A NETWORK OPERATIONS CENTER FOR A COMMUNICATION NETWORK OF FISHING VESSELS AT SEA

ASWINI BALAKRISHNAN, SETHURAMAN RAO, DHANESH RAJ AND KALYAN SASIDHAR
Amrita Center for Wireless Networks and Applications
AMRITA Vishwa Vidyapeetham
Kollam, India
aswinikrishnan30@gmail.com[1], (sethuramanrao[2], dhaneshraj[3], kalyansasidhar[4]) @am.amrita.edu

ABSTRACT: A project is underway at our center to develop a seamless communication network for fishermen at sea. A network operations center (NOC) for the communication network is required to monitor, manage and troubleshoot the problems in the deployed network. With the deployment of a proper NOC at shore, one can discover and authenticate boats entering and leaving the network, provide a topology map, constantly monitor the deployed infrastructure, faults in the network, failure of any node, etc., and take proper corrective actions. In addition, the NOC will send alerts about an imminent storm, intrusion of foreign vessels, maritime border crossing etc., to the fishermen. The NOC will also collect distress signals and other alerts from the boats and relay them to the appropriate stakeholders on land. It will also be used for software upgrades, making configuration changes and other maintenance tasks on the network nodes. This work outlines the design of an effective and functional management subsystem and a NOC for the network of fishing vessels at sea.

KEYWORDS: MICRONet, NOC, Network Management subsystem, Intrusion Detection, Topology

INTRODUCTION

Fishing industry is one of the important sectors in India that contribute food and security to and employs around fourteen million people [1]. There are many fishing communities living alongside the long seashore of India, whose living and occupations over generations have been determined by fishing out in the marine.

One of the major problems faced by the Indian fishermen is the lack of proper communication to land while they are at sea. According to interviews conducted with fishermen, they usually go for fishing for 5 days or more at a stretch, during which they travel anywhere from 20 nautical miles to 65 nautical miles away from the shore. As the distance increases they lose the mobile phone connectivity to the land. Other means of communication are rather expensive and are not affordable to these fishermen.

India has more than 7.000 kilometers of coastline having maritime boundaries with Maldives, Sri Lanka, Myanmar, Indonesia, Thailand, Pakistan and Bangladesh [2]. Fishermen unknowingly cross these maritime boundaries and enter into serious troubles. There have been several alleged incidents like Sri Lankan navy personnel firing on Indian fishermen fishing in Palk Strait, where India and Sri Lanka are only separated by twelve nautical miles [3]. Around 530 fishermen have been killed in the last 30 years. The number of fishermen who are injured and die at sea is very

high. Collision of fishing vessels with huge ships is another threat faced by the fishermen which affects their life and property.

Therefore a new project is underway at our center which focuses on providing communication facility to the fishermen at sea using appropriate low-cost technology with which they can communicate to the land. The project is titled as “Mobile Infrastructure for Coastal Region Offshore communication and Network (MICRONet)”. Sometimes the fishermen face some challenges such as storms, maritime border issues, collision of fishing vessels with ships etc. With the help of proper communication some of the challenges may be avoided.

The main objective of this work is to develop a Network Operations Center (NOC) for the communication network being developed. A Network Operations Center is mainly a work space which is used to monitor, manage and troubleshoot the problems on a network. In short, it is a location from which the network is monitored and controlled or network management is exercised over a computer, telecommunication or satellite network.

With the deployment of a proper NOC one can locate and monitor the operations of all the network devices, ensure continuous operation of the servers and services, provide quality support for the network users and troubleshoot all the network related problems. Apart from this it can also provide alerts about the impending storms, maritime border crossing, intrusion of foreign ships etc., to the fishermen in the sea. The NOC will also collect distress signals and other alerts from the boats and relay them to the appropriate stakeholders on land. It will also be used for software upgrades, making configuration changes and other maintenance tasks on the network nodes.

RELATED WORK

BlueTracker [4] is one of the vessel monitoring system that enables tracking of fishing vessels at sea. The system complies with NEAFC, EU, NAFO and SEAFO regulations to exchange data and joint agreements are commonly made between countries. It also completely complies with EU Commission Regulation and Implementing Regulation. It also provides other features like Ship Security Alert System (SSAS), fuel monitoring, Fleet Tracking and Monitoring (FTM), Long Range Identification and Tracking (LRIT) etc. This system is rather expensive and the vessel owner may also have to pay for the installation, maintenance and continuing communication cost.

Sog Indonesia Asset Monitoring and Surveillance system [5] consists of an equipment to track, monitor and control remote fixed and mobile assets. It helps in vessel monitoring, but one of its main constraints is that it requires long battery life which becomes infeasible for our application.

A satellite-based vessel tracking system [6] enables to monitor the vessel anywhere and anytime in real-time. It also has the ability to monitor fuel usage information as well as transport fuel manifold etc. But this technique uses satellite as backhaul which will be expensive and will not be affordable for the fishermen.

On the other hand, article [7] explains the iDirect system which incorporates an efficient form of TDMA called Multi-Frequency (MF), deterministic TDMA (D-TDMA), which will permit multiple ships to share the same incoming capacity. It guaranties fast response time and is known for the varying nature in which the network can be designed. iDirect’s iVantage Network Management System (NMS) is used to configure, control and monitor the health of the ship’s

communication services from one central location. The service providers can form networks of any size and can upgrade networks automatically without visiting the site.

