RC24961 (W1003-055) March 17, 2010
Computer Science

IBM Research Report

Management of Coalition Sensor Networks

Dinesh Chandra Verma
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598

Theodore Brown, Carolyn Ortega
City University of New York
365 5th Avenue
New York, NY 10016

Management of Coalition Sensor Networks

Dinesh Chandra Verma[a], Theodore Brown and Carolyn Ortega[b]
[a]IBM TJ Watson Research Center, 19 Skyline Drive, Hawthorne, NY 10532, USA
[b]City University of New York, 365 5th St, New York, NY 10016, USA

ABSTRACT

The management of sensor networks in coalition settings has been treated in a piecemeal fashion in the current literature without taking a comprehensive look at the complete life cycle of coalition networks, and determining the different aspects of network management that need to be taken into account for the management of sensor networks in those contexts. In this paper, we provide a holistic approach towards managing sensor networks encountered in the context of coalition operations. We describe how the sensor networks in a coalition ought to be managed at various stages of the life cycle, and the different operations that need to be taken into account for managing various aspects of the networks. In particular, we look at the FCAPS model for network management, and assess the applicability of the FCAPS model to the different aspects of sensor network management in a coalition setting.

Keywords: Sensor Network Management, Coalition Operations, Senor Networks

1. Introduction

Sensor networks are commonly deployed in many types of environments, ranging from military operations to civilian applications such as utility monitoring, livestock tracking and civil surveillance. As the sensor networks grow in their size and complexity, a need arises to manage the networks so that they can continue to operate in a smooth manner. Some issues related to management of sensor networks, e.g. optimizing bandwidth and efficiency, are being addressed in the research community [1]-[6]. However, there is no holistic treatment of the management aspects of sensor networks.

In this paper, we attempt to provide a comprehensive approach to management of sensor networks. Our approach, based on the way computer communication networks are managed,, is to apply the network management model to the domain of sensor networks. There are several key differences in the operational aspects of traditional computer networks and sensor networks, and these differences require consideration when one is looking at the proper management of sensor networks. Our goal in this paper is to articulate these differences and account for changes in the management model that can address those differences. Additionally a sensor network built by a coalition requires careful management between the partners.

To set the stage, we begin this paper with a section that provides an overview of the four stages of the management model for computer communications networks. This is followed by a section which describes the domain of coalition sensor networks and its life-cycle. In the subsequent three sections, we propose a management model for the various life-cycle stages of coalition sensor networks. Finally, we present our summary.

2. Overview of Network Management

The concept of the stages of network management is well developed for computer communication networks and distributed systems. Different types of management tasks are performed during different stages of the life-cycle of a computer network. We begin by describing the life-cycle of a computer network, followed by a discussion of the different types of management operations that are required for each stage of the life-cycle.

2.1. Computer Network Life Cycle

A computer network goes through the four stages or phases of the life-cycle as shown in Figure 1 below. The first phase is planning, in which plans are made for the roll out of the computer network. This is followed by the implementation phase in which the network is physically installed. In the operation phase, the network is up and running. Subsequent to the operation phase, the network may need to be upgraded, or terminated.

The upgrade phase starts the planning, implementation and operation cycle once again.

During the planning phase, network requirements and specifications are developed that must be fulfilled by the network plan. T he plan for the network is developed so that the desired attributes of performance, security and usability experience are satisfied. Typical management tasks that are performed during the planning cycle include capacity planning, energy management planning, security management planning and designing the network. The planning cycle starts with the specification of the requirements of the network, and concludes with a design plan or specification of the network to be implemented.

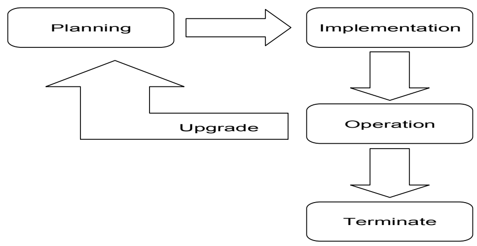

Fig. 1 Life Cycle of a Network

During the implementation phase, the system is rolled out. In the implementation phase, the main network management task is validating that the implemented network conforms to the plans and designs developed in the planning phase.

The bulk of network management operation happens during the operation phase. The network management tasks in the operation phase consist of two components; a management activity chain, which defines the sequence of activities to be performed for management and a functional description for different activities, performed in management.

2.2. Management Activity Sequence

The management activity chain is an abstract description of different types of activities that need to be performed for IT management. As shown in Figure 1, the management activity chain consists of discovery, monitoring, and analysis, which may be followed by reporting or reconfiguring. This activity chain is performed by the staff at the operations center of the IT infrastructure to ensure that the system is running properly.

