QoS Architecture for Tactical Networks

노 병 희
(bhroh@ajou.ac.kr)

 아주대학교 정보통신전문대학원/정보및컴퓨터공학부
모바일 멀티미디어 통신 네트워크 연구실 (http://mmcn.ajou.ac.kr)
 아주대학교 국방전술네트워크 연구센터 (http://tnrc.ajou.ac.kr)
Contents

- NCW (Network-Centric Warfare) Overview
- Challenges on Precedence and Preemption
- Policy-driven Tactical Network Management
- Survivability of Tactical Networks
- Conclusion
NCW Overview

- Challenges on Precedence and Preemption
- Policy-driven Tactical Network Management
- Survivability of Tactical Networks
- Conclusion
NCW (Network Centric Warfare)

- by VADM Arthur Cebrowski, 1997
  - Information and Intelligence architecture built around sensors, information, and engagement grids that would enable new operational concepts of speed of command and self-synchronization

- NCW is
  - more about networking than networks
  - about the increased combat power that can be generated by a network-centric force

[Diagram showing Warfighting Effects with Network-Centric and Platform-Centric approaches and Forces Applied]
Why Networking?

- The tenets of NCW (DoD NCW report to the Congress)
  - A robustly networked force improves information sharing;
  - Information sharing enhances the quality of information and shared situational awareness;
  - Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command.
  - These, in turn, dramatically increase mission effectiveness.

Source: DoD, The Implementation of Network-Centric Warfare, 2007
NCW Vision: Information Anywhere, Anytime

Decision & Information Superiority resulting in more timely, relevant, and accurate effects - Requires full connectivity between network components
NCW Overview

Challenges on Precedence and Preemption

- Policy-driven Tactical Network Management
- Survivability of Tactical Networks
- Conclusion
GI G (Global Information Grid)

The (globally interconnected) Network of Networks

INTEGRATED INFORMATION INFRASTRUCTURE
- Information Services and transport
- Service Agents
- Intelligent, integrated communication intranetwork
- Adaptive, dynamic resource management
- Secure

NAVIGATION GEO-POSITIONING
- Robust
- Distributed
- Inexpensive

LOGISTICS SUPPORT
- Just Enough
- Just In Time
- Fully Visible

INFORMATION OPERATIONS
- Defensive IW
- Offensive IW
- Assurance

SURVEILLANCE
- Continuous
- Global
- High Resolution Imagery
- Day/Night/All Weather

WEAPONS
- Remote/Local
- Accurate
- Responsive
- Inexpensive

FORCE ENHANCEMENT
- Mobile
- Lethal
- Sustainable
- Flexible

COMMAND AND CONTROL
- Commanders Internet
- Situation Monitoring
- Planning and Replanning
Where Tactical Networks in GIG?

DISN: Defense Information Systems Network
TSAT: Transformational Communications Satellite
ADNS: Automated Digital Network System
USMC: United States Marine Corps
TDN: Tactical Data Network
WIN-T: Warfighter Information Network-Tactical
UE: Unit of Employment
UA: Unit of Action
TDC: Theater Deployable Communications

Tactical Networks are small parts of GIG

GIG Transport Network Architecture

- Tier 4 Global Coverage
- Tier 3 Wide Area Coverage
- Tier 2 Inter-Team Coverage
- Tier 1 Team Coverage

R = Internet Router or JTRS WNW

- GEOS
- LEOS
- Aircraft
- AAVs
- TCS

Ground Based

JTRS JAN-TE

JTRS SRW

GIG-BE

People Weapons Sensors

Land Line (wire or fiber)

Radio
Tactical Networks

- WIN-T (Warfighter Information Network-Tactical)
**Tactical Networks**

- **TICN (Tactical Information Communication Network)**
  - HCTR: High Capacity Trunk Radio
  - MSAP: Mobile Subscriber Access Point
  - TMFT: Tactical Multi-Function Terminal
  - TMMR: Tactical Multiband Multirole Radio
Importance of QoS Guarantee in TNs

GI G defines that

"Providing end-to-end QoS guarantees in tactical networks is essential for successful deployment of GI G, a mission critical communications networks".