Paper [8] explains some tips that can be incorporated into a network operations center so as to make it simpler and be able resolve the network issues before it affect the entire infrastructure or organization. This paper discusses some of the useful capabilities that are required to build a network management system. The paper solves many problems like handling all the alerts in a timely manner at the same time managing them at a central level. Each of the tips mentioned in the paper is very useful in the NOC design for MICRONet. Mapping of network topology, customizing the NOC, and centralized alert management are the most important features in the NOC design. The paper gives some of the capabilities which can be implemented in a NOC so as to make it more simplified.

Another work [9] explains the five functional areas of network management which includes performance management, fault management, security management, configuration management and accounting management. The main aim of the paper is to provide information on each functional area to increase the overall productivity of current management tools. It also provides design guidelines for future execution of network management tools and technologies. This paper gives some of the capabilities which can be implemented in a NOC so as to make it more simplified, but it does not provide details of how it can be implemented. The main goal of a network is to provide data transport services to user devices and applications so that they can easily interact with each other and exchange information. So the management of these networks is very essential. A network management system uses various tools and applications that assure optimal configuration, fault, performance, accounting and security management across the entire network infrastructure and applications. All of the five functionalities could be implemented in MICRONet NOC. The network developed for MICRONet should be fault monitored and corrected, should be managed in terms of configuration, security, performance and accounting.

Article [10] is the user manual for AirControl which is a powerful and intuitive device/network management application which allows the operator to manage the network of Ubiquiti devices. This management application allows the operator to manage the network of ubiquiti devices alone. It also provides a north-bound web services API for configuring and monitoring several service parameters. Other vendor devices are not supported by Ubiquiti device manager. It can be used as a management tool for managing the network devices of MICRONet since we will be developing a prototype backhaul network using Ubiquiti base stations and customer premises equipment (CPE). The access network will have devices from other sources. Our aim is to provide a framework for mapping network topology, customizing the NOC, and centralized alert management which can be implemented in the NOC. In addition, our NOC will provide some valuable applications for the fishermen.

In article [11] the author points out the shortcomings of the existing network management solution framework and also examines the existing trends in network management domain. The paper also explains some future outlook on concepts and technologies which can be applied in next generation network management solutions. The author has mentioned smart plugins (SPI) as one of the solutions to manage the new devices, protocols, etc., which may not be generic in nature. But due to the existence of proprietary protocols and technology, information may not be easily available to the developers of these SPIs [11]. Another gap is that the Root Cause Analysis techniques (RCA) are not always straight forward, when the network elements are interconnected

in a complex manner. The author provides a broad view on Environment Aware Network Management Solutions based on MTTR (Mean-Time-To-Repair), RCA and Swarm Intelligence Solutions based on distributed solution along with Predictive Network Management. Our NOC will enable scalability based on swarm intelligence in network management. Another aspect in our NOC will be predictive network management that would result in proactive alerts to avoid maritime border crossing, vessel collisions, avoidance of obstructions etc.

The journal [12] explains some of the network management issues and challenges in sensor and ad hoc networks. Paper says that since the WSN (wireless sensor network) nodes are discardable, the fault management is different from those of traditional wired and wireless cellular networks. The paper also discusses about the significant requirements that must be considered in managing these networks. Some of the factors includes topology management, working in insecure environment, dynamicity, heterogeneity of devices, bandwidth and energy constraint. The issues that should be addressed by the WAHN (Wireless Ad Hoc Network) are node positioning, security, network mobility, network traffic, communication intermittence, misbehavior of communication and routing. The paper also introduces few of the articles that solves the challenges in WAHNs and WSNs. The MICRONet architecture has some attributes of an ad hoc network so the methods used in the paper could be incorporated.

In research paper [13] the authors have tried to address the issue of managing a stable communication path between the two nodes regardless of the mobility of the system. They have established an agent-centric protocol that will achieve uninterrupted communication over the selected routes. This protocol consumes minimal network resources. Their work is divided into two logical steps. In the initial step they describes an agent-based framework with its associated protocols and mechanisms. The main aim of this agent-based framework is to make all the nodes in the system topology aware. For obtaining the velocity, geographical coordinates and direction of movement of each node they use GPS system. The next part of the work tries to make use of this topology awareness to establish and manage a connection between two nodes. For managing the network, the position, velocity and direction of movement should be known to the NOC.

Enterprise Management Associates (EMA) [14] examines the seven challenging areas of a network manager and best practice that are emerging as a result. This research is mainly focused on network management. The seven best practices mentioned by the author includes Integrating Management Functions, True Multi-Vendor Support, Integrated Management of Virtual Networks & Cloud Resources, Automation, Unified Policy Management, Proactive Operations Monitoring, and Communication. These practices can be incorporated to the NOC to make it better.

The research work [15] introduces an adaptive management architecture for ad hoc networks. [16] and [17] explains about the network management and network operations center. The research work [18] introduces a maritime border alert system which uses GPS system. Another research work [19] analyses and proposes a set of innovations for the NOC infrastructure.

