

A FRAMEWORK FOR NET-CENTRIC SERVICES AND USAGE PATTERNS IN MILITARY NETWORKS

Jerome Sonnenberg, Sastri Kota, Harris Corporation
Allen Jones, The Boeing Company

Abstract: The Network Centric Operations Industry Consortium (NCOIC) provides guidance for Network Centric Operations (NCO) interoperable systems. The NCO Interoperability Framework (NIF) [1] provides an organizational construct and repository for enabling this guidance. NIF is a framework that assists industry to design interoperable systems. NIF is based upon standards, including patterns, principles, and processes. The Net-Centric Services Framework [2] is contained in the NIF overarching framework, consistent with the NIF structure requirements: Concepts, Principles, Patterns and Processes.

Key net-centric patterns exist in all network designs and implementations. This paper discusses the Net-Centric Services Framework and describes two important network patterns of particular interest in military networks: DIL (Disconnected, Intermittent, Limited capacity) Communications Service and Isolated Network Join with Synchronization (INJS) Service.

The DIL Communication Service pattern describes how a network of connected links with variable link capacity operates to maintain QoS and situational awareness. The Pattern describes supporting features required at several protocol layers.

The INJS Service pattern describes how a set of mobile nodes that have been truncated from the reach-back capabilities of the main mesh re-join the main tactical mesh network and synchronize their operations and situational awareness view of the overall tactical network. The abstraction of these patterns using the NIF process provides a standards-based artifact that can be used in both development and procurement of military network capabilities.

I. Introduction

A major interoperability problem in the deployment of heterogeneous networks is the coordination of the capacity allocation algorithms associated with, or embedded in, the control of each type of network

device. Capacity allocation is an essential underpinning for the proper operation of network-centric services.

In the wired Internet, capacity allocation is often managed by a single management solution since the underlying technology is nominally homogeneous. For example, the OSPF [3] or EIGRP [4] routing protocols can determine an optimal mesh of land line links that may range across moderate (1.5 Mbps), high (100 Mbps- 1Gbps) and very high (10 Gbps) rates. This mesh will typically include many redundant links that can quickly be employed to support net-centric services by invoking capacity management protocols at the link layer (e.g., Spanning Tree Protocol – IEEE Standard 802.1D) or at the network layer (e.g., OSPF – Open Shortest Path First – IETF RFC 2328).

In tactical wireless environments, the luxury of link over-provisioning typically does not exist. There are both technical and strategic reasons for limiting the number of links. The wireless links themselves are subject to environmental (atmospheric, foliage, jamming) effects that are not as prevalent in the wired Internet.

So these links can become disconnected (when Radio Frequency (RF) or Free Space Optical (FSO) transmission is blocked), intermittent (when connections wax and wane) or limited (when the physical modulation order in the waveform changes to maintain connection in poor conditions, but at a lower bit rate).

Capacity allocation for military UHF satellite communications paths is typically implemented with DAMA [5] (Demand-Assigned Multiple Access) and its variants. A DAMA network allows multiple simultaneous users to employ a single 25 KHz channel with a time division multiple access format. More detail can be found in Kota [6]. Terrestrial Line-Of-Sight (LOS) wireless links have a number of link layer (Media-Access-Control (MAC)) or network layer algorithms that can be used for capacity management [7]. It is imperative that the capacity allocation for all

the wired and wireless components in a services-based network be performed according to the same technical pattern. In this way, the constituent element management algorithms will work in cohesion and not inadvertently cancel or contradict each other.

This paper is structured as follows: Section I completes an introduction, Section II describes Operational, Capability and Technical Pattern features, Section III describes the DIL Technical Pattern, Section IV describes the INJS Technical Pattern, Section V provides conclusions to this pattern analysis, and Section VI describes future work plans.

A. Problem Statement and Context

Most networks need to continue to provide the data transfer capacity that supports network services even when disruptions cause a significant drop in the aggregate data throughput of the network. Rather than just terminating an arbitrary number of SLAs, a robust network implementation should attempt to determine the criticality of supported services and provide a degraded level of service that still transfers the mission-critical data.

Both wireline and wireless network links can become disconnected for a variety of reasons. A wireline link can be cut by accident or by malicious intruders. Hackers can cause wireline and wireless links to lose capacity. Wireless links can be affected by the physical environment (atmosphere, rain fade, movement under a canopy of foliage, just to name a few). Tactical wireless links can be shut down by policy when they otherwise would radiate in a zone that a commander wishes to be emission silent. Such links can be intermittent when the intervening physics causes variations in signal strength.

