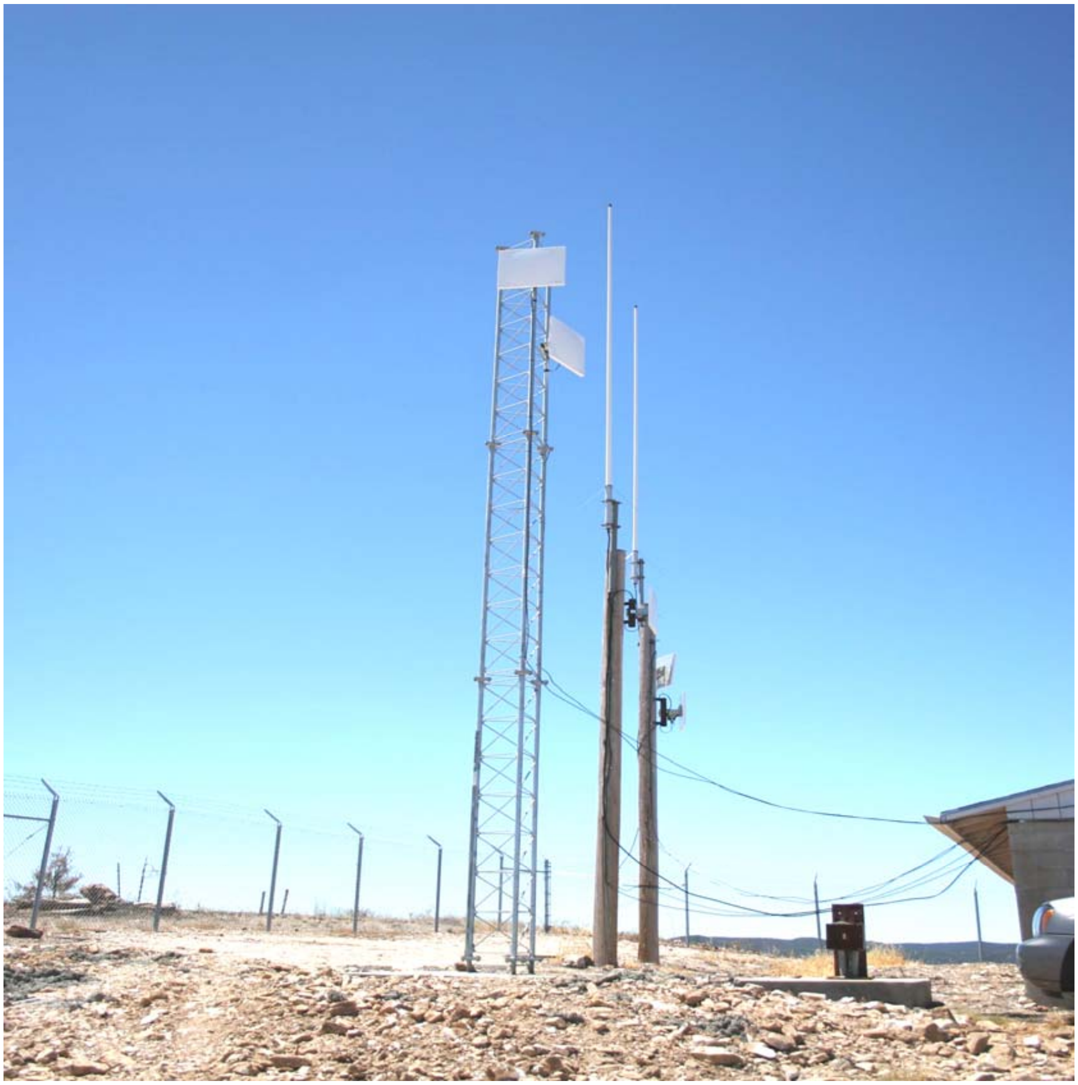


Figure 10. Bald Mountain, CA – CENETIX's OFDM station (From CENETIX site)

3. Basic Collaborative Tools

a) Situational Awareness (SA) Multi-Agent System

The software used by NPS/CENETIX regarding the situational awareness is the (SA) Multi-Agent System, which provides real-time video and position information for all participating assets and targets. It was developed by Dr. Alex Bordetsky and Eugene Bourakov at NPS in 2002, and since then, it has undergone numerous upgrades to support the needs for SA in the modern battlefield environment. The area of operations is depicted via maps or charts as the background layer of the screen while all players are represented by corresponding icons. The geo-location of all players is inserted into the system via Global Positioning System (GPS) or manually via coordinates. The operational picture is stored to the system's database and any change in that picture updates the system's data. Then the data is retransmitted to the rest of the agents in real-time through the established network. (Klopson & Burdian, 2005)

Klopson and Burdian in their thesis (2005) have extensively analyzed this software tool and also given guidance on how to use it.

b) GROOVE Virtual Office 3.0

GROOVE is the software tool used for a server-client type communication linkage between the elements of a network for the secure transfer of data. CENETIX, in general, uses this software more for discussion, instant messaging, chatting and data repository functions throughout the duration of the experiments.

Microsoft has named this program Microsoft Share Point Workspace 2010. "The new name for Microsoft Office Groove expands the boundaries of collaboration by allowing fast, anytime, anywhere access to your Microsoft SharePoint team sites. Synchronize SharePoint Server 2010 document libraries with SharePoint Workspace so you can access, view, and edit files anytime and anywhere from your computer. Lists such as Discussion, Tasks, and custom lists are supported as well. You can even synchronize Business Connectivity Services lists so access to your backend systems is even easier. SharePoint Workspace 2010 ushers in an entirely new way of working with your SharePoint team sites". (Microsoft, 2010)

For further details on Groove software, refer also to Klopson and Burdian (2005), in which they have extensively analyzed it, or to Microsoft's web page for relevant up-to-date information.

In total, the use of Groove in combination with SA Agent in a wireless network environment has been proved by CENETIX to be versatile and valuable for the creation of a Common Operating Picture (COP) for the participating units.

4. TNT/MIO 10-02 Experimentation

The last NPS CENETIX experimentation took part 7–17 June 2010, under the title, “TNT/MIO 10-02 - Networking and Interagency Collaboration on Small Craft Maritime-sourced Nuclear Radiological Threat Detection and Interdiction”. The MIO 10-2 experiment was part of a unique field experimentation campaign, which was conducted jointly with Lawrence Livermore National Laboratory (LLNL). The project recently became a critical part of the Global Initiative for Combating Nuclear Terrorism, spearheaded by the Department of Homeland Security (DHS) Domestic Nuclear Detection Office (DNDO) and the Defense Threat Reduction Agency (DTRA). It is a collaborative effort supported by United States Special Operations Command (USSOCOM), the United States Coast Guard (USCG), first responders in the San Francisco Bay Area, the Port Authority of New York-New Jersey, the Lockheed Martin (LMCO) Center for Innovation (East Coast), the United States Army Aviation Applied Technology Directorate (AATD) at Fort Eustis (East Coast), the United States Army Aviation and Missile Research Development and Engineering Center (AMRDEC), and overseas partners from the Swedish Naval Warfare Center, the Swedish Defense Research Agency (FOI) and Viking 11 program, the University of Bundeswehr, the Bundeswehr Center for Transformation, and the North Atlantic Treaty Organization (NATO) Maritime Interdiction Training Center in Souda Bay, Greece. The overseas part of MIO 10-2 was also supported by German operators from the 1st Battalion, 10th Special Operating Forces (SOF) Group assigned to United States Europe Command (USEUCOM). The MIO 10-2 experiment represents the first phase of 2010 experimentation events, in which the NPS-LLNL team will continue to explore the use of networks, advanced sensors, and collaborative technology for supporting integrated detection and interagency collaboration to counter small craft-sourced nuclear and radiological threats.

The goal for the MIO 10-2 experiment was to extend the operational horizon for small craft-sourced globally distributed threat countering by exploring a set of new models as follows:

a. Integrated detection and interdiction of small craft-sourced nuclear and radiological threats to US installation overseas. This included:

➢ Network-enabled swimmer detection of small craft-sourced threats at overseas points of entry (POEs) (Germany, Greece);

➢ Collaboration between US experts and overseas POE operators on network-controlled choke point setup, drive-by primary and secondary screening, and stand-off detection at high-speed pursuit (Eckernfoerde, Germany);

➢ Modeling application of unmanned surface vehicles (USVs) to small craft screening and pursuit (US experts, POE operators) by remotely controlled maneuvering of POE-manned patrol boats (Eckernfoerde, Germany);

➢ Ground tracking of illicit material transfer to US military sites, collaboration between US units in a foreign country, foreign operations center (FOI-Sweden, University of Bundeswehr and US remote experts), on losing, finding, and tagging the ground target, resolving threat uncertainty through source detection and adjudication (Germany, direction North-South);

➢ Open-waters tracking of another source transfer to the overseas POE, which was close to the collocated NATO and US installation sites (Mediterranean, Souda Bay-Greece);

➢ Collaboration between the patrol crews from different countries on the target small craft tracking, choke point screening, pursuit, and interdiction, combined with the situational awareness transfer and UAV integration (Souda Bay, Greece,).

b. Domestic, network-enabled experimental daily detection service (San Francisco Bay).

For the first time in the MIO experimentation campaign, the NPS-LLNL team integrated network-enabled detection, with reach-back to experts, into the daily patrol activities of two Marine Police boats and USCG vessel crews. This was provided for long-term observation data on daily networking and collaborative command and control patterns occurring between and during the source detection events. (CENETIX, 2010)

THIS PAGE INTENTIONALLY LEFT BLANK

III. CONCEPT OF NETWORK MODEL DESIGN

A. SYSTEM REQUIREMENTS

Countering illegal immigration and related smuggling activities in the Eastern Aegean Sea can be effectively accomplished through a well-designed network, providing maritime domain situational awareness and early warning capabilities to HCG forces. Surveillance to mitigate such illegalities must be deployed across Greece’s territorial waters in the Eastern Aegean on a permanent base. The target, such as a smuggler’s fishing boat, is usually conducting legal activities until it crosses into territorial waters. Then it has accomplished its mission. Illegal migrants are usually abandoned in the middle of the sea. The need for a shore-based surveillance system aimed at detecting suspicious activities in the area between the Eastern Aegean Sea’s Greek islands and the Turkish shoreline is greater than ever.

Taking into account the particularities of that area, it is clear that a number of radar sensor apparatus, capable of detecting a moving vessel with a small radar cross section (RCS), should be interconnected through a network base in order to provide the required awareness in the cross-border zone. (Nohara et al., 2005) Such sensors should also include EO capabilities provided by high PTZ video cameras to support the track’s identification process when needed. This network of several geographically separated sensor nodes should be remotely controlled and collectively monitored by operators’ workstations through the use of wireless networking technology (Figure 11).