A patent by Lee et al [20] provides an apparatus for managing ship networks. Another patent [21] provides a marine threat monitoring and defense system and protects the vessel from obstacles. The patent [22] provides a marine emergency position indication system which can communicate wirelessly between beacon and search engine.

REQUIREMENTS OF NETWORK OPERATION CENTER

Network management can be done in-band or out of band. We assume the presence of an in-band management channel for the purpose of network management. This channel could be routed to the shore station through a combination of Wi-Fi mesh network of boat clusters and a backhaul link from boat to shore. Some of the requirement for the NOC is listed in this section.

Topology Management

Topology management includes locating the node, intrusion detection, grouping of network elements, representation of topology etc.

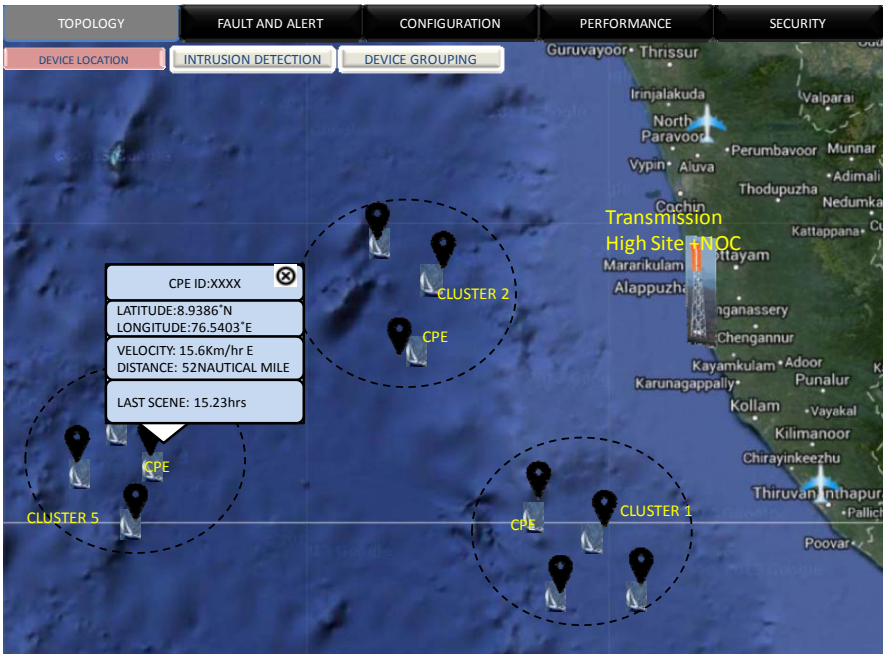

Fig.1. Topology Management of NOC

Discovery of node: The NOC should be able to discover the node in terms of its latitude and longitude and track the movement of the node. Each fishing vessel may contain a CPE which is connected to an access point and the access point further serves the mobile equipment/clients. Discovery of CPE indicates that the fishing vessel in which the CPE is placed is located. CPE details will be fed into the database a priori. Information such as the number of clients attached to access point, connectivity information of the client and network usage by each user can be obtained from the CPE or the access point. Fig. 1 shows the details of fishing vessel in the NOC. It gives the CPE id, location of the fishing vessel in terms of latitude and longitude, velocity of the boat and the distance traveled by the boat from the shore.

Intrusion detection system: A network operations center itself can act as an intrusion detection system that monitors the network for any malicious or foreign nodes. If a new node enters the

network which is not listed in the database, the NOC indicate it as a foreign node that could be potentially malicious and this can be identified in the GUI as any warning or indication. Fig. 2 is the screen shot of the NOC view for intrusion detection.

Grouping of network elements: The network elements in this network can be grouped based on dynamic logical clusters of boats. At a high level, each cluster may be represented as a composite node. It would be easy for a network operator to monitor the health and performance of a cluster of boats.

A network may consist of network elements of different types, models, versions and makers. With such a network, it is difficult to get a logical understanding of network issues. So to solve this, it is better to create a logical grouping of devices based on these attributes, which will allow you to monitor and manage the devices as groups rather than as individual nodes.