GI G QoS Architecture


- DISA (Defense Information Systems Agency) is in charge of GI G QoS WG
Importance of QoS Guarantee in TNs

GIG QoS Architecture (Multi-Plane Framework)

- Service Control Layer
- QoS Service & Network Management
- Management Plane
- Control Plane
- Data Plane

Precedence & Preemption

- Two main QoS requirements for tactical networks
  - to meet or exceed the requirements for networked applications with distinct class of services (precedence)
  - to deliver temporarily mission-critical data with the highest priority (preemption)
Precedence & Preemption

- Why existing commercial QoS schemes are not good for tactical networks?
  - Commercial QoS Schemes
    - Performance-based QoS Assured Service
    - To guarantee throughput, delay, jitter for specific applications
    - Static (not chaned) precedence during session
  - For military application
    - the degree of importances of individual messages even in same application may different
      (varying precedence during session)
    - military precedence depends on the degree of priority and timeliness of individual mission critical messages
### PBAS (Precedence-based Assured Service)

#### MLPP (Multi-Level Precedence and Preemption)
- PBAS applied for voice networks in US Army
- 5 priorities: ROUTINE - PRIORITY - IMMEDIATE - FLASH - FLASH OVERRIDE

<table>
<thead>
<tr>
<th>Levels</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROUTINE</td>
<td>- 우선적인 핸들링을 요구하지는 않지만 전화수단에 의해 빠른 전송이 요구되는 공식적인 미군정부 통신에 적용되는 것</td>
</tr>
<tr>
<td>PRIORITY</td>
<td>- 필수적인 정보를 제공하기 위해 전화 콜을 위한 Precedence</td>
</tr>
<tr>
<td>IMMEDIATE</td>
<td>- 국가보안에 영향을 주는 상황</td>
</tr>
<tr>
<td>FLASH OVERRIDE</td>
<td>- 방어와 공격에 필수적인 군 C2 (Command &amp; Control)</td>
</tr>
<tr>
<td>FLASH OVERRIDE</td>
<td>- 미 대통령, 국방장관, 합참의장</td>
</tr>
<tr>
<td></td>
<td>- defence가 선언된 상황에서 전투지휘관</td>
</tr>
<tr>
<td></td>
<td>- FLASH OVERRIDE는 다른 PL등에 의해 선점(Preemption)되지 않음</td>
</tr>
</tbody>
</table>
PBAS in IP-based Tactical Networks

- MLPP is suitable for Telephone Networks
  - Telephone line is dedicated to two communicating entities
  - P&P Level can be assigned based on persons (or phone lines)

- MLPP in IP-based Networks?
  - It is still question in GIG domain
    - since IP provides flat network, and is based on datagram.
  - But, GIG thinks PBAS is required even in IP-based networks
    - GIG-BE transition plan
PBAS in IP-based Tactical Networks

- DiffServ with a signaling protocol (e.g. RSVP)
  - a candidate solution to support PBAS in IP-based tactical networks
    - Precedence for sessions by DiffServ
    - Preemption for individual critical message (or session) by Signaling

- Five common QoS architecture alternatives
  - DiffServ (Differentiated Services)
  - RT-ECN (Real-Time Explicit Congestion Notification)
  - BB (Bandwidth-Broker)
  - RSVP (Resource Reservation Protocol)
  - ARSVP (Aggregated RSVP)

- Another QoS architecture by GIG NCID QoS
  - measurement-based network admission control
    - similar (or identical) to BB architecture
PBAS in IP-based Tactical Networks

- **DSCP assignment by DoD**

<table>
<thead>
<tr>
<th>Service</th>
<th>Traffic class</th>
<th>DSCP assignment</th>
<th>Decimal values DSCP</th>
<th>Example of applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous Bit Rate</td>
<td>EF</td>
<td>101111, 101110, 101101, 101011, 101001, 101000</td>
<td>47, 46, 45, 43, 41, 40</td>
<td>Interactive voice</td>
</tr>
<tr>
<td>(CBR)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Variable Bit Rate</td>
<td>AF41</td>
<td>100010</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>(VBR)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multimedia</td>
<td>AF42</td>
<td>100100</td>
<td>36</td>
<td>Interactive video</td>
</tr>
<tr>
<td></td>
<td>AF43</td>
<td>100110, 100000</td>
<td>38, 32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AF31</td>
<td>011010</td>
<td>26</td>
<td>Streaming</td>
</tr>
<tr>
<td></td>
<td>AF32</td>
<td>011100</td>
<td>28</td>
<td>multimedia and</td>
</tr>
<tr>
<td></td>
<td>AF33</td>
<td>011110</td>
<td>30</td>
<td>multicast</td>
</tr>
<tr>
<td>Mission Critical</td>
<td>AF21</td>
<td>010010</td>
<td>18</td>
<td>Short blocks of interactive data</td>
</tr>
<tr>
<td></td>
<td>AF22</td>
<td>010100</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AF23</td>
<td>010110</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AF11</td>
<td>001010</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AF12</td>
<td>001100</td>
<td>12</td>
<td>Long blocks of bulk data</td>
</tr>
<tr>
<td></td>
<td>AF13</td>
<td>001110</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>Best effort</td>
<td>Default</td>
<td>000000, 001000, 010000, 011000</td>
<td>0, 8, 16, 24</td>
<td>Everything else</td>
</tr>
<tr>
<td>Control and Management</td>
<td>CS7</td>
<td>111000</td>
<td>56</td>
<td>Network Control</td>
</tr>
<tr>
<td>Control and Management</td>
<td>CS6</td>
<td>110000</td>
<td>48</td>
<td>Intermeshet Control</td>
</tr>
</tbody>
</table>
PBAS in IP-based Tactical Networks

