Interoperability of Security and Quality of Service Policies Over Tactical SOA

Gkioulos Vasileios
and Stephen D. Wolthusen
NISlab, Norwegian University of
Science and Technology, Norway.
{vasileios.gkioulos,
stephen.wolthusen}@ntnu.no

Adam Flizikowski
and Anna Stachowicz
ITTI Sp. z.o.o., Poznan, Poland.
{adam.flizikowski,
anna.stachowicz}@itti.com.pl

Dariusz Nogalski, Kamil Gleba
and Joanna Sliwa
C4I Systems Department,
Military Communication Institute
Zegrze, Poland.
{d.nogalski,k.gleba,j.sliwa}@wil.waw.pl

***Abstract*—Tactical networks are constrained networks that may transition between ad-hoc and mesh configurations and are characterised by frequent disruptions, changes in connectivity, and available resources. Whilst deploying a service-oriented architecture (SOA) allows the efficient provisioning of services at the tactical level, the existing resource limitations and potential attacks, require the dynamic adaptation of both quality of service (QoS) and security mechanisms. Within this environment, security and QoS must not only enforce the requisite functionalities, but also cooperatively seek optimal solutions for them according to their corresponding constraints and requirements. In this paper we propose a multi-domain policy-based decision subsystem supporting service delivery, that relies on an online knowledge-based reasoning mechanism. We describe the characteristics of such subsystem and show its benefits in relation to specific tactical requirements.**

I. Introduction

Tactical command and control (C2) systems are used on contemporary battlefields in order to support the deployed assets fulfilling their corresponding tasks. During the mission execution stage, information and service delivery are of the highest importance. Such information may correspond to blue/red force tracking or alerts, consolidating the required situational awareness. Moreover, where network provisioning allows, it is also desirable to offer access to higher echelons and more resource-intensive services. Current tactical communication systems may operate over SatCom links with long latency on the order of several hundred millisecond, or wireless networks that may allow multi-MBit/s transfer rates but can also be limited to the low kBit/s range for some VHF waveforms, as well as be limited by spectrum contention and attacks. Additionally VHF networks may work with large jitter at the range of 9 seconds caused by channel access mechanisms. According to earlier experiments and field trials [1] the traffic load generated by C2 systems is very often too big for tactical communications systems. Therefore there is a strong need for an intelligent middle-ware layer that would adapt the user traffic, while at the same time supporting reliable and secure delivery of information under dynamic topology changes.

Further dynamic, but partially predictable changes to parameters including connectivity or route availability arise from interactions with node mobility and topography or channel reservation. This is particularly challenging for SOA, as service invocations may span multiple nodes in a given transaction, and where some underlying wireless networks may impose long queues and do not allow for rapid message acknowledgements. Service and message prioritisation is therefore a key aspect of enforcing QoS constraints, where invocations or messages to avoid jeopardising lives and mission objectives must take precedence over optimal network utilisation for multiple competing services.

These challenges are addressed by the EDA TACTICS [2] project, by proposing a SOA based middle-ware (so called TSI-Tactical Service Infrastructure), supporting information distribution on the tactical level. The designed TSI [3] consists of several core services, the configuration and composition of which is to support information delivery. This is however a very complicated task that must take into account the command structure, mission objectives, current situation on the battlefield and risk of releasing vulnerable information to the enemy while maximizing overall mission effectiveness. The overall TSI configuration is a complicated task that cannot be statically predefined.

In public communication systems, the network infrastructure is commonly over-provisioned, giving the possibility to support traffic overload levels that have been predicted in the system planning phase. Communication systems at the battlefield cannot support even those standard information relations due to their generic low capacity. Thus, within TACTICS the problem of traffic adaptation is critical. However limiting the traffic size may require the necessity to modify and shape it, taking into account its priority and the specific requirements of the mission. The military background of TACTICS makes it also necessary to consider the security and reliability dimension of information relations. Some messages must be delivered intact or must be secured (e.g. encrypted, protected from integrity loss) due to the life preservation requirement. Yet, these two concepts may be contradictory given the limited bandwidth of tactical networks. This problem is not common in public networks, but in tactical networks it becomes the main issue very often forgotten in research. The TSI configuration requires that all TSI core services are assigned actions that must be performed in sequence, for the middle-ware to work efficiently under a given set of conditions.