Dynamically adaptable radios can often change modulation order at the physical layer to provide limited data capacity even in poor operating environments.

The Net-Centric Services Framework has identified service-orientation principles that foster creation of automation logic in the form of services. The service-oriented common design principles can be used to characterize services for military tactical networks.

II. Operational, Capability and Technical

Patterns

The NCOIC Lexicon states: “A Net-Centric Pattern (NCP) provides expert guidance based on standards for creating systems with desired Net-Centric capabilities in order to mitigate specific Net-Centric interoperability problems.” Patterns are:

- Prescriptive guidelines for practical use by designers and implementers that can be tailored and re-used for solving interoperability problems
- Sufficiently detailed to facilitate verification of vendor evidence of conformance to the pattern
- Guidance for Hardware, Software, Processes, and Procedures (*more* than just traditional software patterns).

There are three categories of Patterns:

Operational: Describes standard practices and their interoperability requirements needed to conduct activities (military operations or business objectives) in a given mission context

Capability: Describes the standard methodologies and functions needed to support required activities in a mission context from an interoperability perspective as specified in Operational Pattern(s)

Technical: Describes the technical standards, technologies, and interoperability techniques needed to support required capabilities in a functional context specified in Capability Pattern(s)

III. DIL Technical Pattern

This technical pattern addresses the sequence of actions that takes place in many network environments when DIL links are used. Often these actions are manual. The goal is to capture these sequences of actions into patterns for codification and reuse and the reported link capacity metrics to the routing engine.

During the course of operations, communications nodes play many roles. Once an Operational or a Capability Pattern has progressed to a state of operations that includes mission critical communications and processing, some of the communications nodes supporting the network-centric operations become critical.

When asynchronous network events cause the capacity of a link in the mesh to be diminished,

the events are forwarded to the policy based bandwidth manager. The policy manager determines which nodes are essential to continued mission-critical operations. It is important to note that the policy logic and associated actions can be automatic, protocol-based, computer communications actions or they can be (and currently typically are) human-based and distributed over a geographical range of meshed nodes. In some cases, capacity allocation “logic” consists of parameter tables set up in each of the associating nodes (routers, satellite access terminals, or general-purpose processors used with communications equipment that has a specific rule set installed for capacity allocation).

Once the critical nodes are identified, analysis is performed to see which critical services can be maintained. As mentioned above, robust network implementations should attempt to determine the criticality of supported services and provide a degraded level of service that still transfers the mission-critical data.

This activity is summarized in the SysML Activity Diagram of Figure 1.

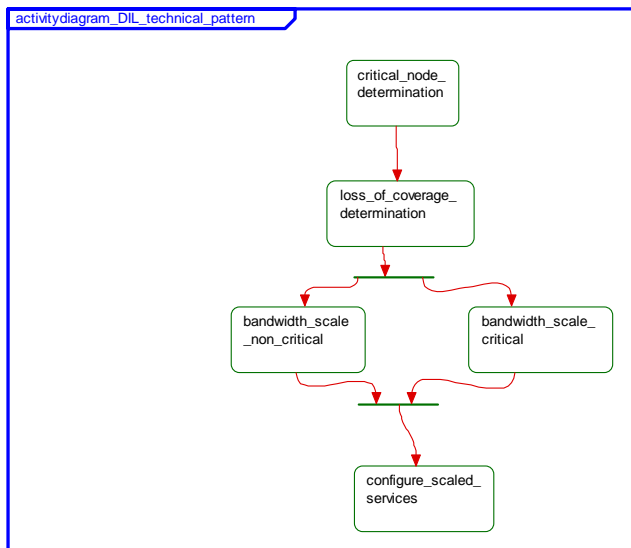


Figure 1: DIL Technical Pattern Activity Diagram

Figure 2 is a SysML Block Definition Diagram that illustrates the participants in the Call For Fire Capability Pattern and the DIL Communications Technical Pattern. The example Call For Fire Use Case illustrates a sample user set for the DIL Technical Communications Pattern.