- Queueing Architecture for QoS and P&P Support

Diagram:
- Signaling
- Classifier
- PE1
- PE2
- EF
- AF
- BE
- Normal DiffServ Queues
- Preemption Queues
- Scheduler
- SLA

Signaling for preemption control
Preemption for precedence control
Normal DiffServ for precedence control
End-to-end PBAS in IP-based TNs

- End-to-end PBAS Guarantee by BB (Bandwidth Broker)
End-to-end PBAS in IP-based TNs

- Multi-domain Support
  - SLA/SLS Issues by TACOM POST 2000
    - SLA example between heterogeneous TNs
  - SLS management

- NCW Overview
- Challenges on Precedence and Preemption
- **Policy-driven Tactical Network Management**
- Survivability of Tactical Networks
- Conclusion
Policy-based Network Management

- Current state of the art in IP Management

Policy-based Network Management

- Policy-based IP Management
  - Policies are used to tie together the operations of the network management components

Policies automate network reconfiguration based on network status
Policy-based Network Management

- **Comparisons**
  - **Current IP Network Management**
    - Choice of network configuration made statically, without taking into account network dynamics
    - User manually reconfigures network in response to monitored network status
    - No attempt is made to re-visit configuration choices based on changing network conditions
  - **Policy-based Management**
    - Choice of network configuration made based on policies
    - Policies can be changed by network planners
    - **Automated management based on changing network conditions**
Policy-based Network Management

- Coupling of FCAPS and Policy Management Functions

FCAPS: Fault, Configuration, Accounting, Performance, and Security
Example: FCS NMS

- FCS (Future Combat System) NMS
  - Integrates multiple management subsystems
  - UA Network managed by FCS NMS
    - 500 vehicle based platforms and 2500 soldier nodes
      → distributed multi-tier management architecture for scalability and survivability

- Full Spectrum of Management Capabilities
- Adaptive and Automated Management
- Distributed architecture for scalability and survivability
- Network Communication Services
- Operated by Brigade Intelligence and Communications (BIC) Company
Multi-tier Management Architecture (1/2)

- Same NMS software in every node
  - MoM, NM, and PM are NMS roles with different management scope
  - Roles initially planned and dynamically adjusted

Policy dissemination to subordinates

Summarized information to superior

Manager of Managers
Network Manager
Platform Manager
Example: FCS NMS

- Multi-tier Management Architecture (2/2)
  - Soldier Network Management by FCS NMS at Bottom Level

- Soldier Network Management by FCS NMS at Bottom Level

FCS NMS derives topology for SRW network using routing protocols

FCS MGV Platform is gateway node for Soldier Network
  - Provides range extension
  - Provides connectivity to WNW backbone for reach back

For local SRW elements
Platform Manager collects:
  - Performance statistics,
  - Fault alarms,
  - IA alerts

MGV: Manned Ground Vehicle
SRW: Soldier Radio Waveform
Example: FCS NMS

FCS NMS: Functional Components

Planning input from Higher Echelons and Mission Planning

QoS Control

Naming Service

Mobility Management

Session Management

Policy Mgmt

Spectrum Mgmt

Configuration Mgmt

Network Planning

Policy change

Configuration Directives

Network resource policies

Policy creation

Correlated events

Integrated Event Correlation

Performance Monitoring

- Perf. data collection
- Reporting
- Threshold monitoring

Fault Monitoring

- Fault processing
- Fault correlation
- Fault isolation

IA Correlation Engine (SoS COE)