Whilst some parameters and choices can be configured during the mission preparation stage, many will become known only during the mission itself and must hence be responded to dynamically. We therefore argue that a policy-based mechanism capable of incorporating situational context and decisions is desirable for tactical networks middle-ware control. Having previously demonstrated the effectiveness of such on-line reasoning mechanisms for adapting decisions over security policies [4]–[8] and research results on system to system mediation by overcoming structural domain differences [9]–[11], in this paper we propose a security and QoS interoperability mechanism.

This article focuses on the problem of the QoS and security domains interoperability as it has been studied in the EDA TACTICS project. Interoperation between TACTICS decision domains refers to achieving an agreed decision via trade-offs between the QoS and Security domain controllers. We highlight the selected TACTICS QoS and security requirements, and present the developed decision subsystem architecture. The control logic (context dependent rules) to conduct adaptations will be subject to following research (validation step). Hereby we only present a simple integration example according to the designed tactical service infrastructure. The remainder of this paper is structured as follows: Chapter 2 presents related work in the corresponding areas. Chapters 3 and 4 present individual and complementary aspects of the topic under the scope of security and QoS, based on our earlier studies. Chapters 5,6 and 7 provide an overview of the designed solutions, referring to the decision subsystem, policy framework and interoperability mechanism.

II. Related work

The dynamic orchestration of services has been known to be a hard problem, Yu et al. demonstrated that even for a static configuration, selecting optimal services, whether for QoS, security, or both, is an $\mathcal{NP}$-hard problem [12]. Subsequent work such as by Nejdl et al. investigated further heuristic approaches [13] where e.g. Ben Mabrouk et al. proposed the use of a guided heuristic for dynamic service composition [14] whilst Li et al. proposed a QoS-based composition, tolerating random faults via case-based reasoning [15]. The authors are not aware of work explicitly covering dynamic networks such as tactical networks with existing work focusing on near-optimal selection of *end-to-end* QoS, which may not be possible in a highly dynamic tactical network where decisions may be required also locally [16]. However, Al Ridhawi and Karmouch recently proposed a semantically-oriented per-hop approximation of service composition that is applicable to mobile networks [17]. Similar considerations as for composition also apply to QoS-aware service discovery [18] even where service registries are largely static as may be the case for configurations set up at the mission preparation stage in tactical networks.

Ontological models for describing QoS characteristics have also been studied building e.g. on the DARPA Agent Markup Language-Service (DAML) [19] for service discovery in early work; a more recent survey and analysis is provided by Zeshan et al. [20]. Similar works aimed to enhance web service discovery/selection [21]–[25] and composition [26], [27]. Yet, facets such as ontology-based approach for QoS monitoring and QoS adaptation in SOA systems even if mentioned, are not thoroughly investigated.

Similar efforts have also focused on adding security metadata and capabilities to service descriptions such as the NRL Security Ontology by Kim et al. [28] as the WS-SecurityPolicy standard does not offer explicit semantics; this has led to efforts such as work by Di Modica and Tomarchino to augment WS-Policy documents [29] and more recently efforts to map these into an OWL-DL ontology by Ben Brahim et al. [30]. Our earlier work [4]–[8] has described capturing security properties and objectives for the dynamic modelling and evaluation of security policies in the form of ontologies over which a descriptive logic (DL) fragment can be used for on-line, distributed reasoning. However the work concentrated mainly on security measures and policies, and further research is needed how such an approach can fit into a combined QoS and Security policy framework.