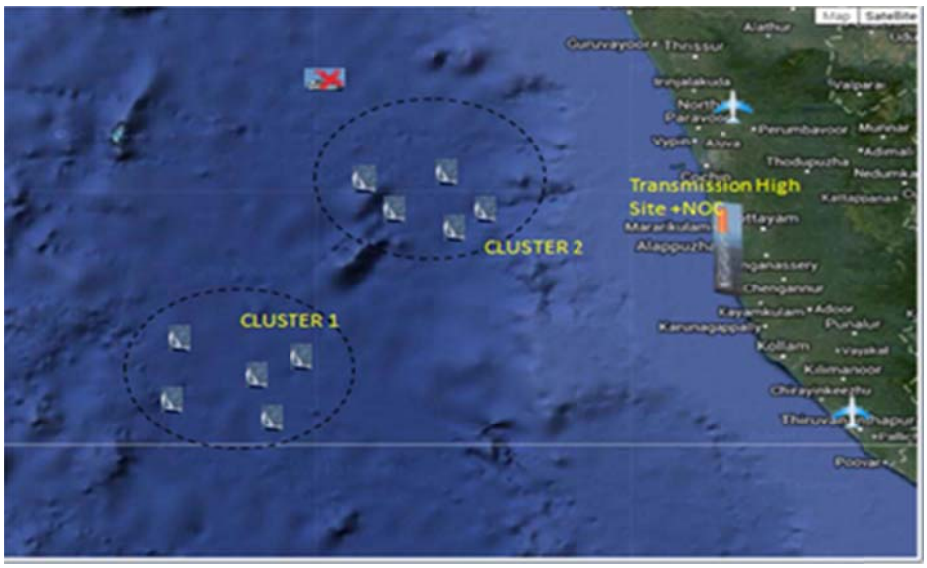

Fig.2. NOC view for intrusion detection

Representation of topology: There should be a topology representation for every network for the ease of monitoring the network. Usually fishermen go for fishing in small groups or clusters, where in each cluster there are a few boats. Some boats equipped with a CPE may act as backhaul links. A primary and secondary backhaul link may be present in each cluster. All boats in a cluster are served by the primary backhaul link. The secondary backhaul acts as a redundant node and in case of any failure of primary backhaul, the secondary backhaul comes into play. They may also provide some load-balancing in an active-active configuration.

At a high level each cluster may be represented as a composite node. The composite node can be drilled down to get the details of that cluster. All boats in the cluster will be shown in a pop-up window. Drilling down further into a boat will show the CPE, access point and user equipment on that boat. Fig. 3 shows the drill down function on NOC.

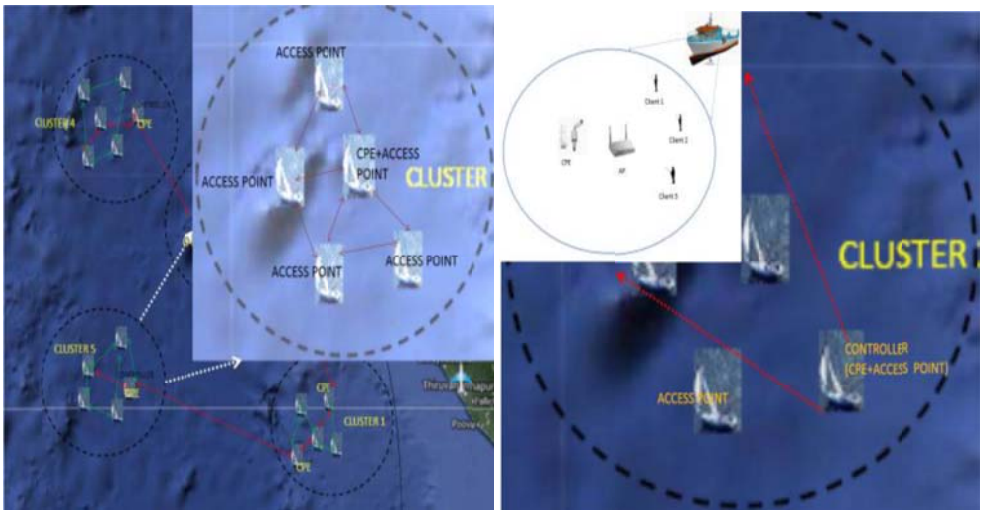

Fig.3. Drill down Function of NOC

Fault and Alarm Management

Fault and alarm management helps to detect and isolate the faults encountered in a network and notify the operator about them. Faults in a network can cause unacceptable network degradation and therefore fault management is very essential in a network [9].

Alerts and alarms: Alerts and alarms are very useful in a network with huge number of network devices of different manufactures. It would be easier for a network operator to analyze and debug when the alerts and alarms are received at a centralized location. Receiving the alerts at a centralized location helps to compare the alerts, eliminate inaccurate alarms, deduce alert patterns and track alert history. The main challenges of alert management are receiving alerts in a timely manner and managing them at a centralized level [8].

Correlation of events: In a network, a number of informational messages are generated by the devices. It might become difficult for a network operator to identify the critical information. Event correlation can reduce the information overload by taking care of typical scenarios like frequent alarms and duplicate alarms. With event correlation, a network operator can discriminate between warnings, errors, information messages etc. For example in the case of MICRONet, the network operator can discriminate whether there is a boat disruption, power down of the device or a lost connectivity.

*Dynamic prioritizing**:*** Dynamic prioritizing allows analyzing the data faster so that the network operator can understand what needs attention first, such as which node is currently moving closer to maritime border, what are the major errors in the network, what are the critical alarms that need to be attended faster, and so on. Fig. 4 shows a screenshot of fault and alert management of network operations center.