Correlated events

Event Logging

Correlated events

Failure alerts

Security alerts

Network Elements

Agents

Net Mgmt Apps

Net Comm Apps

SoS COE

Net Sensors

IDS

Radio element configuration

IP network configuration

IA element configuration

Network services configuration

Reconfiguration

Perf. alerts

Performance Monitoring

Correlated events
Example: FCS NMS

- QoS Planning and Configuration Flow (1/3)
Example: FCS NMS

QoS Planning and Configuration Flow (2/3)

1. The mission planner in conjunction with C2 planning function supplies network planning input to the Network Planning component in MoM.

2. Based on this input, Network Planning generates network QoS policies and stores them in the local copy of NMS Database. The following types of policies are generated: DiffServ class and priority assignment for different types of FCS applications; link bandwidth limits for different DiffServ classes; and event rules that prescribe what management actions are to be invoked upon different types of network events.

3. Policy Management in MoM retrieves these policies and identifies the management actions to be invoked.

4. Policy Management in MoM invokes Configuration Management to trigger policy configuration in the network.

5. Configuration Management in MoM retrieves these policies and translates the policies to QoS configuration parameters. For example, queuing policies are translated to queuing parameters (queue length, dispatch policy), and DiffServ class assignment policies are translated into traffic classification policies based on IP header information.

6. Configuration Management in MoM configures the QoS parameters in the radio in the local platform. Note that this configuration involves access to both Red and Black parts of the radio.

7. The QoS policy information stored in the NMS Database in the FCS platform hosting the MoM is disseminated to all platforms in Subnet2 and to the platform in Subnet1 that hosts the NM. This data dissemination occurs via the SoS COE Data Store service.

8. Policy Management in NM retrieves these policies and identifies the management actions to be invoked.
Example: FCS NMS

QoS Planning and Configuration Flow (3/3)

9. Policy Management in NM invokes Configuration Management to trigger policy configuration in the network.
10. Configuration Management in NM retrieves these policies and translates the policies to QoS configuration parameters.
11. Configuration Management in NM configures the QoS parameters in the radio in the local platform.
12. The QoS policy information stored in the NMS Database in the FCS platform hosting the NM is disseminated to PMs in each platform in Subnet1. Steps 13-16 are executed by each PM in Subnet1 and Subnet2.
13. Policy Management in PM retrieves policies and identifies the management actions to be invoked.
14. Policy Management in PM invokes Configuration Management to trigger policy configuration in the network.
15. Configuration Management in PM retrieves policies and translates the policies to QoS configuration parameters.
16. Configuration Management in PM configures the QoS parameters in the radio in the local platform.
Example: FCS NMS

Performance Monitoring and QoS Policy Adaptation Flow

1. Alerts from radios: “Throughput for AF1 too high”
2. PMs propagate alerts to NM
3. NM determines AF1 traffic is reaching the BW limit in the subnet
4. NM allocates more BW for AF1
5. NM records the policy change
6. The policy change disseminated to PMs
7. PMs detect the policy change
8. Affected NMS applns are notified of the policy change
9. Radios in all platforms in the subnet are reconfigured
- NCW Overview
- Challenges on Precedence and Preemption
- Policy-driven Tactical Network Management
- **Survivability of Tactical Networks**
- Conclusion
Survivability

- Due to the dynamic and unreliable nature of tactical network,
  - it is critical that the tactical network be survivable by itself
  - it should be able to handle random disconnections, mobility, high link loss rates, and so on.

- Definitions of Survivability
  - Several definitions exist.
  - Possible definition of survivability
    - the ability to maintain communication among nodes, i.e. the probability of node pairs which still have one path at least, when the network being attacked by the enemy
  - Considering Points
    - "Connectivity"
    - "Traffic Capacity"
    - "The degree of Self-Healing"
Example of Survivability Measures

- PSTN Survivability Model (Example)

\[ \pi_j^P = \frac{\left(\frac{\lambda}{\mu}\right)^j / j!}{\sum_{k=0}^{n} \left(\frac{\lambda}{\mu}\right)^k / k!} \]

\[ \pi_i^A = \frac{\left(\frac{\tau}{\gamma}\right)^i / i!}{\sum_{k=0}^{n} \left(\frac{\tau}{\gamma}\right)^k / k!} \]

\[ P_{b_k}' = \sum_{k=0}^{n} \pi_{k, k}^C \]

where \( \pi_{k, k}^C \) is the steady state probability of state \((k, k)\)
Example of Survivability Measures