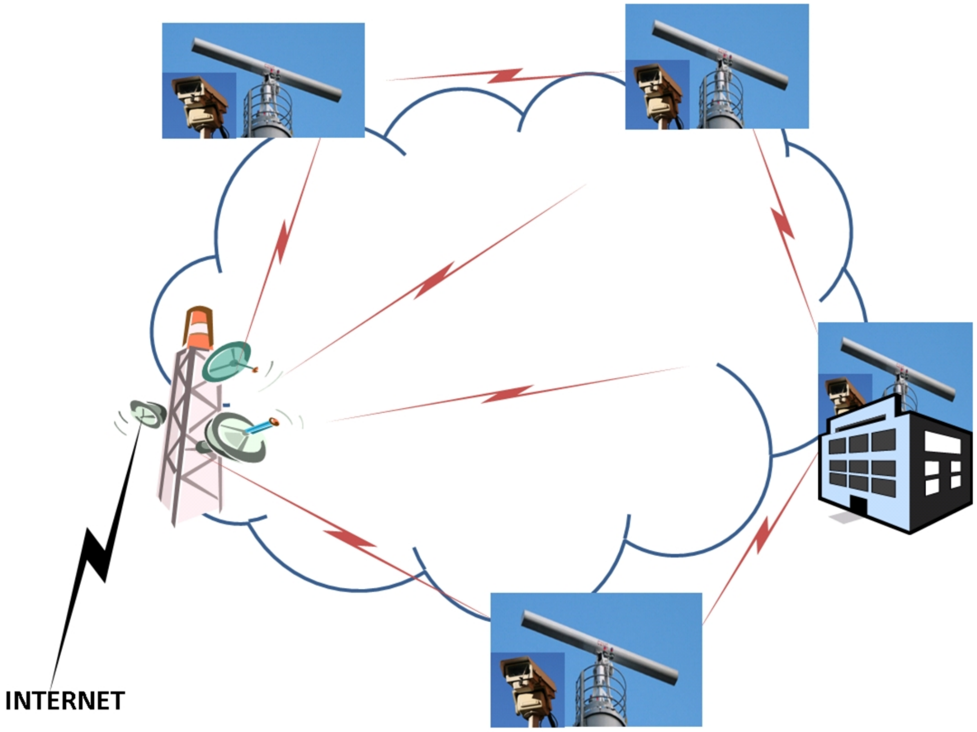


Figure 11. Cluster sensor network

In general, the system should be considered as a low-cost (purchase, operation and maintenance) practical solution based on the technologies already developed and successfully used by the CENETIX/TNT test bed, to cover the above mentioned needs. In particular, it should also meet the following specifications, requirements and characteristics:

➢ Highly reliable 24/7 radar surveillance operation under all weather conditions with automatic detection and tracking capabilities.

➢ User friendly, computer-based control and display, single-person operated with modifiable and upgradable software. (Israel Aerospace Industries Systems, 2009)

➢ Each node to be relatively small, and easy land-mountable.

- Single composite picture from whole network area of responsibility (AoR), clutter-eliminating radar display including map layer background, with automated threat detection and modifiable alert provision.
- EO capabilities on demand, in slaved and autonomous mode.
- Track data to include at least heading, velocity, track history, Geographic Information System (GIS) positioning, and Automatic Identification System (AIS) data if available. (Seibert et al, 2006)
- Long storage memory capability for keeping target tracks' radar and EO data available for investigation, prosecution and intelligence analysis for suspect routes and patterns identification.
- Internet connection capability for the establishment of a larger network through VPN tunneling as well as for further remote monitoring and control.

B. OPERATIONAL REQUIREMENTS

The requirements at each level can be described as follows:

1. Tactical Level

- Radar detection capability up to 30 km for very small RCS boats.
- EO remote surveillance and identification capability for relatively long distances. Infrared (IR) capabilities to be included for identification purposes.
- Real-time streaming of nodes data to the head node/Tactical Operations Center (TOC).
- Tracks to be displayed by their geo-location in real-time in order to be directly exploitable from the involved patrolling forces. Data for target location should be also provided in several forms (azimuth-range, geographic coordinates).
- 24/7 nodes maintenance checking capability from the head node.

2. Operational Level

- Cluster network connectivity for data sharing in real-time. (Nohara, Weber, Jones, Ukrainec & Premji, 2008)
- Security provisions in data streaming.

- SA tools for collaboration purposes between the cluster networks.

3. Strategic Level

- Future extension capability of the sensor network and connection compatibility provisions for different kinds of sensors.
- Real-time data streaming to and from the end node through SA tools.
- Security in data streaming.

C. SYSTEM ARCHITECTURE IN ACCORDANCE WITH OPERATIONAL DEMANDS

1. Single Cluster Mesh Sensor Network (Tactical Level)

The architecture of the system depends primarily on the operational demands. Going step by step, in order to fulfill the needs at the tactical level, we should design the lower level of the system as that of an autonomous cluster sensor network deployed on each major Eastern Aegean Sea Island (Lesvos-Chios-Samos-Kos-Rhodes), as shown in Figure 12.

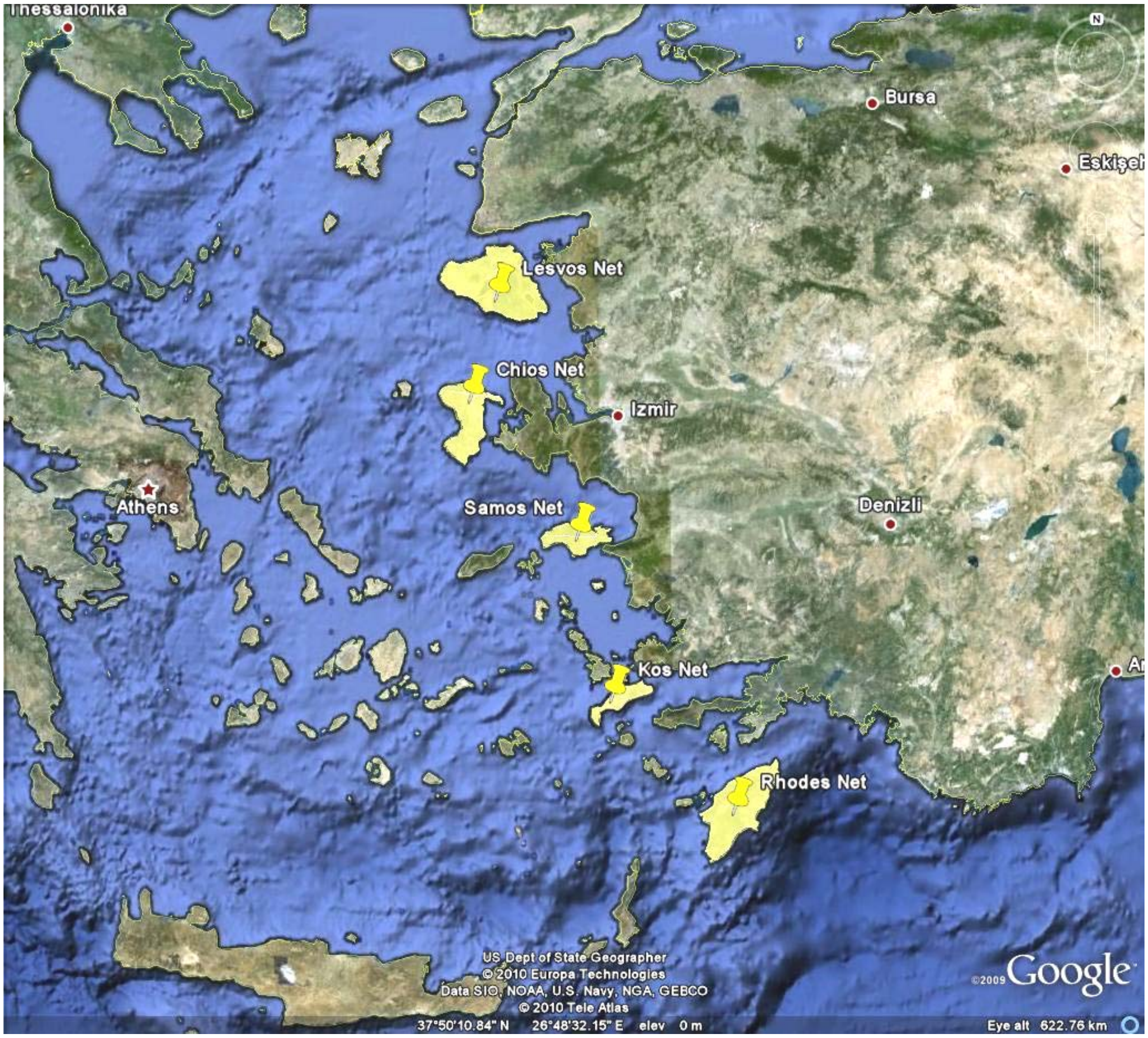


Figure 12. Island-based cluster sensor network

A cluster network would be comprised of sensor and communication nodes as well as a TOC, preferably collocated with the head node. The sensor nodes perform not only the basic sensing duty, but also general purpose processing and networking. The data from the sensor nodes are transmitted through each other to the head node, which provides the capability for presenting the sensors' aggregated picture, data storage, remote control, and WAN connectivity for further extension of the network. Thus, each cluster network provides the capability for situational awareness coverage on its corresponding area of responsibility, as shown in Figure 13.