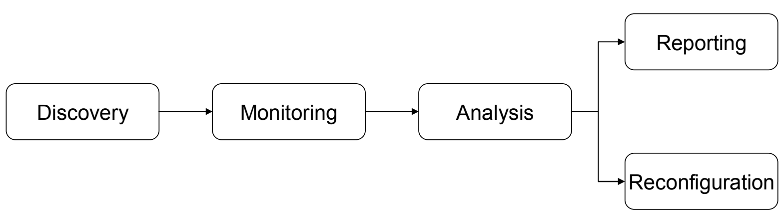

Fig. 2 Activity Sequence for Network Management

The first management activity required of the operations center staff is that to know what is in the infrastructure, where the infrastructure is located, and what its various constituents are. The operations staff cannot manage elements of the infrastructure whose existence is unknown. The first function at the operations center is the function of discovery of the elements of the infrastructure. The discovered elements in the infrastructure form the inventory of assets in the IT infrastructure. An asset is any element of the IT infrastructure. The assets that are found during the discovery may be physical, e.g. networking gear, server boxes, and other equipment, or they may be virtual entities such as installed software, software packages, and their configuration.

Monitoring consists of retrieving the right management data from the IT infrastructure. Different management functions may require monitoring different types of data. Performance monitoring may require reading in counters of assorted types from different elements of the infrastructure, while fault monitoring may require processing reading error logs within the system.

Analysis consists of understanding the monitored data, processing it to reduce its volume, and determine the right reaction to any issue that arises from its analysis. The analysis function is the area where data analytics is commonly applied, but data analytics has its impact on the other activities as well.

The output from the analysis is either a report to an external entity or report identifying a need for a reconfiguration. An example of a report to an external entity could be an accounting analysis, which could result in a report to a billing system to be processed further, or a performance analysis, which could provide periodic performance results of the network. An example of a report, which may result in the reconfiguration of the system, is a performance analysis. The performance analysis could indicate that some elements or parameters of the system require reconfiguration for optimal performance.

2.3. Management Functions

The activity chain is repeated for different types of management functions that are needed. In a telecommunications network, it is common to describe these functions using the FCAPS paradigm: management is traditionally classified into five functions abbreviated as FCAPS, which is an abbreviation for **F**ault, **C**onfiguration, **A**ccounting, **P**erformance and **S**ecurity. The concept of these five functions of network management originates from various network management specifications provided by the International Telecommunications Union (ITU). While these specifications were targeted for the telephone network rather than general IT management, the FCAPS paradigm provides a reasonable conceptual model to study the different aspects of management for many different types of networks.

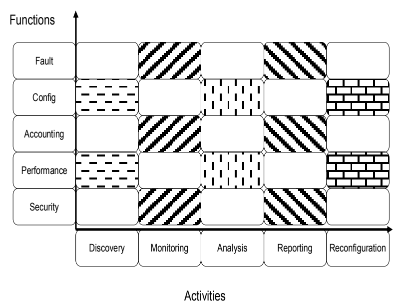

Fig. 3 The Matrix of Management Tasks in Operational Stage

The focus of fault management is on detecting and identifying the failures that occur in the network, and taking corrective actions to work around those failures. The corrective action may be taken by an automated system or with human intervention. Configuration management ensures that different elements (hardware as well as software) that are required for the operation of the system are configured in an appropriate manner. Accounting management deals with maintaining charges and costs that are associated with the use of the system. Performance management ensures the system is operating with an acceptable level of response time. Security management deals with mechanisms to thwart hackers, and ensuring that system and information access is restricted to duly authorized and authenticated users.

3. Coalition Sensor Networks

In order to examine the management tasks required for coalition sensor networks, we need to look at the specific nature of such networks and compile a list of management tasks that must be performed at various stages of the life-cycle. A coalition sensor network consists of a sensor network that is built and operated using ISR assets from two or more partners operating in a coalition. In a typical coalition operation, an ISR Community of Interest (CoI) is dynamically formed to conduct joint coalition operations. An ISR CoI can be an ad-hoc team consisting of several coalition partners executing many concurrent missions. Such missions include border/perimeter reconnaissance and surveillance, camp site surveillance, and detection/classification of human activities in concealed/confined spaces or locations of human infrastructures. A CoI brings together a set of ISR assets, specific missions, and sets of policies that govern information security and fusion and sharing/dissemination of information.