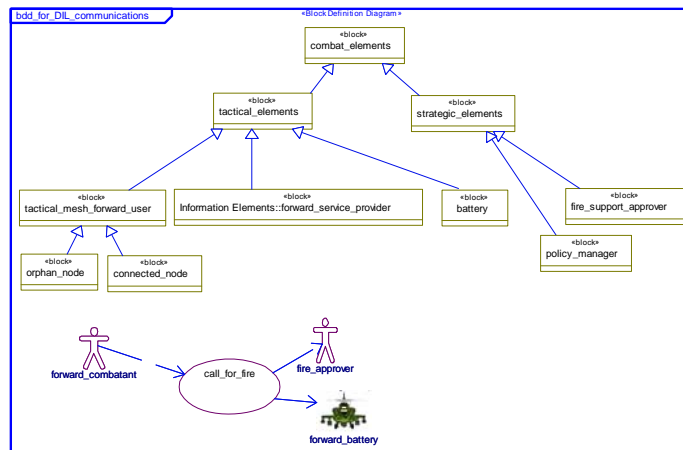


Figure 2: DIL and CFF Patterns

The primary participants of the DIL Technical Pattern are:

- The tactical mesh member communications nodes experiencing DIL communications
- The policy based bandwidth manager
- Tactical mesh communications nodes placed in a critical path by operational events
- Tactical mesh members maintaining membership in the tactical mesh (providing capacity to and from the mesh and the policy based bandwidth manager)

The sequence of communications among these members is illustrated in Figure 3.