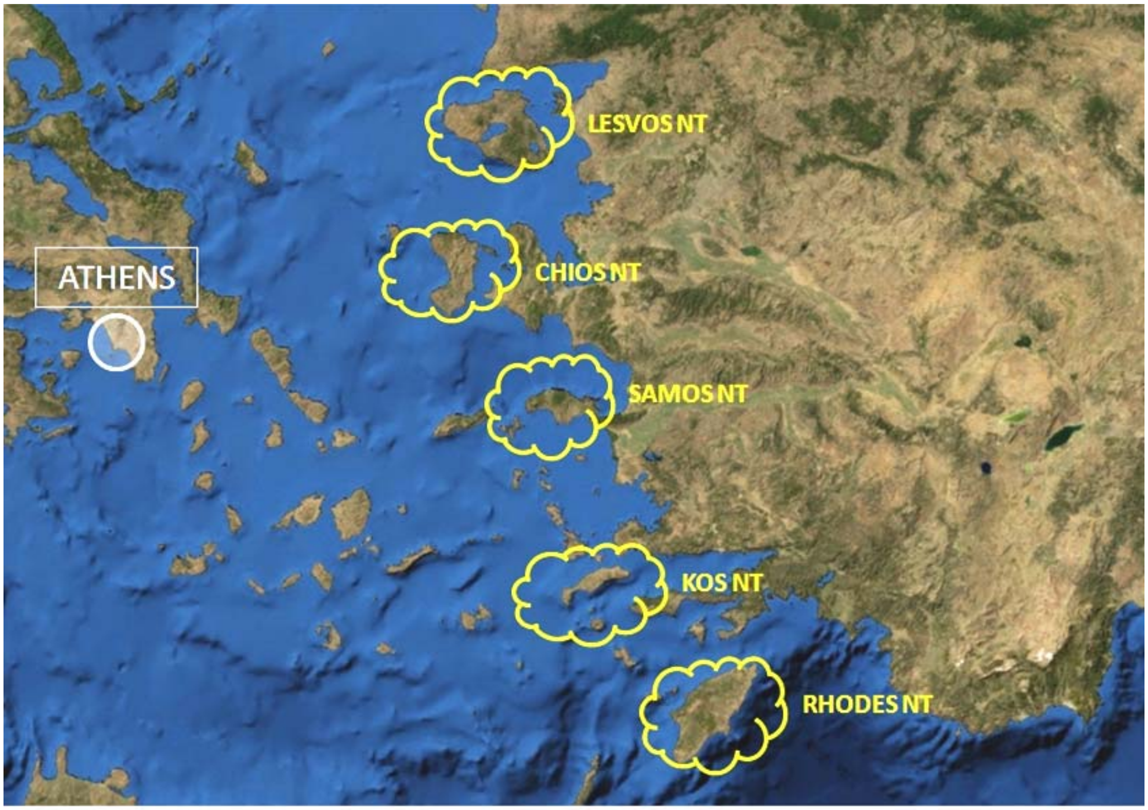


Figure 13. Tactical-level network

2. Grouped Cluster Mesh Sensor Networks (Operational Level)

Going further and discussing the operational level and the need for a more collective approach to the issue, the system should be expanded by interconnecting all the clusters (island-based networks). Every single cluster head node has the ability to cooperate with its adjacent cluster network and transfer data on targets and activities taking part in their respective AoRs. In parallel, they can transfer data regarding suspect vessels, smugglers, and so forth. In such a case, the overall system resembles that of an Eastern Aegean Sea electronic “fence” providing a common operational picture and data sharing to all network users and, of course, offers a more collective manipulation of the issue at that level (Figure 14). This can be accomplished by the use of broadband technology for connecting the relaying nodes of the cluster networks through Internet VPN tunneling. In such architecture, one of the TOCs serves also as the operational coordination center (OCC) for the whole network.

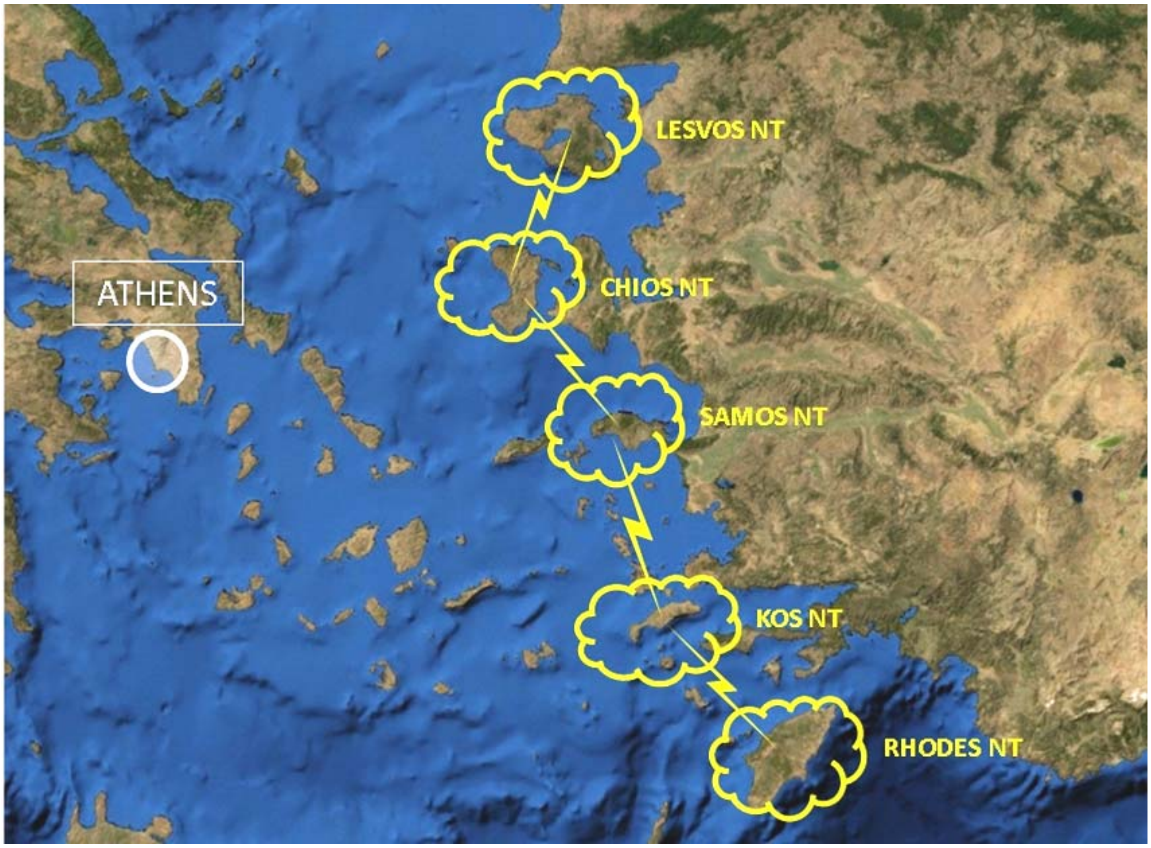


Figure 14. Operational-level network

3. Nationwide Wireless Broadband Cluster Sensor Networks (Strategic/National Level)

Through VPN tunneling technology or satellite communication, we can also extend our design to support the highest hierarchical level, that of national/strategic needs. That means that we intend to provide circulation of data towards the C2 Coast Guard Center in Athens and vice versa. In this way, we bring the commander together with the experts and specialists on the scene of any incident in real-time, providing secure voice, data and video streaming. In parallel, we can extend the surveillance network to other areas beset with smuggling and cross-border criminal activities, such as Corfu Island (Figure 15). The benefits of this networking can be shared with the Air Force and Navy, at least for SAR purposes. In total, such a system could be characterized as a Coast Guard Nationwide Wireless Broadband Sensor Network.

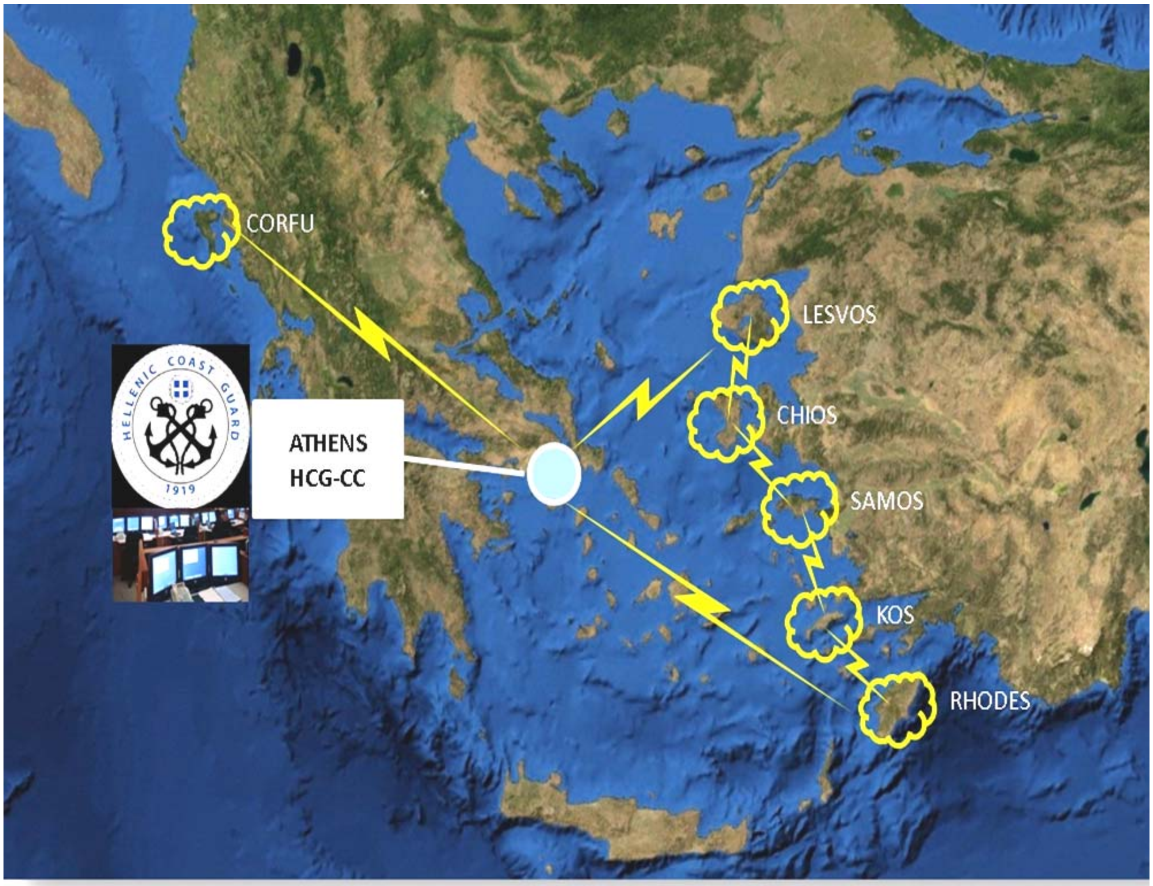


Figure 15. National-level network

D. NETWORKING

1. Communicating Through Nodes

For the creation of an 802.16 wireless network, several pairs of Redline Access Nodes-80 (AN-80i) should be used (Figure 16). According to the manufacturing company, Redline Communications, the AN-80i is a radio transceiver for high-performance wireless broadband transport solutions for quickly establishing point-to-point and point-to-multipoint links that extend the networks to great distances.

Operating in the license-exempt 5-GHz band, the AN-80i leverages proven OFDM technology to deliver industry-leading, high-speed Ethernet throughput. With its exceptional long-range capabilities, the AN-80i is able to establish and maintain reliable, robust connectivity that can exceed 80 km (50 miles) in clear line-of-sight conditions.