In current practice, much of the management of coalition networks happens in an ad-hoc manner. However, if one postulates a variation of the life-cycle model for general networks and tries to follow the life-cycle stages in the management aspects of this network, the network can be operated in a better manner and satisfy all requirements and constraints imposed by individual nations making up a coalition. In this section, we propose a life-cycle model of coalition networks modeled towards this goal as shown in Figure 4. The nuances of coalition operation with a sensor network require the explicit calling out of its differences.

Such a model is shown in Figure 4. As shown in the figure, the life-cycle of the coalition ISR network consists of five distinct phases. Comparing the life-cycle diagram to that of Figure 1, we notice that the planning phase is broken down into two stages, mission planning and operation planning. This refinement of the life-cycle into two stages is a consequence of the specific structure of coalition operations, where distinct decisions need to be taken in these two steps.

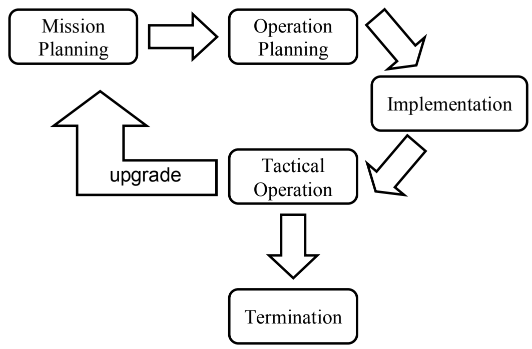

Figure 4. Life Cycle of Coalition ISR Network

In the *mission planning phase*, decision makers from different coalition partners come together to negotiate and develop the common operating principles and policies that would apply to coalition information flows and any ISR assets that may be shared during coalition operations in the specific area. At this stage, the ISR networks and systems are not necessarily fully deployed, established or operational in the area of operation. However, if there are not enough assets deployed already, each partner in a coalition would need to have an inventory of ISR assets that they are willing to share/deploy for coalition operations and be willing to allow limited visibility to the other coalition partners to that inventory and its capabilities.

In the *operation planning stage*, members from the coalition come together to design and plan the structure of the coalition ISR network that will be deployed in the area of operation. The operational planners need to follow the policies that have been established by the mission planners in the previous stage.

The operation planners would be tasked to plan how to undertake and execute the mission. During this stage, they would need to determine the nature of the ISR network they need. They would need to find out the optimal (or minimally required) set of ISR assets and the network configuration of those assets in order to perform the tactical operation.

In the *tactical operations stage*, the ISR networks are deployed and available for operation. The different ISR networks would be interconnected between coalition partners through policy-enabled gateways. These gateways would enforce any policy constraints that are applicable as information flows between different ISR networks.

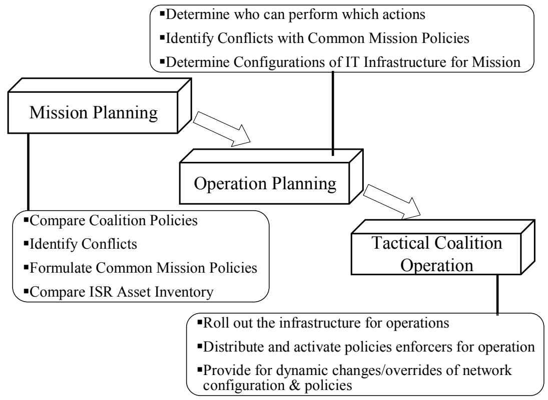

Figure 5. Operations in different Life Cycle Stages

Each operation needs to end, and the coalition ISR network may need to be terminated at the end of the operation (*termination stage*). In this case, the operators may need to retrieve the assets from the area of operation and return the assets to respective coalition partners. Any data retention and end-of-life policies related to disposing of data and information would need to be complied with at this stage.

Figure 5, which follows the paradigm described in [10] enumerates the different operations that are needed to be done during different stages of the life-cycle. Let us now focus on the management aspects of the coalition sensor networks that need to be performed at each of these stages of the life-cycle.

4. Management Tasks during Mission Planning

Let us examine in more detail the different operations related to management that are required during the mission planning life-cycle stage. Although the primary goal of the mission planning life-cycle stage is the determination of the guidelines, policies and other constraints which will be applicable for the mission planning cycles, different subsets of sensor network management need to be taken into account when performing the actions of the mission planning life-cycle stages.

Since our focus is on the management aspects of mission planning within the coalition, we look at the non-functional requirements of the mission planning stages. The non-functional requirements deal with aspects such as performance, security, and resiliency attributes that need to be satisfied during the mission planning stage, as opposed to functional requirements, which specify the nature of the data collection and operation of the sensor networks that will be planned in this stage. As was described for the management tasks of the general network, we will specify the management tasks of the sensor network by means of an activity diagram and a function matrix.

