Protecting Tactical Service Oriented Architectures
-Gkioulous Vasileios
TACTICS consortium consists of 12 members and subcontractors, while the projects studies will:

- Propose the definition of a service-oriented architecture (SOA) compatible with the constraints of tactical radio networks.
- Suggest feasible ways of adapting services to the constraints of the tactical radio networks.
- Demonstrate the capacity of a Tactical Service Infrastructure to offer operational services in a real tactical environment.

(*TACTICal Service oriented architecture, Proposal for EDA ad hoc B Program)
The role of NTNU in TACTICS security

- Monitor and advice on security related aspects/requirements
- Secure cross-layer network capabilities
- Secure protocols and algorithms for robust distributed service storage, retrieval, and discovery
- Secure, efficient and robust overlay routing with the incorporation of cross-layer information
- Necessary enhancements for the optimised performance of routing and QoS mechanisms
- Investigation of protection goals and requirements for tactical SOA
- Robust and adaptable security policies for tactical SOA
- Lightweight and dynamic protection mechanisms
- Information filtering, classification and provenance assurance

(*TACTICAL Service oriented architecture – Partners Contributions, Proposal for EDA ad hoc B Program)
Investigation of protection goals and requirements for tactical SOA

Robust and adaptable security policies for tactical SOA

Lightweight and dynamic protection mechanisms

How can a security policy that is sufficiently expressive to allow the incorporation of discretionary access control equivalent to restricted access matrices and label-based mandatory access control, be formulated in such a way that the policy and its computations can be distributed across a set of nodes in a distributed system with intermittent connectivity, yet remain consistent?
Protecting tactical service oriented architectures

1-Which are the distinct characteristics of tactical networks?
2-Which are the distinct characteristics of SOA (Constraints, Requirements, Opportunities)

SECURITY (What exists? Is it enough? What is missing?)

How can we accommodate the requirements and constraints? (Dynamic adaptation.. Robustness.. Expressivity..)

Security policy distribution (How?)
- ANSASA

Security policy reconciliation (How?)
- ISC

Security & QoS interoperability (How?)
- MILCOM
• **Node limitations**
  • Transmission/Reception range
  • Input/Output limitations
  • Power consumption
  • Physical limitations
  • Environmental conditions
  • Interconnection capabilities
  • Computational capacity

• **Network limitations**
  • Transmission disruptions
    • Due to radio range, interference (e.g. packet collisions, multipath transmission, jamming), physical obstacles, active attacks (e.g. wormhole, black-hole, denial of service)
  • Mobility
    • Due to dynamic network configurations (Referring both to routing and IP/ID planning and management), coalition operations, service delivery handover, multinetwork affiliation.
  • Communication
    • Due to scarcity of available radio resources (e.g. bandwidth, frequencies), protocols, and radio characteristics (e.g. packet error rate, jitter, delay)
  • Application layer
    • Due to service delivery, discovery and registry management.
• **Generic protection goals, similar to those found in other systems, such as:**
  - Confidentiality
  - Control
  - Integrity
  - Authenticity
  - Availability
  - Authentication
  - Authorization
  - Non Repudiation
  - Utility
  - Accountability
  - Trust
  - Traceability
Incorporation of cross layer information originating from:

- Services
- Data
- Network
- Radios
- Terminals
- Users
• Fine-grained conceptualization of constituent network elements
• Anticipated processes
• Operational requirements

\[
\text{Individual\_Domain} \cap \text{Individual\_Capability} = \{\text{Individual\_Action\_A}(k), \text{Individual\_Action\_A}(k+1), \ldots, \text{Individual\_Action\_A}(k+j)\}
\]

where
\[
\text{Individual\_Action\_A}(k) \approx \text{Rule A}[k(z)], \text{Rule A}[k(z+1)], \ldots, \text{Rule A}[k(z+i)]
\]
• **Description logic (DL) fragments**

  • ALC + role hierarchies and inclusion, inversion, nominals, functionality properties and qualified cardinality restrictions – SHOIN(D)

\[
\text{Terminal} \equiv \text{individual} \land \exists \text{has\_Terminal\_ID}.

\text{Local\_Provider} \equiv \text{Terminal} \land \exists \text{Has\_Operational\_Group.OG2} \\
\land \exists \text{Has\_Status.Offline} \land \exists \text{Has\_Functionality.SP}

\text{Available\_Service} \equiv \text{Service} \land \leq 1 \exists \text{Has\_Local\_Provider}
\]

**Concept assertion**

\[
\text{File} \sqcap \text{Video(Message}_x) : \text{Message}_x \text{ is a video file}
\]

**Role assertion**

\[
\text{hasSource(Message}_x, \text{Terminal}_y) : \text{Terminal}_y \text{ is the source of Message}_x
\]
• **Diversity of node capabilities**
  - (Nodes can not be expected to be able to support all the security mechanisms)
    - Distinct platforms, with diverse capabilities and requirements
    - Dynamically adaptable policies are too heavyweight for some types of tactical nodes

• **Operational and functional diversity of deployed assets**
  - (Nodes are not required to support all the security mechanisms)

• **Dynamic network topologies**
  - (No centralized security dedicated entity can be assumed, due to constant alteration of the available resources and connectivity)
What effects the policy distribution?