AN-80i Specifications:

System Capability: LOS, optical-LOS, and non-LOS (OFDM)

RF Band: 5.725-5.850 GHz, TDD

Channel Size: 20 MHz, 40 MHz (software selectable)

Data Rate: Up to 90 Mbps average Ethernet rate

Max TX Power: 20 dBm (region specific)

Rx Sensitivity: -82 dBm @ 6 Mbps (BER of 1x10e-9)

PoE Cable: Up to 91m (300 ft)

Network Attributes: Transparent bridge, automatic link distance ranging, 802.3x, 802.1p,DHCP pass-through, encryption

Modulation: BPSK to 64 QAM (bidirectional dynamic adaptive)

Dynamic Channel Control: ATPC

MAC: PTP, concatenation, ARQ

Range: Beyond 80 km (50 mi) LOS@ 48 dBm EIRP

Network Connection: 10/100 Ethernet (RJ-45)

System Configuration: HTTP (Web) interface, SNMP,Telnet

Network Management: SNMP: standard/proprietary MIBs

Power Consumption: Standard IEEE 802.3af (15.4 W

(Redline Communications, 2010b)

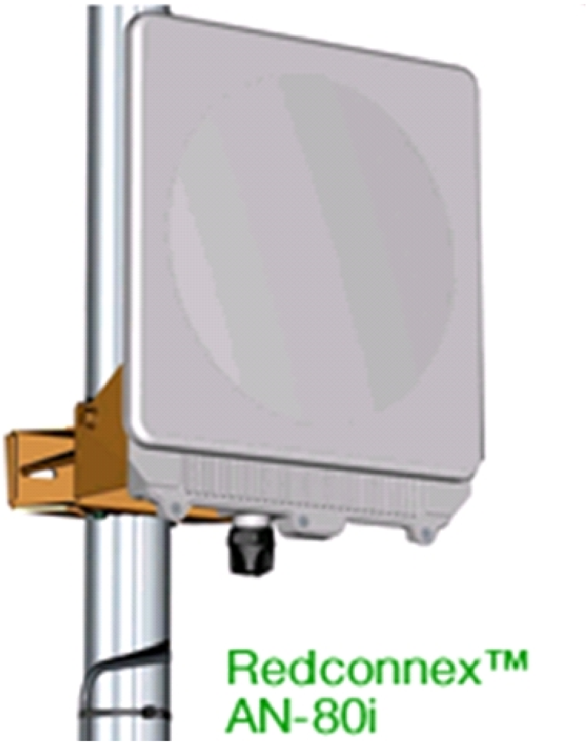


Figure 16. Access Node AN-80i (From Redline Communications site)

Each radio is mounted on permanent communication towers in LOS distances which provide the point-to-point transmission of the signals. Further extension of the network can be accomplished through VPN tunneling via the Internet, which bridges each communication relaying node with the corresponding node of the adjacent network. In a similar way, a further extension can be easily achieved between the networks and the HCG C2 center in Athens.

The communication link node is a single or multiple pairs transceivers entity for automatically transmitting the data received from the adjacent surveillance node to the other communication link nodes (point-to-multipoint) and/or for relaying towards the head of the network nodes (multipoint-to-point). In cases where it is adjacent to a surveillance node, it is wire-linked with the sensor node and preferably shares the same installations (tower and power supply). For all cases of connectivity, LOS conditions between the adjacent network nodes, as well as the distance limits, are the major concerns for ensuring the network mesh connection and coverage.

2. Surveillance Via Sensors

The surveillance node is comprised of the radar and the EO sensing unit, their processors, the transceiver and the power supply unit. The sensors are made up of the sensing subunit and the analog-to-digital conversion (ADC) unit for the transformation of the analog signals to digital before they are received by the processor (Figure 17). (Akyildiz, Su, Sankarasubramaniam, & Cayirci, 2002).

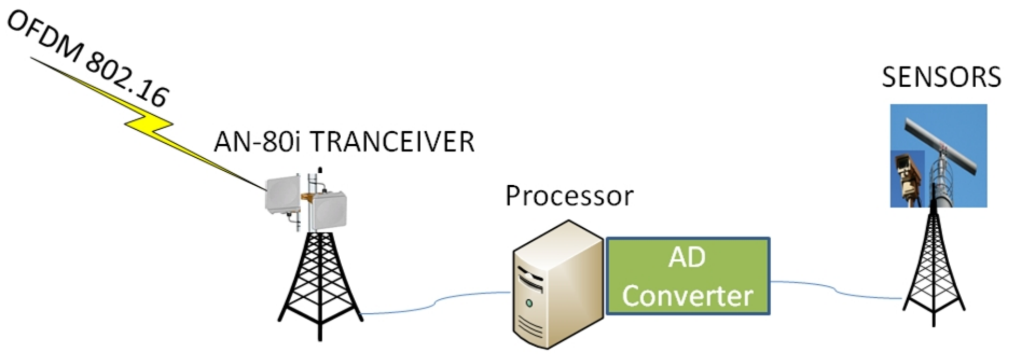


Figure 17. Sensor node configuration

In this network, the radar sensor operates in a steady-state condition and, in cases where a target needs to be identified; the video sensor is involved complementarily to support the objective. Consequently, two ways of communication are anticipated: that of the inter-node between the sensors and processor and that of multi-hop wireless video streaming (802.16) to the head node (TOC). The processing unit converges the sensors output (radar and EO) after it has passed through the ADC unit and automatically sends the data to the head node through the network’s chain of transceivers. The data received by the data server are processed and stored and automatically provided to the operator.

For the surface surveillance of areas which can be described as straits with limited dimensions, instead of closed sea, HF maritime radar may be used for automatic detection and tracking on low RCS vessels with high accuracy and resolution under all weather conditions in a cluttered environment.

Regarding the EO device, it should be a combination of a high PTZ camera with infrared capabilities in a weatherproof housing, able to aid in track identification and visual observation remotely, on the TOC's officer command. The camera is synergistically engaged with the radar processor. When a target of interest is detected and tracked by the radar, the camera automatically focuses on this target and provides live video to the head node, for observation by the officer on duty. In such a case, he remotely manipulates all features provided by the camera in order to improve sensing and acquire and optionally store the valuable video data. The video processing should also include a standard video compression technique (e.g., MPEG-4, MJPEG) for streaming towards the head node. (Little, Konrad, & Ishwar, 2007)

The source of energy for the continuous operation of the nodes can be provided directly by the urban infrastructure available in cases where the nodes are deployed adjacent to such areas. Otherwise, the power can be provided by solar panels or wind generators, both available in the Aegean Sea environment. CENETIX's backbone network infrastructure uses such alternative electrical power supplies (solar panels) in the Nacimiento relaying station (Figure 18).

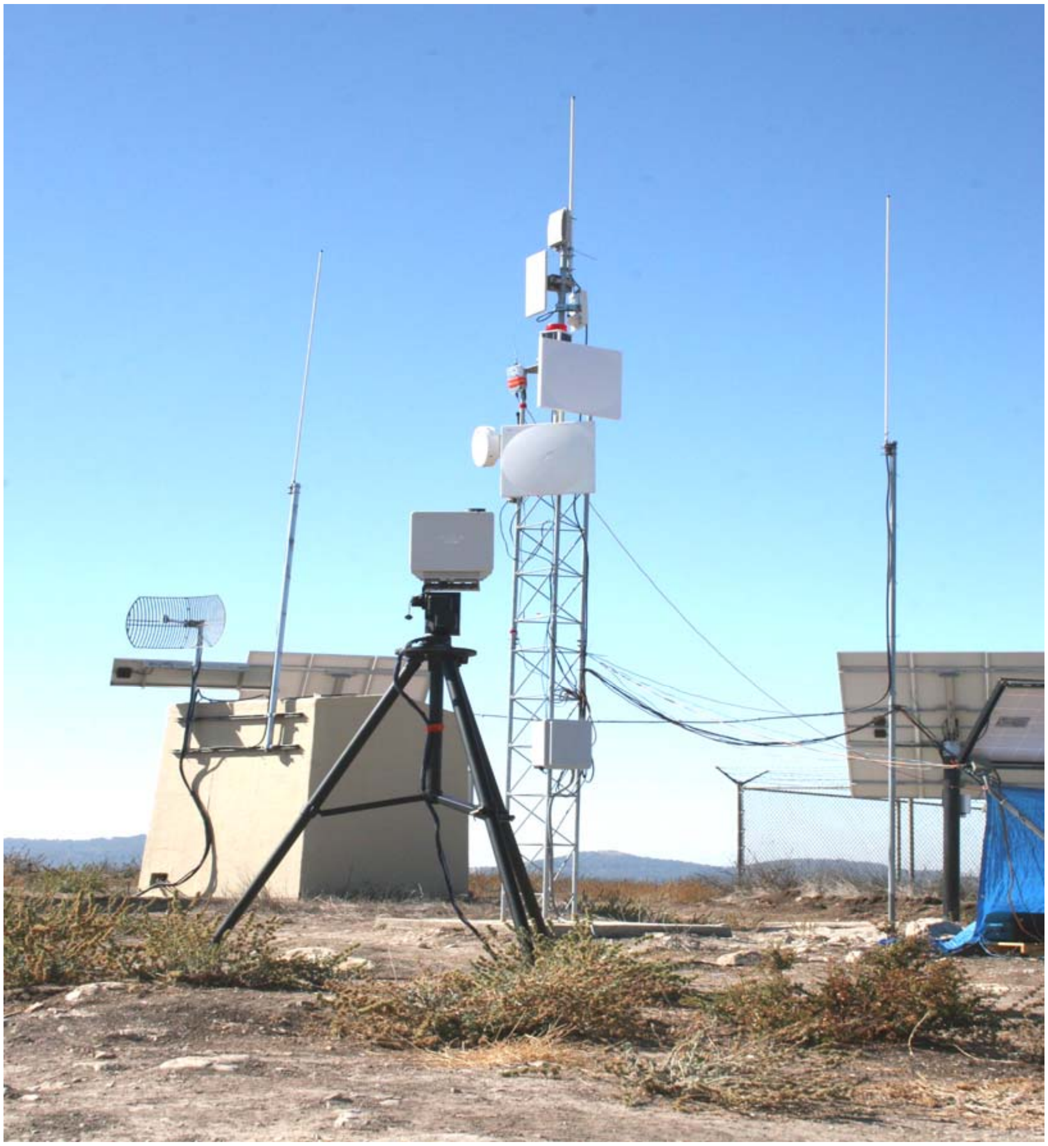


Figure 18. Nacimiento, CA-CENETIX's RN infrastructure-solar panels (From CENETIX site)

3. Collaborating Through SA Tools

In a cluster net of surveillance sensors, the fusion node is where the aggregated data are received and processed through the SA tools by the controllers. Real-time updates regarding the AoR are presented for viewing, analysis and alerting of the corresponding patrol forces. Consequently, the TOC in such a case should be stationed with the already available local HCG operational center on each island. This means that the officer on duty can be also charged with monitoring the aggregated picture delivered by the corresponding network.

A Data Server (DS) is the core element of the TOC's design, since it provides connectivity between the end user (duty officer) and the sensor nodes. The DS receives the entire target information product from all the active sensor nodes. Subsequently, it stores all data for further exploitation, also allowing access for real-time monitoring and processing, as well as for further specific tasks, such as intelligence gathering and prosecution.

Since the TOC is the end user of the cluster network, a firewall and router should also be used for the extension of the network to a WAN via Internet to ensure security, availability and integrity of the data. In addition, the accessibility of the server's data should be provided only through encryption techniques and authorization procedures (Figure 19).