Tactical Network Survivability Measure (1/3)

- **Survivability Measure**

\[ SM(G) = \sum_{k=0}^{m-1} CM(k) \]

The number of nodes in a given MCN \( G \) is \( n \)

\( CM(k) \) is Connectivity Measure of \( G_k \) which is made by removing the most important node from \( G_{k-1} \)

- **Connectivity Measure**

\[ CM(k) = \sum_{i=1}^{n-k-1} \sum_{j=i+1}^{n-k} NC_k(i,j) \]

- **Node Connectivity**

\[ NC_k(i,j) = \sum_{t=1}^{x} \frac{1}{JN(t)} \]

- \( x \) is the number of independent path
- \( JN(t) \) is the number of jumps along \( t \)-th independent path between \( i \) and \( j \)

Example of Survivability Measures

Tactical Network Survivability Measure (2/3)

CM(0) = \( \sum \sum NC_0(i,j) = 9.67 \)

Node 4 is the most important node in G0

CM(1) = \( \sum \sum NC_1(i,j) = 2.5 \)

Node 2 is the most important node in G1

CM(2) = 0

SM = CM(0) + CM(1) = 9.67 + 2.5 = 12.17
Example of Survivability Measures

- Tactical Network Survivability Measure (3/3)

The image shows four different network diagrams, each with a survivability measure (SM) indicated:

1. SM = 63.75
2. SM = 79.75
3. SM = 81.83
Survivability Management

- Survivability Management Steps:
  - for a given topology, find critical nodes
  - assign alternate path at the nodes that have paths through the critical nodes
    - those alternate path assignment is done through policy management and QoS monitoring
Survivability Management

- Failure Recovery Scenarios

Before Failure:
- Source 2
- Node 2
- Node 3 (cluster head)
- Destination 2
- Destination 2'
- Source 1
- Node 1
- Destination 1

After Failure:
- Source 2
- Node 2
- Node 3 (cluster head)
- Destination 2'
- Source 1
- Node 1
- Destination 2
- Destination 1

Before Failure:
- Source 2
- Node 2
- Node 3 (cluster head)
- Destination 2'
- Source 1
- Node 1
- Destination 2
- Destination 1

After Failure:
- Source 2
- Node 2
- Node 3 (cluster head)
- Destination 2'
- Source 1
- Node 1
- Destination 2
- Destination 1
## Survivability Management

### Survivability Measure Examples

<table>
<thead>
<tr>
<th>Measure</th>
<th>Threshold Metric</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to detect change in network quality of service</td>
<td>less than a certain time (e.g. &lt; 10 sec)</td>
<td>NMS Dependent</td>
</tr>
<tr>
<td>Identification and implementation of alternative network paths</td>
<td>No loss of communications</td>
<td>Seamless Routing</td>
</tr>
<tr>
<td>Network Capacity</td>
<td>Total Data Throughput</td>
<td>Decrease, but Cont.</td>
</tr>
<tr>
<td>Message Completion Rate</td>
<td>Service Flow Dependent</td>
<td>QoS Met</td>
</tr>
<tr>
<td>Message Delay</td>
<td>Time to Recover</td>
<td>less than a certain time (e.g. &lt; 250 ms)</td>
</tr>
</tbody>
</table>
Survivability Management

- Policy-Driven Survivability Management Architecture

Diagram:
- Policies triggered based on root cause events
  - Root Cause Events
  - Monitoring and Correlation
  - Element Monitoring
  - Managed system/network element
- Policy Management
- Configuration
- Network reconfiguration actions triggered by policy
- Element Configuration
NCW Overview
Challenges on Precedence and Preemption
Policy-driven Tactical Network Management
Survivability of Tactical Networks

Conclusion
Conclusion

- We discussed on
  - NCW Overview
  - Precedence and Preemption Requirements
  - Policy-Driven Tatical Network Management
  - Survivability Issues

- Especially,
  - QoS guarantee with Network Management is considered as an essential factor for successfully deploying tactical networks
  - Most of solutions for them have been studied and derived from DoD

- For TICN,
  - Currently, connectivity has been mainly concerned on it.
  - it should have QoS and Network Management guidelines asap.
Thank You
For any query and more information, please contact bhroh@ajou.ac.kr