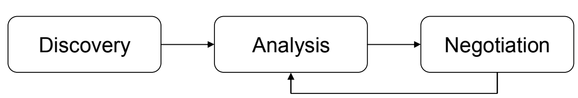

Fig. 6 Activity Sequence for Mission Planning Life Cycle Stage

The activity diagram describes the actions that need to be taken for the management tasks related to network operations. This activity diagram consists of three stages: (a) a discovery stage in which the applicable policies of the current coalition partners is determined (b) a conflict analysis stage where the conflict between the different policies are evaluated and (c) a negotiation stage where the applicable policies for coalition operations are negotiated.

After applying the functional matrix of FCAPS to the task of mission planning, we can now determine the type of policies that ought to be negotiated in the mission planning stage. Specifically, the discovery, analysis, and negotiation ought to cover the following types of policies:

Fault Policies: These policies should specify which partner is responsible for fixing problems and failures that arise in the coalition networks, and how assets could be shared across different members in the eventuality of a fault or failure arising within the network.

Configuration Policies: These policies ought to describe the required software configuration, and system configuration that should be supported during the operation of the coalition sensor networks.

Accounting Policies: These policies ought to describe how the coalition sensor assets would be tracked, monitored, and inventoried. These may require use of specific tools, or specific responsibilities to be undertaken by different coalition members. This can be especially sensitive when partners do not fully trust one another.

Performance policies: These policies need to describe the performance characteristics of the system that the different coalition partners would bring to the table, including aspects such as quality of information, latency in measuring, latency in reporting and desired battery lifetime that should be satisfied by the assets deployed in coalition sensor networks.

Security Policies: These policies need to describe the security characteristics of information collected, stored and disseminated in the coalition networks, including aspects such as which asset or information is visible or partially visible to which coalition partners, and under what circumstances.

Each of these different types of policies should be negotiated, their conflicts among different coalition members determined, and the impact analyzed by the mission planners to come to a mutually acceptable set of consistent coalition policies.

5. Management Tasks during Operations Planning

The major task in the operations planning phase is determining the nature of the sensor network that is to be deployed into the network. This stage of the planning is involved in obtaining the sensor network to be deployed while satisfying the policies negotiated in the mission planning stage, and meeting the desired non-functional requirements of the coalition sensor network. The planning activity diagram would consist of (a) taking an inventory of available assets (b) identifying the requirements and policies and (c) designing a network to satisfy the requirements.

Without going into the complete details of the various planning steps (see Chapter 2 in [7] for a more detailed discussion), the requirement identification and network design would need to look at the following attributes obtained from the FCAPS model.

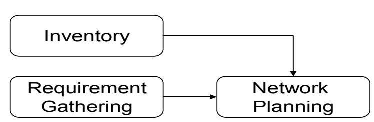

Fig. 7. Activity Sequence for Mission Planning Life Cycle Stage

Fault Requirements: These requirements would specify the level of redundancy of the coalition ISR network and the degree of k-redundancy required to define its coverage of any monitored area. It could include inter-coalition partner redundancy cooperation.

Configuration Requirements: These requirements would specify how the configuration and reconfiguration of the sensor network would be done, including any systems that need to be put into place for validating compliance of the configuration with the desired guidelines.

Accounting Requirements: These requirements describe how the coalition sensor assets would be tracked, monitored, and inventoried. Satisfying the requirements may require periodic use of an inventorying or a data monitoring tool.

Performance Requirements: These describe the latency and bandwidth constrains to be met by the deployed network.

Security Requirements: These would specify the security mechanisms, information sharing requirements and information confidentiality requirements imposed on the network.

Looking at the requirements in this functional model ensures that the planning process has incorporated all aspects of the requirements, as opposed to being performed in an ad-hoc manner.

6. Management Tasks during Network Operation

Of all the phases, the network operations phase in the life-cycle phase of the management burden is maximal in commercial communications networks. Similarly, the management tasks that need to be performed in the operational phase of the sensor network is the most complex one. The additional complexity in the management tasks of coalition ISR networks is created by the fact that the bandwidth and connectivity to the sensor networks is usually constrained, making some of the tasks to be performed in regular network management harder. Although the activity diagram for management tasks would remain the same as in Figure 2, the nature in which the operations are performed would be very different.

Discovery: Since the sensor network is not always connected, discovery of the coalition's sensor network should be performed by a combination of inventory asset tracking and by locating its assets, e.g., when a reconnaissance platform is driven nearby the sensor and can identify the location. An alternate way to discover the sensor network is by examining the sensors that are sending information actively to the monitoring station, and identify those assets as being active. Extrapolation from the monitored information and combining them with the asset discovery allow for discovery of an entire sensor network without using up precious bandwidth.