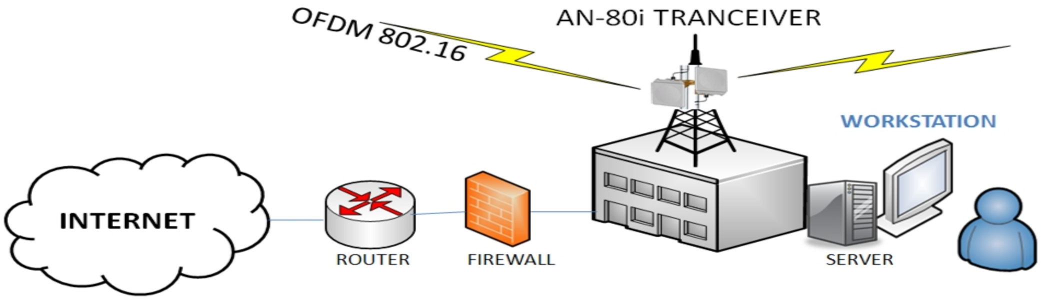


Figure 19. Head node configuration

IV. ISLAND-BASED SURVEILLANCE NETWORK (CLUSTER)

A. NETWORK TOPOLOGY/TOPOGRAPHY

The whole network of islands in the Eastern Aegean Sea should be comprised of five autonomous peripheral networks with its corresponding TOCs located in their capital cities. For simplification, we will focus on a single cluster sensor network design, based on the island of Lesvos, also known by its capital's name, Mytilene (Figure 20).

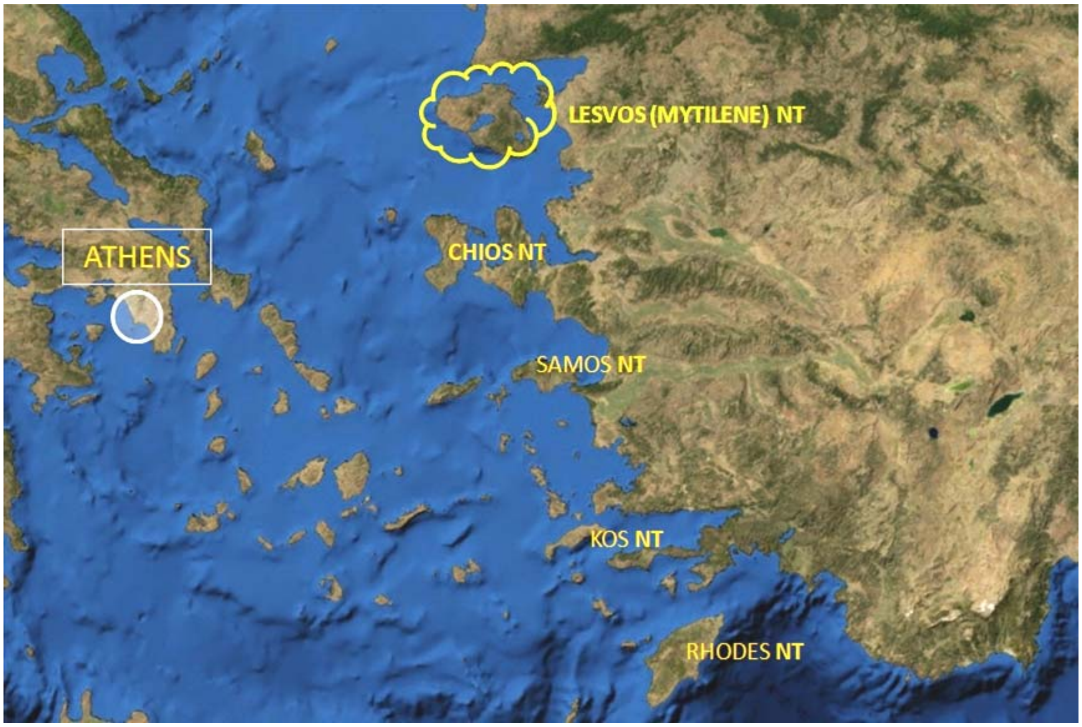


Figure 20. Lesvos island cluster sensor network

Mytilene, as an island, is considered to be one of the major entry points into Greece for the smuggling networks. With distances varying from 8 to 15 kilometers from the Turkish shoreline, and also taking into account the equidistant territorial middle line in the channel, the reaction time is limited for HCG crews (Figure 21).

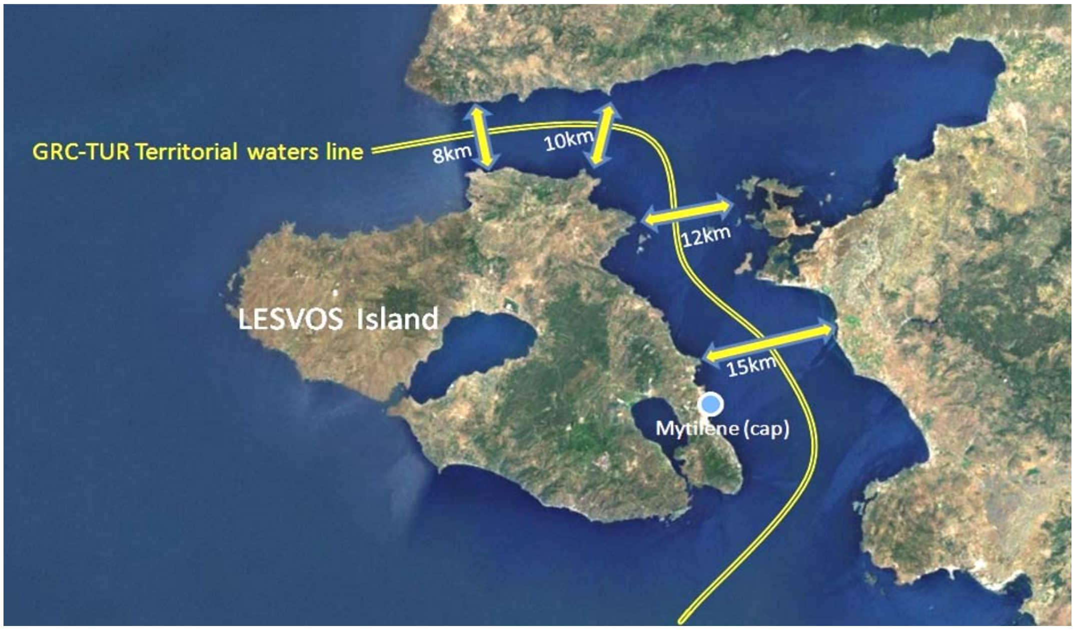


Figure 21. Lesvos island topography

Therefore, the topology of such a sensor network should be oriented towards these straits. An AoR can be designated and assigned for that surveillance network, as represented in Figure 22.

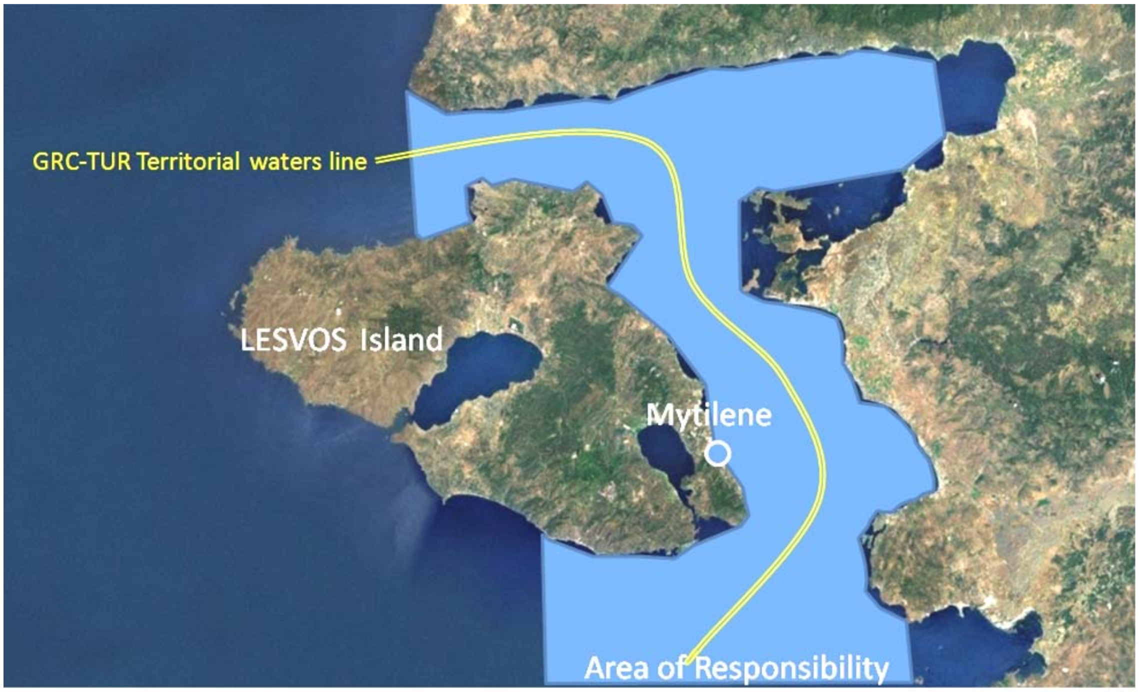


Figure 22. Lesvos cluster network AoR

Consequently, to cover this AoR, the sensor nodes should be mounted on the northern and eastern parts of the island facing the opposite shoreline. The number of surveillance sensors needed for sufficient coverage of the corresponding AoR is no more than four since both the ranges required and the radar surveillance capabilities satisfy the needs and, in some cases, there is overlapping coverage.

It is preferable that all sensor nodes (SNs) are close to the urban facilities of a village or town in order to receive the required electrical power and to have physical protection and ease of accessibility for maintenance purposes. A provision for CCTV capability can also contribute to the remote surveillance of the node facility itself, as well as for deterring any potential "visitors".

The head node, which should be facilitated by the already available HCG TOC in the island's capital, Mytilene, will serve as the information fusion center of the network (Figure 22). The data extracted from the sensors are routed to a sensor data server which automatically stores and distributes them to the network monitoring station in the TOC. Apart from monitoring, analyzing and alerting through the workstation, a provision for administrative and remote maintenance capabilities for the system is also provided.

Taking into account the dimensions, the geo-morphology and also the orientation of the island towards the AoR, as well as the location of Mytilene and the need for LOS between the adjacent network nodes, we proceed to the following network deployment architecture. Mytilene's sensoring network model should be comprised of four sensor nodes.