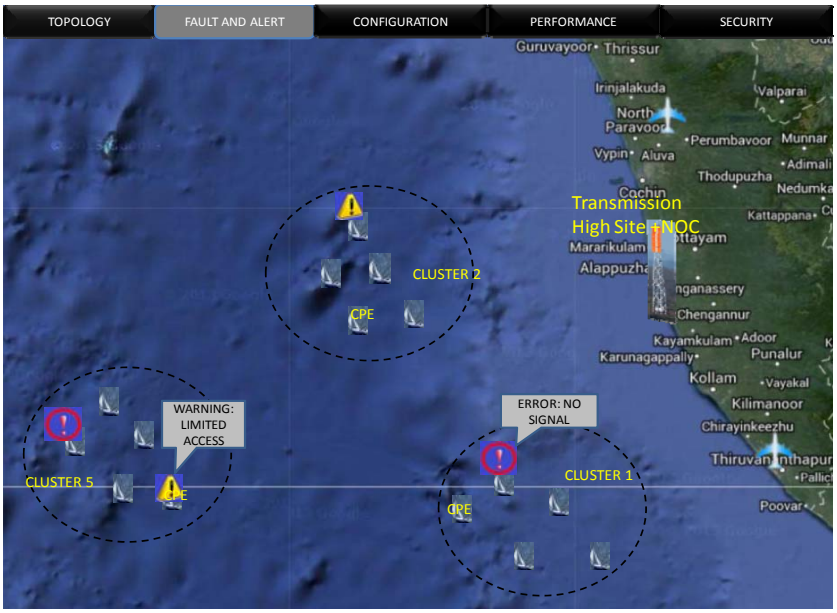

Fig.4. Fault Management of NOC

Configuration Management

The main objective of configuration management is to monitor the configuration information of the network and system so that the effects on network operation of a variety of hardware and software elements can be tracked and managed.

Inventory management: For discovering a device in a network, the network management platform should have the list of its devices in the inventory database. Detailed configuration information on network devices is provided by the inventory database. The nodes using the MICRONet network should initially register their device in the inventory database.

Apart from this, remote backing up of the device configuration helps in restoring the content if the configuration file is lost or corrupted on the device. Also with the help of firmware upgrade and troubleshooting the network operator can add extra features to the device and fix the bugs.

Performance management

Performance management mainly focuses on the performance of the network. It includes throughput of the network, packet loss in the network, quality of service, data rate, delay and heterogeneous data management.

Predictive modeling

Predictive modeling can be very useful in MICRONet. The NOC will get signals at constant period of time. The information about the speed and velocity of the vessels will be known to the NOC. Using this information the new location and the trajectory of the vessels can be predicted.

Also, from the previous message history and activity log NOC can predict if the vessel is approaching any obstacles. Predictive modeling can also be used in prior fault detection.

Integration of Device Management Applications
In a network different devices may be of different vendors and they use different vendor applications for management. Integrating the vendor applications can reduce time and money and will help the network operator to get a comprehensive view of the NOC functions. Integrating the vendor applications simplifies the operations, allows the network operator to customize the interface, and NOC could be operated with fewer work forces. The integration could be tight or loose depending on the north-bound interfaces provided by the device managers of different vendors.

Security management
The main objective of security management is to control the network resource access, thereby protecting the network resources from being disrupted. Security management can keep an eye on users logging onto a network resource, and refuse access to unauthenticated users.

Authentication and access control: Authentication is a method to identify the users before allowing them to access the network. All the users using the MICRONet should be registered initially, only the registered users should be able to access the network. For node authentication and access control, AAA servers such as RADIUS can be used in the NOC.

Accounting
Accounting allows the network operator to identify the services that users are accessing and to bill the users according to the network resources they are consuming. A suitable accounting and billing model could be developed for MICRONet.

NOC SYSTEM ARCHITECTURE

Fig. 5 is the proposed system architecture of MICRONet. The fishermen usually go for fishing in small groups or clusters. In each cluster few boats provide the backhaul links through which communication to the base station takes place. The backhaul will serve the entire cluster and provide connectivity to the internet through the base station at shore. The proposed architecture uses long range Wi-Fi to communicate to the shore. There will be a network operations center situated near each base station which will manage the devices in the network under that base station.

Fig. 6 shows the system architecture of NOC. A network consists of several devices of different vendors. Each device is managed by a device manager of that particular vendor. Finally they are integrated together using a north bound APIs provided by the vendor to a single Network Operations Center. The device manager uses management protocols like SNMP, HTTP, UDP and SSH to communicate with the device.