Monitoring: The monitoring of sensors for their status and health metrics is a critical part of sensor information. Since bandwidth is limited in sensor networks, the traditional approach for collecting monitored information separately is not adequate. Sensor networks can be monitored by extrapolating their health using the sensed information sent by the sensors. Sensors that can periodically include their health and management information as a metadata field of the sensed information would be easier to manage and track than those that do not. When necessary, some of sensors can be requested to send its metadata.

Analysis: Once the monitored information about the health of the sensors in the field is obtained by monitoring, the different functional aspects of the sensors need to be determined, and the root cause of any failure ought to be determined. Unlike connected communication networks, one cannot run diagnostics tests over a sensor network. As a result, schemes such as decision trees may not be appropriate for sensor networks. However, one could develop mechanisms to identify faulty sensors from the stream of information they are collecting by checking on the quality of information they are generating [8].

The reporting and reconfiguration aspects of the sensor networks remain the same as in communication networks, except that they should be performed using mechanisms that will work in sensor networks.

Looking at the functional aspects of FCAPS, the main impact in the sensor networks comes in determining the fault and capacity information from management information that cannot be observed directly, but needs to be inferred by indirect extrapolation from information generated by the sensors. In particular, the following aspects need to be considered in managing sensor networks.

Fault Management: Since fault information is often inferred indirectly [9], the analysis and corrective actions need to be tentative. Therefore, instead of determining one potential correction action for the fault management, sensor management systems need to have a slate of corrective actions that can be investigated and appropriate ones applied when there is a connectivity problem to the actual sensor.

Configuration Management: In the context of sensor network, configuration management consists of managing software updates, and the network configuration of different sensors in the field. It includes schemes for checking that the configuration has not been tampered with, and for updating software over the air in the field.

Accounting Management: comprises of periodically validating that the sensors are deployed in the configurations that they were intended to, and are generating information as intended.

Performance Management: consists of tracking the quality of information obtained from the sensors, and diagnosing the appropriate causes when the quality falls below desired thresholds. This also includes tracking the battery lifetime remaining and taking corrective steps when battery life is about to run out.

Security Management: consists of commissioning sensors so that they cannot be readily tempered with, detecting any security vulnerabilities and putting in mechanisms for fixing them.

Thus, a holistic management of sensor network management requires a solution very different from that of a traditional communication network, yet performs the same higher layer of functions.

7. Conclusions

In this paper, we have presented a model for managing sensor networks for coalition operations. We have taken the FCAPS paradigm of network management and shown how it needs to be modified in order to provide for the special conditions under which sensor networks operate and run.

8. Acknowledgement

This research was sponsored by the US Army Research Laboratory and the UK Ministry of Defence and was accomplished under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the author(s) and should not be interpreted as representing the official policies, either expressed or implied, of the US Army Research Laboratory, the US Government, the UK Ministry of Defence or the UK Government. The US and UK Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon. This paper includes British Crown copyright material.

9. References

1. K. Liu et. al, A dual space approach to tracking and sensor management in wireless sensor networks, Proc. 1st ACM International Workshop on Wireless Sensor Networks and Applications, Atlanta, GA, pp. 131-139, 2002.
2. C. Shurgers et. al, Topology Management for Sensor Networks: Exploiting ltency and Density, Proc. of 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2003.
3. LB Ruiz, JM Nogueira, AAF Loureiro, Manna: A management architecture for wireless sensor networks, IEEE Communications Magazine, 2003
4. H. Song et. al. UPnP based Sensor Network Management Architecture, Proc. Second International Conference on Mobile Computing and Ubiquitous Networking, Osaka, Japan, 2005.
5. M. Younis, M. Youseff and K. Arisha, Energy Aware Management for cluster based sensor networks, Elsevier Computer Networks, December 2003.
6. G. Tolle and D. Culler, Design of an Application-Cooperative Management System for Wireless Sensor Networks, Proc. Second IEEE Workshop on Wireless Sensor Networks, 2005.
7. D. Verma, Principles of Computer Systems and Networks Management, Springer Verlag, 2009
8. C. Bisdikian et. al, Quality of Information in Snesor Networks, Proceedings of First Annual Conference of the ITA, Washington, DC, 2007.
9. S. Ganeriwal, A. Kansal and M. Srivastava, Self-aware actuation for fault repair in sensor networks, In Proceedings of the IEEE International Conference on Robotics and Automation(ICRA), May 2004
10. D. Verma et. al., An end to end life cycle for ISR in coalition networks, Proceedings of Information Fusion 2009.