The specific locations for the network's deployment are the following (Figure 23):

- SN 1: Mithymna (N 39°22'25, E 26°11'22- Elev.12m)
- SN 2: Tsonia (N 39°22'27, E26°21'50- Elev.15m)
- SN 3: Mytilene (N 39° 6'32, E26°33'51- Elev.36m)
- SN 4: Fteli (N 38°59'14, E26°32'26- Elev.35m)

The distances among the nodes are as follows:

- SN1-SN2:15km SN2-SN3: 35km SN3-SN4: 11km

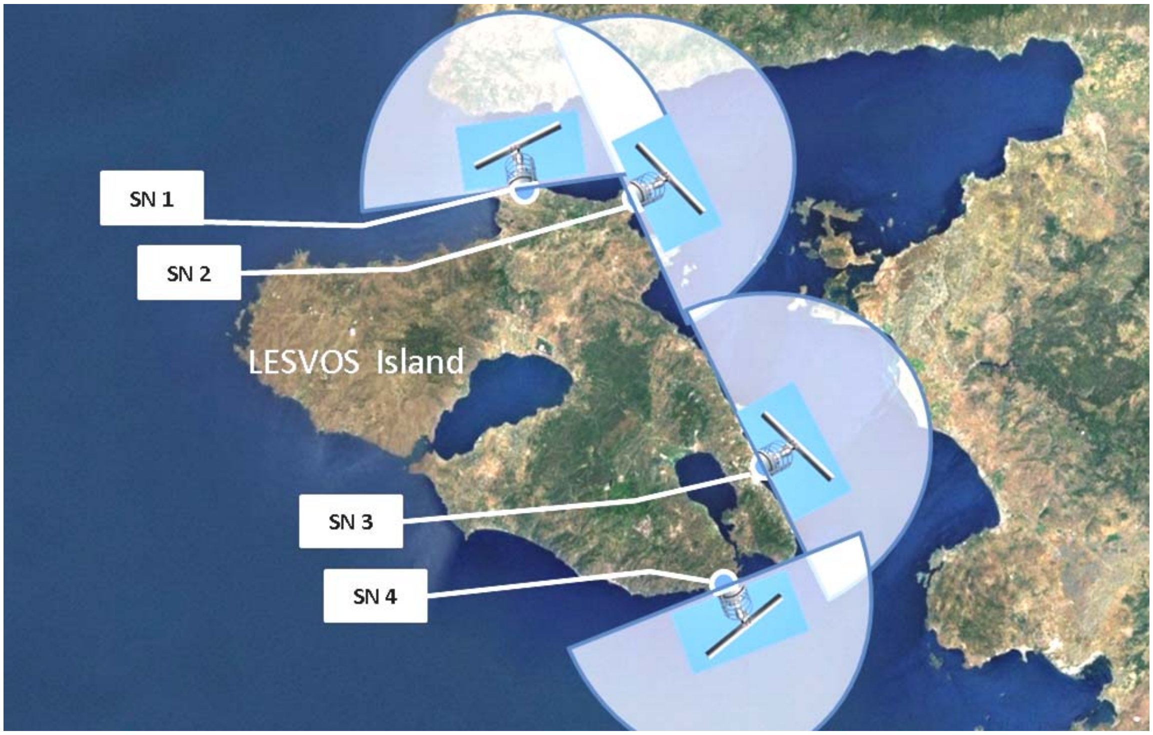


Figure 23. Lesvos model network surveillance coverage

To complete the backbone of the Lesvos network, we should specify the number and the locations of the relaying nodes (RNs) needed for the interconnection of the entire system. In a case where the island has only flat-terrain morphology, given the relatively short distances between each node, we would not need an RN at all. Unfortunately, Lesvos has rocky terrain morphology, as most of the Aegean islands do, making the need for RNs profound. By specifying the minimum number of RNs needed for the creation of this link, and their exact locations, we can present the basic feasible architecture for an operable surveillance network but with no or limited redundancy (Figure 24). That means that to achieve full redundancy through full or almost full mesh networking, we should add more RNs.

Trying to specify the fundamental network design of the Lesvos network, we proceed to the network's simulation through a software application named the Systems Planning Engineering and Evaluation Device (SPEED), created by Northrop Grumman for United States Marine Corps (USMC) operational communication needs.

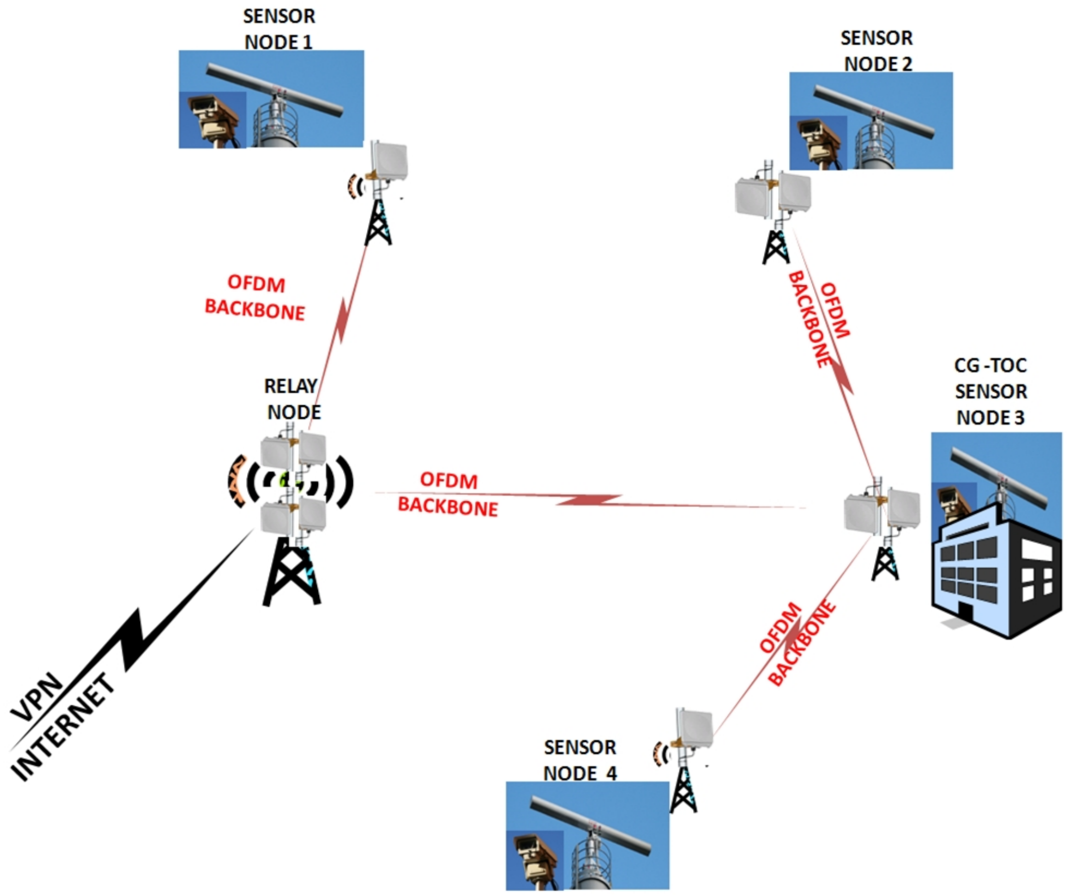


Figure 24. Sensor network of limited redundancy

B. NETWORK'S COMMUNICATION SIMULATION TEST (SPEED)

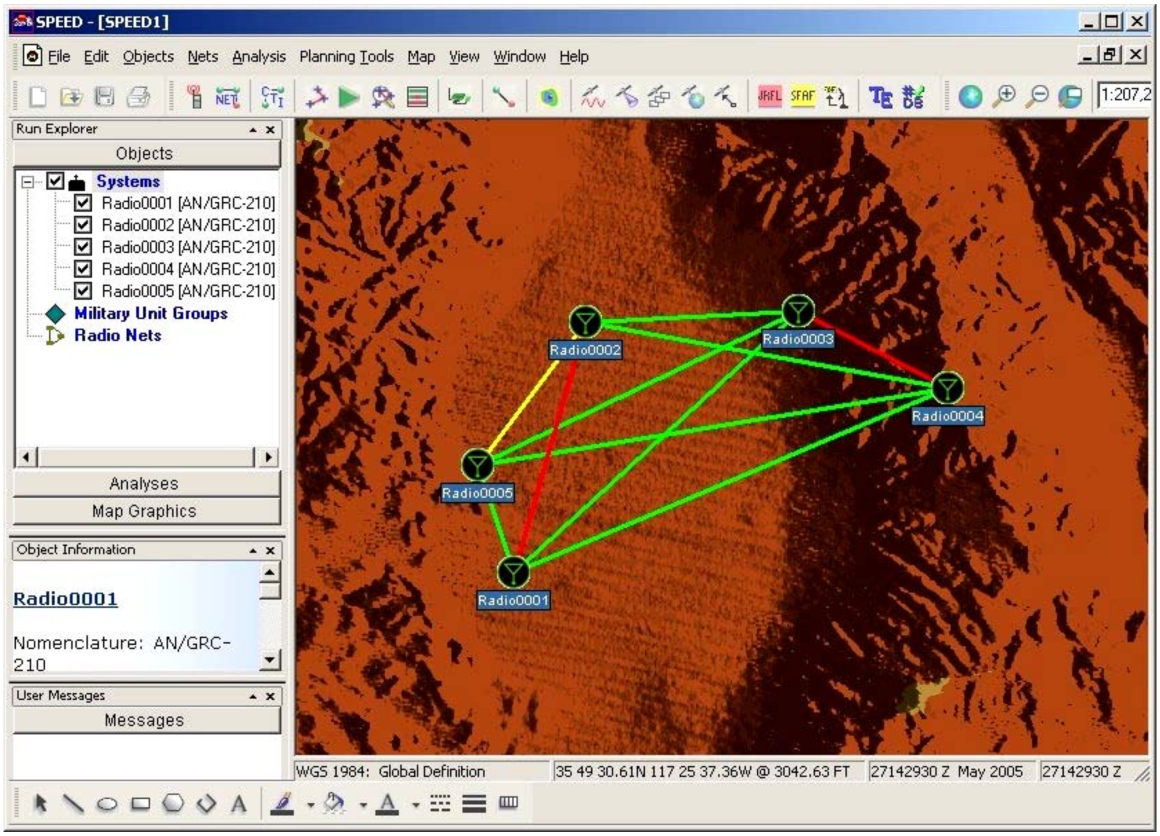
SPEED is a fully integrated system for generating, storing, and disseminating communications information. SPEED provides rapid communications planning and support for maneuver warfare in rapidly changing tactical environments. SPEED also provides communications planners and spectrum managers at all levels with a set of tools that can be used to perform a wide range of communications planning, radio frequency (RF) engineering and spectrum management functionality to support the tactical environment. Among several others, SPEED includes the Point-to-Point (PTP) Analysis Tool, which provides point-to-point communications analysis, engineering, and planning of the very high frequency (VHF), ultra high frequency (UHF) and super high frequency (SHF) radio bands. It evaluates the performance of any network configuration of connected transceivers, provides two-dimensional terrain profile displays between the connected transceivers, and provides a powerful and graphical set of tools for optimizing the performance of these systems.