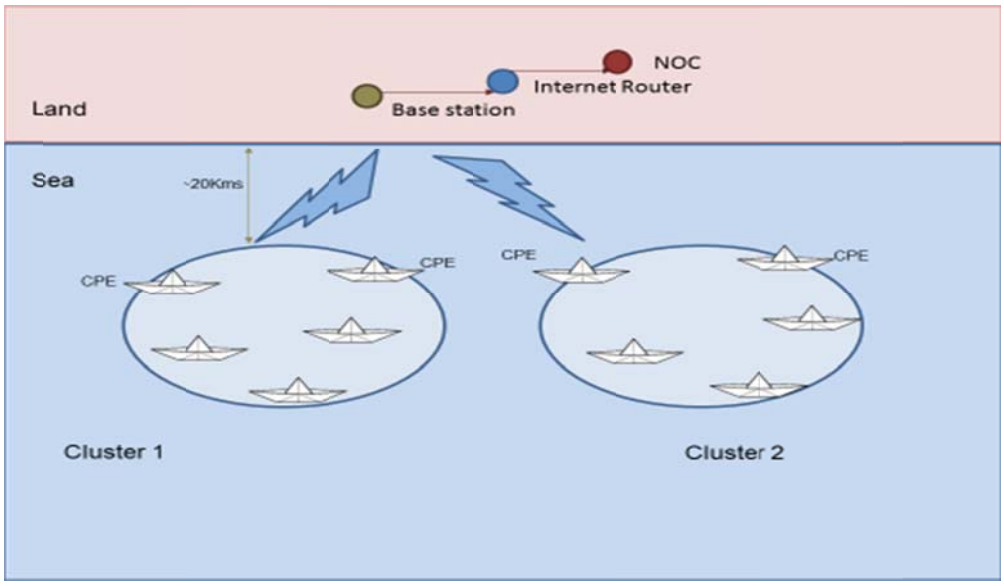

Fig.5. Generalized Architecture of MICRONet

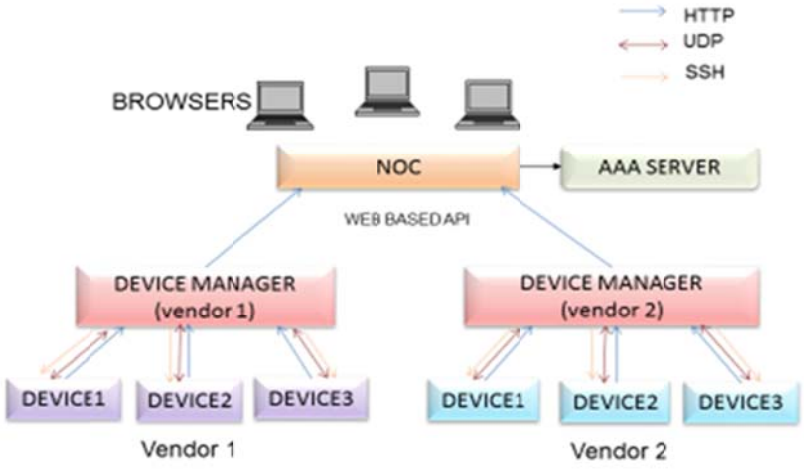

Fig.6. System Architecture of NOC

Initially, the device manager sends a request challenge to the devices which will send a response back to the device manager. Once the device manger gets an authentic response from a device, it puts it under management. The managed devices appear in the device list of the device manager. The device under management will establish a key based secure shell protocol which will ensure the security of the transferred data. The data from the device is transferred to the device manager

with the help of HTTP protocol. Further the device managers are integrated together in a network operations center with the help of a north bound application programming interfaces provided by the vendor.

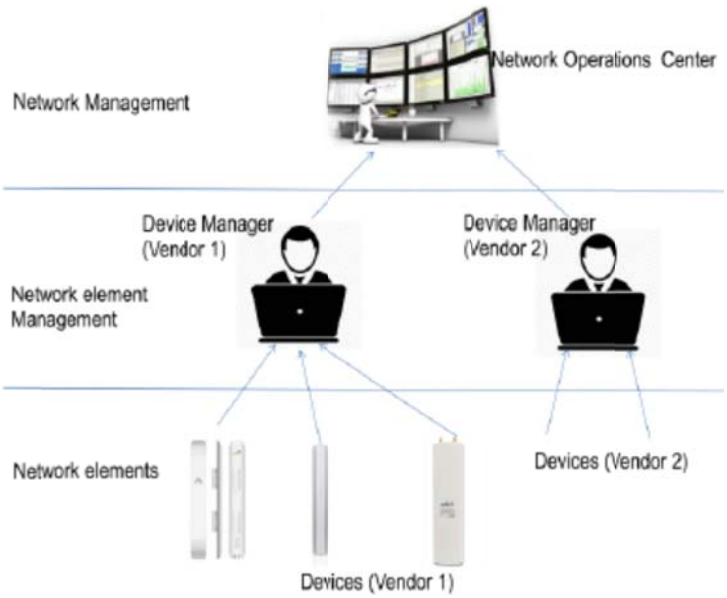

Fig.7. A Typical NOC

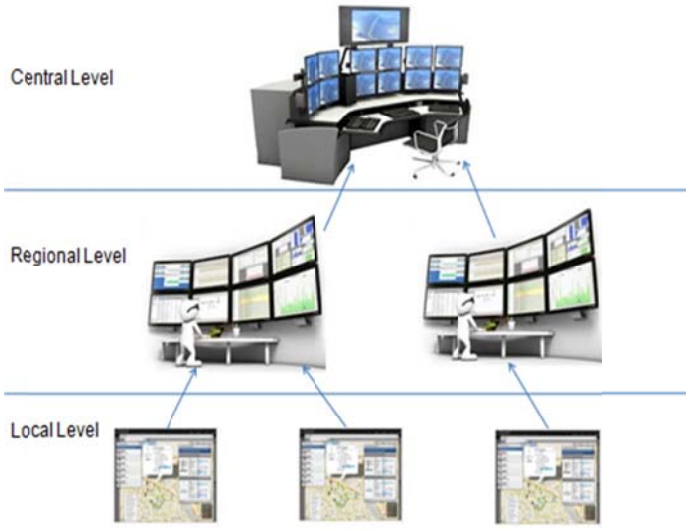

Fig.8. NOC Hierarchy

As shown in Fig. 7, a network operation center consists of three levels. The network element level contains devices in the network, the network element management level contains the device manager and the network management level contains the NOC.