- **Ontology (policy)**
  - Syntactic complexity
  - Structural complexity

- **Tactical nodes**
  - Operational specialization
  - Functional specialization
  - Operating features

- **Dynamism**
  - Dynamic attributes
  - Dynamic policy evaluation
  - Tactical decision cycle

- Action: $A'n = (D\hat{i} + C\hat{j} + A\hat{g})$, Where $\hat{i}$, $\hat{j}$, $\hat{g}$ are unit vectors
  - Security policy: $SpOg(x) = \{V_i, V_{i+1}, ..., V_{i+n}\}$
  - $SpOg(x) = SpFg(j) \cup SpFg(j+1) \cup ... \cup SpFg(j+n)$
    - $V(n) = \{R(i), R(i+1), ..., R(i+n)\}$
  - Vector complexity: $CV(n) = \sum_{i=1}^{n} CR(i)$
    - ...

- Maximize: $D = \sum_{i=1}^{k} \sum_{j=1}^{n} pR(j) \cdot X_{ij}$

- Subject to: $\sum_{j=1}^{n} CR(j) \cdot X_{ij} \leq CCFg(i), i = [1, ..., k]$
  - $\sum_{j=1}^{n} X_{ij} = 1, i = [1, ..., k]$
  - $X_{ij} = 1$ or $0, i = [1, ..., k], j = [1, ..., n]$

- $X_{ij} = \begin{cases} 1 & \text{if } R(j) \text{ is selected for } Fg(i) \\ 0 & \text{if not} \end{cases}$
Types of divergences to be reconciled

- **Strict syntactic, terminological and semiotic homogeneity**
  - (The distributed ontologies are consistent to the central model)
    - Conceptual heterogeneity

- **The local ontologies operate within only two dimensions of context dependent representation (Partiality and perspective)**
  - Approximation is only utilized across the governing rules

- **Thus:**
  - We face only conceptualization mismatches and differences in perspective
  - Explicitation mismatches, coverage differences and granularity differences will not occur
  - These changes will only occur on data and object properties
  - The only allowed alterations are modifications
  - Extensions and reductions are not allowed
Ontology mapping is mature...

but what about communication constraints?

- Cannot transmit the entire local ontology
- Cannot include multi-transaction negotiation methods
- Cannot depend on a centralized entity
- Must limit the number of involved nodes
- Increased reconciliation confidence is required
- Must maintain history of updates
- Roll back capability is required
• **Local ontology**
  • Fragment of global policy

• **Local node assignment list**
  • Fragment of global node assignment list, responsible for the identification of the subset of nodes, which incorporate the altered element.

• **Local change ontology**
  • Maintains a copy of locally sensed and enforced changes for audit and roll back purposes

• **Criticality/ timeliness measure**
  • For prioritization purposes

• **Archive of requested changes**
  • Maintains a copy of externally requested changes for audit and roll back purposes

• $\Delta$
  • It includes the altered element, and various characteristics of the alteration, such as justification, time, actor.
Security and QoS interoperability

- **Security related considerations**
  - Enforcement of protection goals (under the aforementioned constraints)

- **QoS related considerations**
  - Message encapsulation and processing, down to the level of packets sent over radio, has been carefully adjusted across the TSI stack before radio emission.
    - Messages of higher priority/reliability will always receive prioritized treatment.
    - Messages temporized or degraded should be dealt with appropriately.
  - Etc (traffic management, battery consumption ... )
- **Ontology and policy framework adjusted to TACTICS**
  - **Observable objects**
    - Static and dynamic attributes both in raw, aggregated or statistical form
  - **Enforcement mechanisms**
    - Session manager, service registry, encryption, message adaptation etc
  - **Actions**
    - Prioritise service invocation, drop message, isolate compromised node etc.

![Diagram showing the relationship between Sec, QoS, and Core categories with observable objects and their actions.
• **Interoperability mechanism**
  - Based on TACTICS architecture and Tactical Service Infrastructure.

---

**Proposed solution**

[Diagram showing TSI (TACTICS Service Infrastructure) components and their interactions.]

- **TSI** (TACTICS Service Infrastructure)
  - Processing Pipeline
    - Service Mediator
    - Message Session Manager
    - Proxy Services
    - Message Payload Reduction Service
    - Logging Service
    - Message Queue Service
  - Message Handler
    - Messaging Service
    - Message Transport Services
    - Packet Handler
    - Packet Handling Service
  - Radio Access

- **Controller**
  - QoS Handling Service
  - Metadata Handling Service
  - Security Handling Services
  - Service Registry
  - Service Discovery
  - Policy Management Services
  - Contextual Monitoring Service
  - Routing Service
  - Name Service

- **Information System**
  - MTF Availability Service Consumer

- **Diagram Nodes**
  - Security
  - PDP
  - QoS
  - PDP
  - PIP
  - Contextual Monitoring
  - Metadata Handler

- **Interactions**
  - 1. Action Enforcer
  - 2. Security
  - 3. PEP
  - 4. QoS PDP
  - 5. PIP
  - 6. Contextual Monitoring
  - 7. Metadata Handler
  - 8. QoS Handler
Thank you

Vasileios Gkioulous
vasileios.gkioulous@ntnu.no