The point-to-point analysis now contains a quality of service (QoS) analysis that uses the path loss determined from a Terrain Integrated Rough Earth Model (TIREM) and other user selectable parameters to determine the energy per bit-to-noise power spectral density (Eb/No) ratio, carrier- to-receiver noise (C/kT) ratio, carrier-to-noise (C/N) ratio, and theoretical bit error rate (BER) values for that particular digital link. The theoretical BER is calculated using an approximated Q-function from the Eb/No and C/N values. The BER is a statistical measurement of the probability of errors in the digital signal, and is therefore used to determine if the link is considered to be acceptable or unacceptable.

The PTP Analysis Tool contains default settings that determine how the analysis will be performed. The Default Point-to-Point Analysis Interval dialog displays the default values for the interval between the collection of elevation points. The finer the analysis is, the better the resulting product will be.

A minimum of two radios operating with the same modulation type and frequency must be selected to perform a PTP analysis. More radios can be selected if desired.

Performing a PTP analysis produces a link-status line connecting selected radios. The color of the link-status line indicates the predicted status of the link, based on the link parameters and the terrain-dependent signal path loss. Each PTP link-status line consists of one analysis line. The analysis line connecting each radio indicates overall link performance in the least favorable direction. A solid green line indicates an acceptable predicted signal-to-noise (S/N) ratio in both directions, a yellow line indicates a marginal predicted S/N ratio in one or both directions, and a dotted red line indicates an unacceptable predicted S/N ratio in one or both directions (Figure 25).



Radio0001

Nomenclature: AN/GRC-210

WGS 1984: Global Definition | 35 49 30.61N 117 25 37.36W @ 3042.63 FT | 27142930 Z May 2005 | 27142930 Z

Figure 25. Point-to-point analysis (From SPEED's Manual)

A feature of the PTP tool is the capability to drag any radio connected by an analysis line to a new location on the map to determine the predicted status of the link immediately by the color of the analysis line. Then, the PTP Analysis Tool will automatically re-analyze all links based on the new location.

The PTP Analysis window enables the communications planner to view the data on a specific communications link and the PTP Analysis window can be used to analyze, optimize and plan VHF, UHF, and SHF communication links. This window is also used to display the following PTP analysis information:

- Terrain Profiles
- Fresnel Clearance Zones
- Antenna Pointing Azimuths
- S/N predictions

- RSL predictions
- Troposcatter Reliability predictions
- Link Margin predictions
- Path Loss predictions
- Propagation Mode determination
- SINCGARS Cosite Interference Evaluation

The PTP Analysis window can be entered any time, if there is at least one link connection on the World Map or Digital Terrain Elevation Data (DTED) Mapsheet window.

The terrain profile display is a cross-section of the terrain along the great-circle path between two connected radios. At each end of the link, the elevation of each radio is displayed along with the radio's antenna height. If the path is unobstructed by terrain, an LOS line is drawn between the two radio's antennas. The Fresnel clearance zones may be shown if LOS exists between the two radios. The terrain elevation points displayed are plotted on an earth surface that is deliberately distorted to account for atmospheric refractivity, which tends to bend a radio wave. (Northrop Grumman, n.d.)

C. SPEED'S APPLICATION FOR SIMULATION OF LESVOS NETWORK

Taking into account that the topography of the radar surveillance nodes (SNs) is relatively unique for the coverage of the Lesvos AoR, we deduce that the interconnection via OFDM link between the nodes can vary from a full mesh network to just a simple serial one. Since the criterion of distance (max 37 km) is not going to impact the network's performance, then it is up to studying the terrain morphology for the establishment of the required LOS for tranceiving between the nodes. Therefore, the signal propagation simulation test through the SPEED application can show us the potential applicable Lesvos network topology and any compromises we may have on its deployment.

To proceed to such a simulation, the system requires data for the specifications of the communications hardware elements (Redline's AN-80i), the fixed locations of the sensor nodes as well as the digital terrain elevation data (DTED) for the island of Lesvos.

D. RESULTS

The simulation of the system revealed the following observations and deficiencies:

- The morphology of the island does not allow for easily achievable links since great masses of mountains divide the area of deployment, precluding direct LOS between the peripheral nodes. That means for achieving a mesh interconnection of the network, we need more than one RN to be placed between the nodes.
- Taking into account the permanent locations of the two northeastern as well as the two southeastern sensor nodes, in accordance with their surrounding terrain, we deduce that the linkage can be achieved only by treating them as two different elements. That means that we first managed to connect the elements of each pair with an RN and after that we tried to connect the two RNs with each other.
- The use of that software requires thorough knowledge of the area's terrain morphology and subtle manipulation of its capabilities for identifying the ideal positions of the network elements in the minimum possible time.

The outcome of that simulation test was successful for the creation of the fundamental basis of a cluster sensor network on the island of Lesvos, as it is depicted in Figure 26.

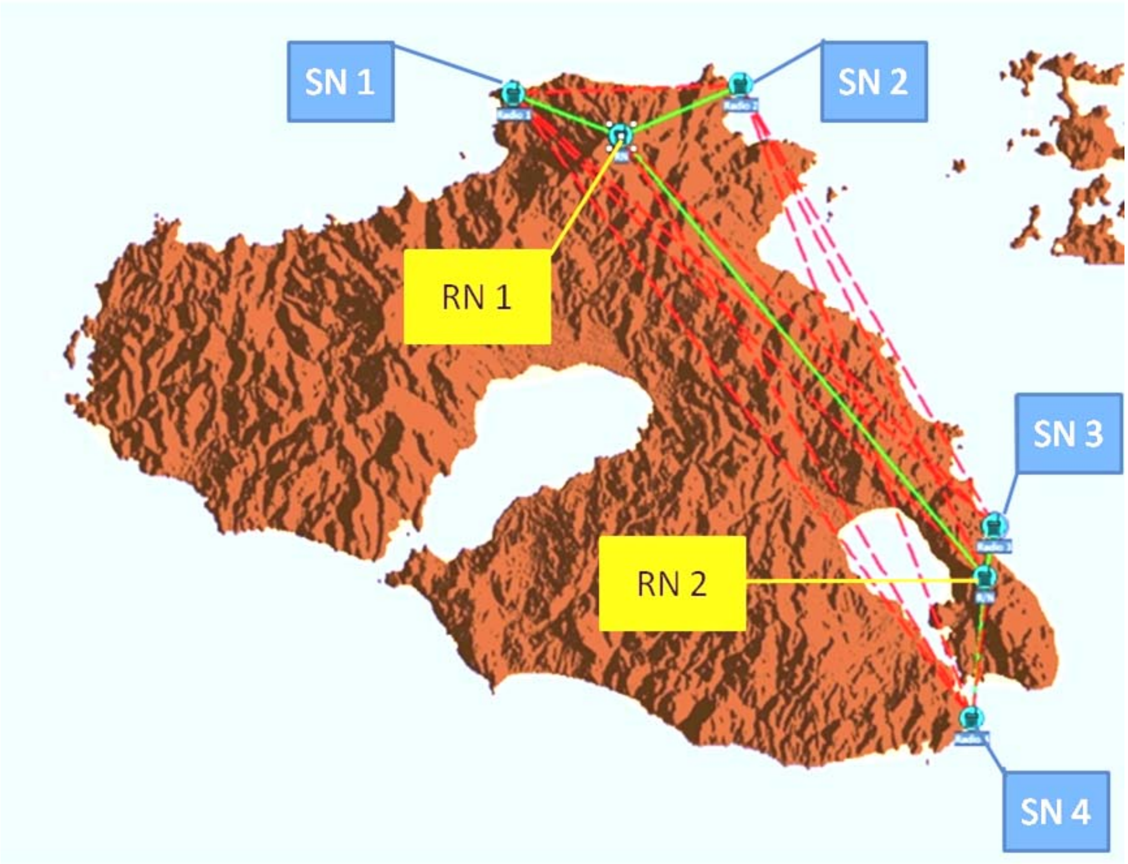


Figure 26. SPEED’s application outcome

It represents the basic network OFDM backhaul, comprising four SNs and two RNs, required to achieve the synergy needed between the network’s elements. The specific location of each of these two RNs as well as the relevant distance between each one of the SNs is the following:

- RN1 : Argenos (N39°20'57, E26°15'38– Elev.697m)
- RN2 : Akrotiri (N39° 04'54. E 26°33'14– Elev.258m)
- RN1-SN1: 7km RN1-SN2: 10km
- RN1-SN3: 37km RN1-SN4: 47km
- RN2-SN1: 46km RN2-SN2: 37km
- RN2-SN3: 4km RN2-SN4: 11km
- RN1-RN2: 39km

Obviously, the above outcome does not provide complete meshing capability to the system, which means that in case of any failure of the RNs, the network is automatically rendered partially or totally out of order. Therefore, for achieving mesh attributes in that network's architecture, we should add one or two more RNs between the northern and southern nodes for further inter-linkage extension (Figure 27).

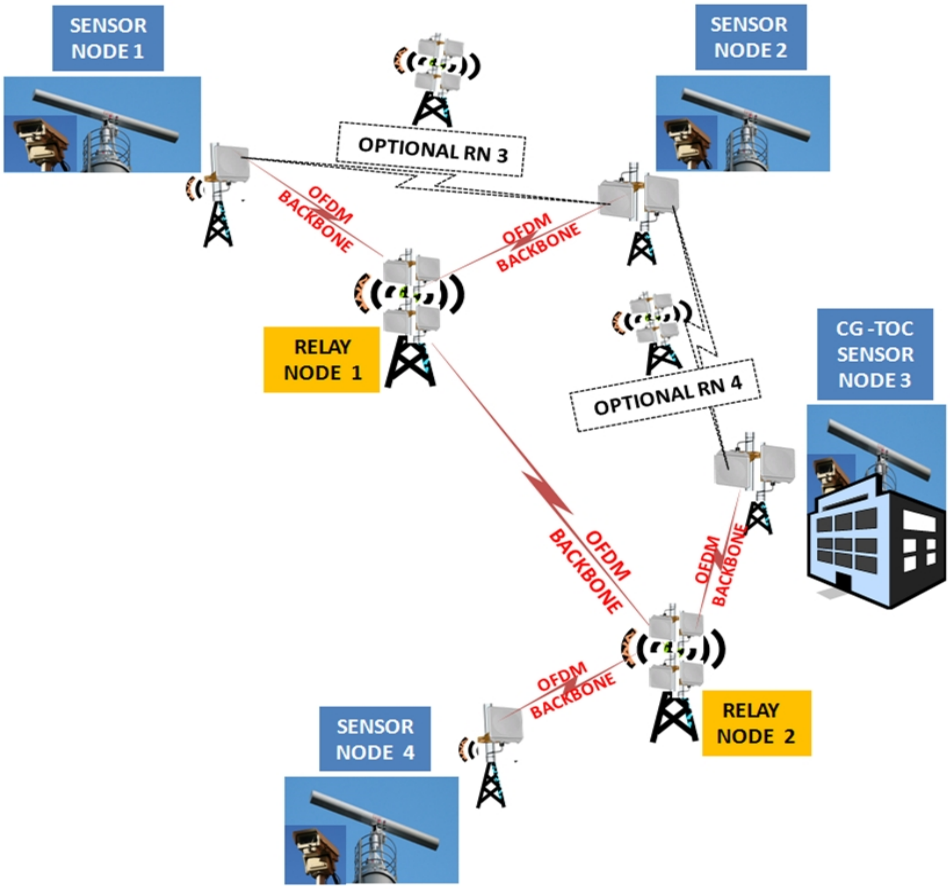


Figure 27. Basic and optional (mesh) extension of Lesvos network architecture

The cost, which was set as a fundamental criterion for the development of such a network infrastructure, can be roughly estimated (based on the similar CENETIX backbone) to be US$300,000 for a six-node (2RNs + 4SNs) basic cluster sensor network, or US$400,000 for an eight-node (4RNs + 4SNs) partial mesh network. Taking into consideration that the terrain morphology of Lesvos is the most inconvenient for deploying such a network, it is apparent that the rest of the major islands will require less extensive and consequently less expensive infrastructure than Lesvos.