Each base station at the shore is co-located with a network operations center which acts as a local level network operations center. The local NOCs can be integrated together to form a regional NOC which can be further integrated to central level NOC. Thus there can be a NOC hierarchy. Fig. 8 represents the NOC hierarchy.

VALUE-ADDED APPLICATIONS

The network operations center designed for a communication network of fishing vessels at sea could be able to locate, monitor and track the registered fishing vessels, detect intrusion of unauthorized vessels, raise alarms and alerts when needed, and provide value-added applications and services to the fishermen. Some of the services that could be provided by the network operations center to improve the safety and quality of life of fishermen are given below.

Maritime Border Crossing alert

India shares more than 7000km of coastline boundaries with countries like Maldives, Sri Lanka, Myanmar, Indonesia, Thailand, Pakistan and Bangladesh. Crossing the boundaries has become a serious issue. There are several incidents of fishermen being arrested or killed by the navy personnel of neighboring countries due to carelessness or unknowingly crossing the boundaries. In such a situation the life of fishermen is in danger.

With the deployment of a proper NOC one can constantly monitor and locate the fishing vessels and thereby proactively inform the fishermen about the maritime boundary crossing and ensure the safety of fishermen. Fig. 9 shows the NOC view for maritime border crossing alert.

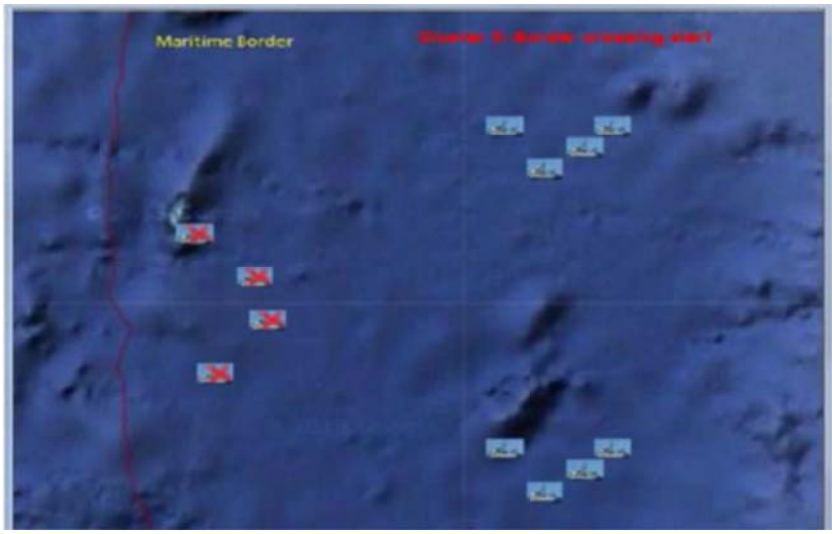

Fig.9. NOC view of maritime border crossing

Collision detection of fishing vessels

Collision between fishing vessels and ships has become a common and frequent threat to fishermen. Fishermen claim that 'near miss' situations are very common and it is of serious concern to them.

A network operations center that could monitor the upcoming ships with their velocity, predict potential collisions based on the trajectories of ships and fishing vessels and inform the fishermen in advance can be very helpful. An AIS system will be installed at the NOC for this purpose. Fig. 10 is the NOC view for collision detection alert.

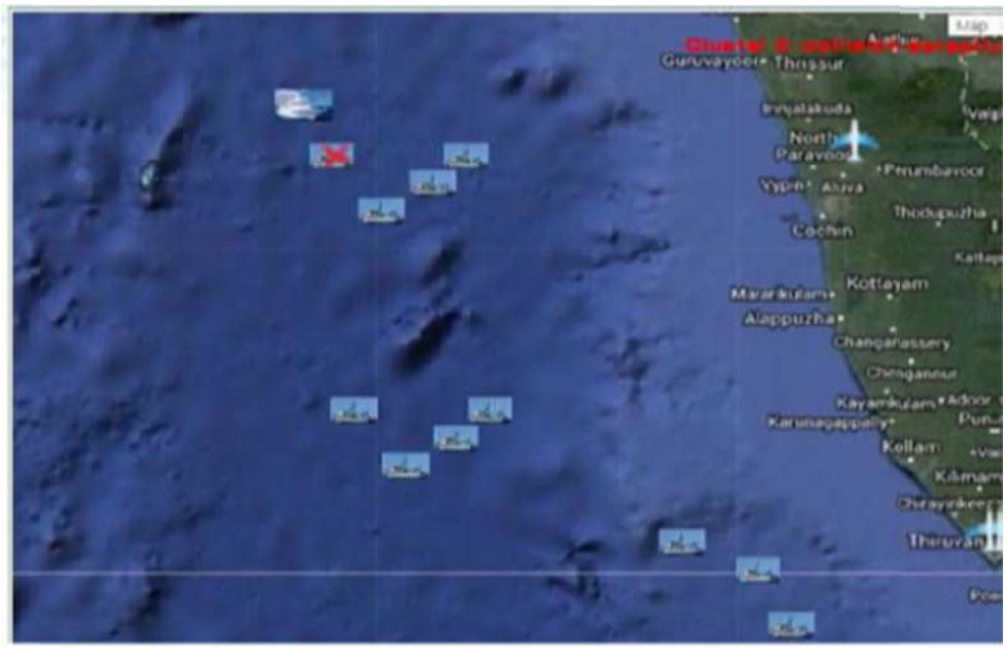

Fig.10. NOC view for Collision detection alert

Obstacle alert system

Many of the fishing vessels in India have an echo sounder which helps the fishermen to locate the shoal of fish and the obstacles in the sea bed that could damage their fishing net. The network operations center can have a database or activity history that could save the position of the obstacles and inform the fishermen in advance about the safe location where they could fish and about the locations they need to avoid. This will be especially helpful for the smaller boats not equipped with an echo finder.