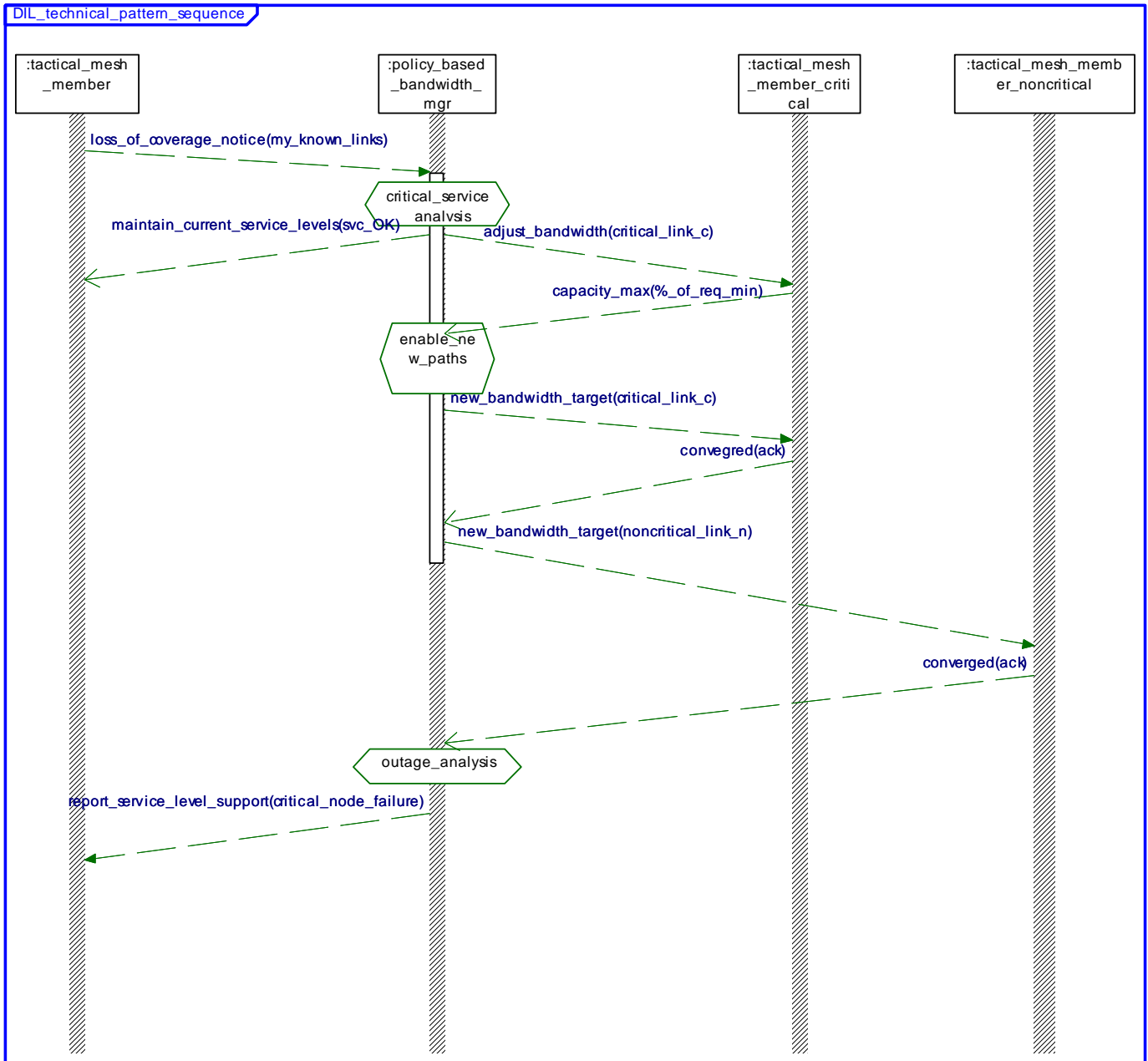


Figure 3: DIL Communications Sequence Diagram

Each flow in Figure 3 is a stereotype of the many flows between the policy manager and the communications mesh nodes (critical and non-critical). In the case where the incoming event(s) do not lower the mesh capacity below the critically-needed threshold, the node raising the event is responded to with a message to maintain current service levels.

The set of critical links (c_i) are informed of new bandwidth requirements by the policy manager and

each responds with the percentage amount of that capacity that can be supported. The policy manager determines if new paths are required and invokes the physical, link and network layer protocols to create a new mesh that will support mission critical operations. In instances where the mission criticality can be measured in seconds rather than minutes, it is incumbent that the analysis and enabling logic be computer-based.

The set of non-critical links (n_j) are informed of their new capacity assignments. For example, should a MAC-layer protocol divide capacity via TDMA or

FDMA techniques, and the assignment of timeslots or frequencies can be done dynamically, then the non-critical nodes can be set to use less total capacity if such capacity can be given to the now-critical links.

Both critical and non-critical nodes report the re-convergence of the network. Convergence has a specific meaning in the layer 3 network protocols common in the Internet. However, in this context, the convergence acknowledgement is the superset of all the mesh node responses that tell the network manager (central or distributed, human or computer) that the mesh of links supporting DIL Communications has settled to a new state (before the next event).

IV. INJS Technical Pattern

Figure 4 illustrates the activity associated with the INJS technical pattern, which is defined in more detail in the sequence diagram of Figure 5.

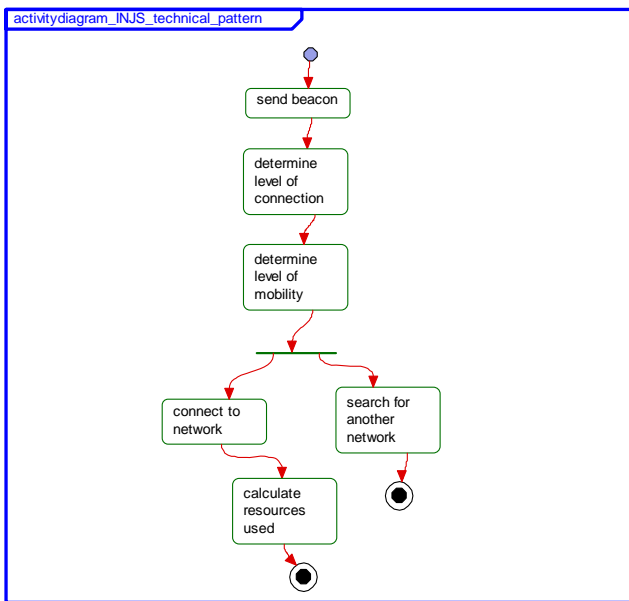


Figure 4: INJS activity diagram

An orphan node sends out a beacon message to locate a compatible network-connected node. In a tactical environment, there are more metrics involved in deciding whether or not a node can join a network than just waveform compatibility. The first node found by an orphan may have poor neighbor connectivity, i.e., it may be several links away from a desired gateway. Additionally, the target network mobility may be such that the orphan may not remain connected for a long time.

Once connected, the former orphan and the collection of nodes that make up the new tactical mesh network must calculate how the communications resources (frequencies, timeslots, codes) are allocated.

Figure 5 is the sequence diagram for the INJS technical pattern.