Nevertheless, in trying to evaluate the potential feasibility of such a proposed system and identifying the major constraints of its establishment and operation, the following estimations were considered:

- The already existing technological background and the available information technology (IT) accessible in the open market, as well as the expertise of the personnel of the relevant companies, means that the development of the system is realistically achievable. To that end, the available simulation tools can ensure, through reliable and relatively inexpensive testing, each step toward the gradual accomplishment of such project.

- Also concerning the factor of operational feasibility, such a system can be measured in advance, since it satisfies the requirements set at the design phase and seems to be capable of providing the necessary assistance to law enforcement authorities for countering smuggling activities in that area.

- Considering the autonomous operation of this surveillance system and the already proven reliability of similar systems (e.g., CENETIX's OFDM backbone), we can state that it is a very competent and cost-effective solution. An extra economic benefit from its use is the indirect savings in personnel and manpower through the network-based management of HCG forces, while, on the other hand, they are able to carry out their duties with enhanced efficiency.

- All things considered, and having in mind the island's terrain morphology factor and the fine software manipulations needed for designing the topology of the network, it is illustrated that the major constraint on the feasibility of such project would be mainly centered on that the terrain factor. To that end, a preliminary site survey of the specific area by IT experts could reveal all relevant data and associated restrictions that may impair the establishment of such system.

V. CONCLUSIONS

A. CONCLUSIONS

The deployment of an island-based autonomous wireless sensor network, as designed and presented above, and its applicability proven by Northrop Grumman's SPEED simulation test, for surveillance purposes on the Eastern Aegean Sea islands is believed feasible. It involves Redline communications technology, a manufacturer of a wide range of OFDM equipment, which is also successfully used by the NPS/CENETIX TNT test bed, to provide an OFDM 802.16 long-haul link, enabling high-bandwidth connectivity.

The composite (Radar+EO) sensor network which was described herein provides wide-area surveillance through monitoring and tranceiving real-time video, voice and data streaming at a relatively affordable cost. It generates situational awareness as well as the alerts needed to HCG forces for any kind of threat or maritime incident. Thus, it contributes decisively at least to saving more lives, either on illegal immigration cases or in other ones, and there can be no doubt that its operation dissuades potential smugglers from their intentions.

Considering that each cluster network requires no more than one person (the officer on duty) to monitor and exploit operationally, it can save workload and serve in general as a force multiplier. In addition, the construction of the overall network elements is somewhat covert and limited in dimension, making the need for building extra installations relatively unnecessary.

It is obvious that setting up just the first island-based network, for instance that of Lesvos would be the wisest base step for the creation of a whole set of clusters, enough to cover all the "fragile" area of the Eastern Aegean Sea. The feedback on its operability and efficiency, once it is settled, can contribute greatly to any further deployment of the collaborative environment, thus ultimately resulting in a gradually enhanced surveillance and security capability in that region.

B. OTHER APPLICATIONS

With no doubt, such a system can be used for similar purposes in riverine and lake environments, port surveillance, security of littoral military facilities, monitoring for illegal fishing and oil spilling, and so forth. But, apart from maritime surveillance for illegal activities, the major contribution is that of the enhancement of the SAR capability for each area of coverage. Any single vessel voyage is archived in the main data server from the first until the last trace-contact, thus making the SAR mission much easier. In parallel, through the network's coverage, all HCG maritime forces are under positive control, thus enhancing their overall management as well as their safety.

Taking into account the advances in sensor devices and wireless radio communication technology, the resulting design provides a platform for multipurpose use and exploitation even beyond mitigating smuggling activities. Such a terrestrial long-haul wireless network backbone can give the opportunity for further extensions of the network, mainly by mobile nodes aboard HCG vessels carrying special sensors for detecting nuclear materials, drugs and so forth. Similarly, it can be linked with UAV assets for detached surveillance purposes, SAR and even for wider range maritime operations.

Additional exploitation of these expanded mobile capabilities can nowadays be easily achieved through the establishment of a secure; two-way; voice, picture, and video data stream in real-time between capital-metropolitan centers and remote sites-islands, thus "transferring" the decision makers and the experts onto the real tactical theater. The parallel use of modern biometric technology by the patrolling forces can also contribute to an advantageous synchronized collaboration via wireless interconnection with the command post, based on a related smuggling networks database. Such guidance and support for the ongoing missions can certainly lead to more secure and fruitful conduct of law enforcement operations. At the end of the day, the humanitarian aspect can be effectively serviced by such infrastructure, a lesson which has already successfully taught and learned by the deployment of CENETIX's network for the relief of Hurricanes Katrina's homeless people.

LIST OF REFERENCES

Akyildiz, F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks, volume number 38*. 393–422.

CENETIX (2010). TNT/MIO 10-02 - Networking and interagency collaboration on small craft maritime-sourced nuclear radiological threat detection and interdiction. (After-action report of joint NPS-LLNL field experiment sponsored by USSOCOM, DHS MDSP, AND OSD/HD programs, July 2010).

Dahlman, E., Parkvall, S., Bovik, A., & Beming, P. (2009). *Communications engineering desk reference,* Oxford, UK: Academic Press. 247–256.

Israel Aerospace Industries Systems (2009). *EL/M radar systems family - EL/M 2226 Brochure*. Retrieved from http://www.iai.co.il/sip_storage/FILES/2/36842.pdf. (Last accessed September 10, 2010).

Klopson, E. and Burdian, V. (2005). Collaborative applications used in a wireless environment at sea for use in CG law enforcement and homeland security missions. Master's Thesis, Naval Postgraduate School, Monterey, CA. 17–26, 27–40.

LAN. (n.d.) In *Webopedia Online Computer Dictionary*. Retrieved at http://www.webopedia.com/TERM/l/local_area_network_LAN.html (Last accessed September 10, 2010).

Little, T., Konrad, J., and Ishwar, P. (2007). A wireless video sensor network for autonomous coastal sensing. *Proceedings from Conference on Coastal Environmental Sensing Networks (CESN 2007),* Boston, MA: Boston University.

MAN. (n.d.) In *Webopedia Online Computer Dictionary*. Retrieved at http://www.webopedia.com/TERM/M/MAN.html. (Last accessed September 10, 2010).

Mesh. (n.d.) In *Webopedia Online Computer Dictionary*. Retrieved at http://www.webopedia.com/TERM/m/mesh.html. (Last accessed September 10, 2010).

Microsoft (2010). The business collaboration platform for the enterprise and the internet – Share Point 2010. Retrieved from http://sharepoint.microsoft.com/en-us/Pages/default.aspx. (Last accessed September 10, 2010).

Mir, N. (2007). *Computer and communication networks.* Upper Saddle River, NJ: Prentice Hall. 431–437, 536–537.

Naval Postgraduate School (2010). CENETIX home page. Retrieved from http://cenetix.nps.edu/cenetix/cenetix.asp. (Last accessed September 10, 2010).

NOC. (n.d.) In *Webopedia Online Computer Dictionary.* Retrieved at http://www.webopedia.com/TERM/N/NOC.html. (Last accessed September 10, 2010).

Northrop Grumman (n.d.). SPEED Manual.

Nohara, T., Premji, A., Ukrainec, A., Weber, P., Jones, G., and Krasnor, C. (2005). Low cost, high-performance radar networks. United States Patent Application No. 11/110,436, Publication No. US 2006/0238406 A1, Filing Date: April 20, 2005.

Nohara, T., Weber, P., Jones, G., Ukrainec, A., and Premji, A. (2008). Affordable high-performance radar networks for homeland security applications. *Proceedings of 2008 IEEE Radar Conference*. Rome, Italy: Institute of Electrical and Electronics Engineers (IEEE). 1–6.

OFDM. (n.d.). In *Webopedia Online Computer Dictionary.* Retrieved at http://www.webopedia.com/TERM/O/OFDM.html. (Last accessed September 10, 2010).

Redline Communications (2010a). Turkey video surveillance case study. Retrieved from http://www.redlinecommunications.com/index.php/download_file/view/39/ (Last accessed September 10, 2010).

Redline Communications (2010b). AN-80i broadband wireless backhaul data sheet. Retrieved from http://www.redlinecommunications.com/products/bwi-family/an-80i-broadband-wireless-backhaul/. (Last accessed September 10, 2010).

Sicom Systems (2004). Homeland security network-enabled Great Lakes wide area radar surveillance. Retrieved from http://www.accipiterradar.com/HS_WideAreaSurveillance%281%29.pdf. (Last accessed September 10, 2010).

Seibert, M., Rhodes, B., Bomberger, N., Beane, P., Sroka, J., Kogel, W.,…Tillson, R. (2006). SeaCoast port surveillance. *Proceedings of SPIE Vol.6204: Photonics for Port and Harbor Security II.* Orlando, FL: Society of Photographic Instrumentation Engineers (SPIE).

802.11. (n.d.). In *Webopedia Online Computer Dictionary.* Retrieved at http://www.webopedia.com/TERM/8/802_11.html. (Last accessed September 10, 2010).

802.16. (n.d.). In *Webopedia Online Computer Dictionary.* Retrieved at http://www.webopedia.com/TERM/8/802_16.html. (Last accessed September 10, 2010).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Alexander Bordetsky
   Naval Postgraduate School
   Monterey, California

4. Eugene Bourakov
   Naval Postgraduate School
   Monterey, California

5. Dan Boger
   Naval Postgraduate School
   Monterey, California

6. Dionysios Kotsifas
   Naval Postgraduate School
   Monterey, California