E-Commerce

With the help of network operations center the fishermen can be informed about the current market trends which could be very beneficial for them so that they could fish accordingly. They could also be informed about vessels in their vicinity that may be interested in buying their catch or transporting their catch to the shore.

CONCLUSION

A communication network which could provide a seamless communication facility for the Indian fishermen at sea would be a great boon to them. A Network Operations Center for this communication network would monitor, manage and troubleshoot the entire network and also provide value added applications and services to the fishermen. In this paper, we described the functional requirements of the network operations center followed by the system architecture and some of the value added applications of network operations center.

FUTURE WORK

A prototype implementation of MICRONet is planned using long-range Wi-Fi technology and directional antennas. In this context, a NOC incorporating the functional requirements outlined in this paper will be built. The value-added applications described in this paper will also be implemented.

ACKNOWLEDGEMENT

This project is partly funded by a grant from Information Technology Research Agency (ITRA), Department of Electronics and Information Technology (DeitY), Govt. of India.

REFERENCES

B. Meenakumari, Fisheries in India- Way Forward, Website, 2013. [Online]. Available: http://indomareclim-nerci.in/publication/mppw2013/PdfWinterSchoolx/Meenakumari.pdf

Capitão-tenente, "Naval Power In India`S Geopolitics", January 2013 http://www.revistamilitar.pt/artigo.php?art_id=798

The Times of India, Jan 24 2011, *Second TN fisherman killed by Lankan Navy*, http://timesofindia.indiatimes.com/india/Second-TN-fisherman-killed-by-Lankan-Navy/articleshow/7350366.cms?referral=PM

BlueTracker, "Vessel Monitoring System (VMS)," [Online]. Available: http://www.bluetraker.com/solutions/vessel-monitoring-system-vms/

Sog Indonesia, "Asset Monitoring and survellance System," [Online]. Available: http://www.pt-sog.com/ats.html

Instink, "Ship Management System," [Online]. Available: http://www.instink.co.id/ship-management-system

iDirect, "Maritime vsat communications solutions," 2010. [Online]. Available: http://www.idirect.net/_/media/Files/Maritimeritime.ashx

Vinod Mohan ,"5_tips_for Creating your ow Network Operations Center", SolarWinds, 2014

Network Management System: Best practices White Paper, CISCO, July 11, 2007

Aircontrol User's Guide, Air Control UbiQuiti, 13 July 2011

Ankur Gupta, "Network Management: Current Trends and Future Perspectives," Journal of Network and Systems Management, 17 October 2006

Mehmet Ulema, Jose Marcos Nogueira, and Barcin Kozbe, "Management of wireless Ad Hoc Networks and Wireless Sensor Networks," in Journal of Network and Systems Management, Vol. 14, No.3,September,2006.

Romit Roy Choudhury, Krishna Paul, Somprakash and Bandyopadhyay, “An Agent-Based Connection Management Protocol for Ad Hoc Wireless Networks,” in Journal of Network and Systems Management, Vol. 10, No.4, December, 2002.

EMA, “Seven best practices for network management,” 2013. [Online]. Available: http://h20195.www2.hp.com/V2/getpdf.aspx/4AA4-5440ENW.pdf

C.-C. Shen, C. Srisathapornphat, and C. Jaikaeo, “An adaptive management architecture for ad hoc networks,” Communications Magazine, IEEE, vol. 41, no. 2, pp. 108–115, Feb 2003.

D. W. Stevenson, “Network management what it is and what it isn’t.” 1995. [Online]. Available: http://www.sce.carleton.ca/netmanage/NetMngmnt/NetMngmnt.html

R. Blum, “Network operations centers,” 2001. [Online]. Available: http://penta2.ufrgs.br/tutorials/qos/noc01.pdf

M. Sivaramaganesh, M. Ramya, V. Goutham, T. Bharathi, G. Jeevitha “Implementation of Maritime Border Alert System,” International Journal of Innovative Research in Electrical Electronics Instrumentation and Control Engineering, pp. 1254–1257, Mar 2014.

R. Prasad, P. Donadio, A. Cimmino, “A cloud infrastructure to manage future internet: The virtual network operation center,” Journal of Green Engineering, pp. 255–265, Mar 2011.

K. Lee, J. H. Park, “Apparatus for Managing Ship Network,” U.S. Patent 20140129701A1, May 8, 2014.

J. R. Gagliardi, D. Flynn, J. Grant, “Marine Threat Monitoring and Defense System,” U.S. Patent 008612129B2, December 17, 2013.

X. Yan, Y. Liang, P. Yan, “Marine Emergency Position Indicating System,” U.S. Patent 20140191865A1, July 10, 2014.