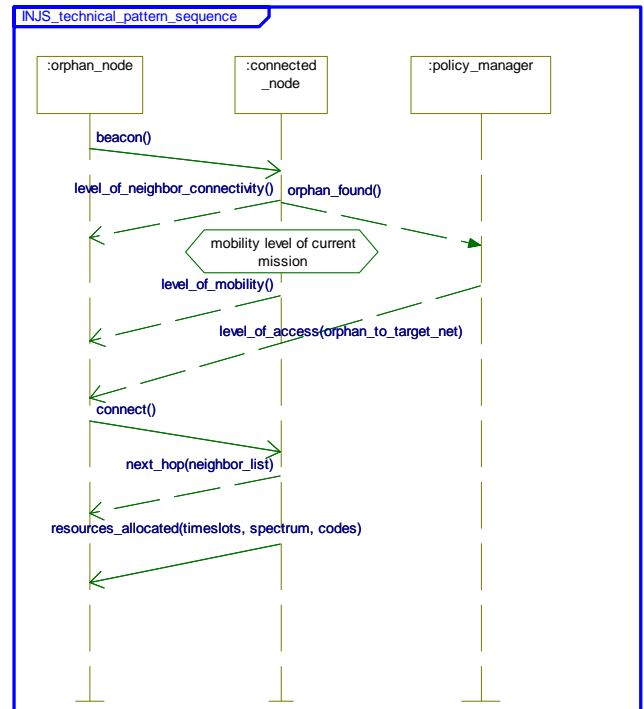


Figure 5: INJS Technical Pattern Sequence Diagram

The primary participants are shown in the Block Definition Diagram of Figure 2 as:

- An orphan node that has lost communications with all compatible RF or FSO neighbors
- A connected node that is part of a tactical network
- The policy manager that contains the logic used in the Area of Operations to allow or disallow connection of nodes to an operational network, based on mission needs

Both the orphan and the connected nodes use policies to determine if a connection should be made once a beacon is seen between them. It is important to note that these policies can be hard-coded, hand-configured at initialization, or dynamically managed by a centralized or distributed policy management entity.

In order for a connected node to receive the orphan’s beacon it must have waveform compatibility and encryption (key) compatibility. The connected node

also informs the policy manager of the identity of the found orphan. At this point, three pieces of information are returned to the orphan:

- Level of neighbor connectivity
- Level of mobility
- Level of access

The orphan's internal policy (configuration) settings may dictate that it seek better (or just different) neighbor connectivity. The connected node is part of an operational mesh network that has a current assigned mission. This mission may involve a level of mobility that is incompatible with the policy goals of the orphan. The policy manager is aware of any mission needs that would preclude the orphan from joining the target network. For example, the target network may be a Special Operations network and while the orphan is physically and logically compatible with the target network, the Area of Operations policy management logic does not want it to use any of the communications resources (timeslots, frequencies, codes) that are planned for the Special operations task.

V. Conclusions

Network-centric operations are replete in every aspect of current military operations. Within the deployed networks, patterns have emerged to establish, configure and utilize network capacity. Most importantly, patterns are evolving for the use of Disconnected, Intermittent and Limited (DIL) Communications Services. It is important that the pattern for using DIL Communications Services be consistent across heterogeneous components of a deployed network.

With mobile networks gaining ground in the deployed arena, it is also important that pattern for network joining by an isolated node be consistent. The INJS Technical Pattern documents the guidance for creating a network join service.

VI. Future Work

The NCOIC Working Groups are continuing to refine the NIF as well as Specialized Frameworks such as the Network-Centric Services Framework. The next step in following the NCOIC development path is to define and validate conformance criteria for Network-Centric patterns such as DIL and INJS. Completion of

conformance criteria will allow procurers to state requirements as a function of technical Patterns and will allow providers to test their network products against these conformance criteria. Our work will continue within the NCOIC and will be reported at www.ncoic.org.

References

- [1] NCOIC Interoperability Framework (NIF™)
<https://www.ncoic.org/technology/deliverables/nif/>
- [2] Net-Centric Services Framework
https://www.ncoic.org/apps/group_public/document.php?document_id=11351
- [3] Open Shortest Path First <http://www.ietf.org/rfc/rfc2328.txt>
- [4] Enhanced Interior Gateway Routing Protocol
<http://en.wikipedia.org/wiki/EIGRP>:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f07.shtml
- [5] Interoperability Standard for UHF SATCOM DAMA Orderwire Messages and Protocols
http://assistdocs.com/search/document_details.cfm?ident_number=107857&StartRow=1&PaginatorPageNumber=1&title=UHF&status%5Fall=ON&search%5Fmethod=BASIC
- [6] Sastri Kota, Kaveh Pahlavan, Pentti Leppanen, *Broadband Satellite Communications for Internet Access* 2004, Kluwer Academic Publishers, Chapter 16
- [7] J. Bibb Cain, Tom Billhartz, Larry Foore, Edwin Althouse, John Schlorff; "A link scheduling and ad hoc networking approach using directional antennas", Proc. IEEE MILCOM, 2003, pp. 643 - 648, October 2003.