Interoperability in military systems [9]–[11], [31]–[34] can refer to the physical [35] (Interoperability of radio communication), syntactical [36] (Common data modelling) or semantic level [10] (Ability of two computerized systems to exchange information for a specific task and make sure that the meaning of the information is accurately and automatically interpreted by the receiving system). The role of a knowledge-based C2 system mediator is to solve the conceptual mismatch problem knowing the context under which the two systems interoperate and the common operational goal. The research however does not address the tactical wireless network constraints but rather higher levels of commands where network problems are reduced.

It is evident that earlier work focused on the incorporation of limited security related aspects within developed QoS frameworks and conversely. Yet, the attainment of the required functionalities within tactical networks requires a mechanism dedicated to the consolidation of the unique and domain specific requirements, given the underlying constraints.

III. Constraints and Requirements

The security and QoS requirements must be satisfied both pro-actively and reactively. An ontological representation does not permit contradictions within a common knowledge base; however, conflicting objectives among QoS and security are inevitable and must be kept representationally disjoint.

A. Security Related Considerations

As shown earlier, requirements for security of individual and composed services refer both to fundamental protection goals (such as Confidentiality, integrity, availability) and layered requirements (such as non-repudiation, labelling, traceability) referring to transmitted or data at rest and the processing procedures constituting the service delivery. For that purpose, the security mechanisms must be scalable and should incorporate information from various layers of the SOA platform. Such cross-layer information can become visible and be utilised within the defined security policies, in order to support their dynamic adaptation to the continuous network alterations. Additionally, the functional constraints of tactical nodes require the adaptation of the implemented security mechanisms, in order to support both isolated and cooperative operation. In the context of dynamic adaptation, this partitioning capability can allow the partial or complete delegation of security related functionalities across the deployed actors, provided that standalone operability is maintained.

B. QoS Related Considerations

Although a large body of knowledge relevant to QoS can be configured in the mission preparation stage such as service types and priorities or node capabilities including radios and mobility, dynamic adaptation plays a larger role. For some services such as blue force tracking it will be possible to configure the maximum delay for which such messages can be queued, diverted, or be put on hold before discarding, while maintaining sufficiently frequent updates to retain a situational picture. Similarly, certain types of messages and service invocations such as MEDEVAC requests must be prioritised. Reasoning and decisions over QoS in tactical networks must occur at several levels from radio frequency interface selection and message queueing, via route selection and service invocation, up to service semantics where e.g.service substitution may need to occur. QoS mechanisms frequently rely on discovery of available resources and services, and will use explicit resource reservation to enforce requirements and constraints. Yet, given the limitations of tactical networks this would require allocation of a substantial fraction of all available resources to the QoS infrastructure. Instead, we argue that QoS mechanisms for tactical networks can only rely on implicitly available information obtained from the local node. This information such as on routing or channel characteristics, including latency and packet loss rate, is gathered in the knowledge base from several abstraction layers, however, and only in rare instances can this be augmented by a node-external query. A key requirement, moreover, is that the adaptation mechanism is itself sufficiently agile that decisions for selecting services or their configuration occur in a timely manner before the configuration of the tactical network changes and thereby invalidates the evaluated configuration.

IV. Interoperability Requirement

The interoperability requirement between the security and QoS mechanisms results from the aforementioned distinction of priorities and motivation, which at times may impose contradictory objectives. Furtheremore, equally important is the notion of policy dynamicity, which refers to the on-line adaptation of security and QoS policies due to alteration of contextual parameters. QoS aims to adapt the traffic flow (user traffic and TSI outgoing traffic) to fit into the limited communication channel, maximizing resource utilization by the user data. Concurrently, security aims to guarantee the enforcement of corresponding protection goals, such as privacy, integrity, authentication, authorization and intrusion detection. This however comes with a price of additional overhead, that leads to resource deprivation from the transmission of plain user data. Thus the aim of security and QoS interoperability is to reach a common agreement given the highest good-put and the optimum denominator in terms of security measures.

If for a given action (e.g. Service invocation) the cumulative security and QoS overhead exceeds the available channel bandwidth, an alternative solution must be negotiated, referring either to action substitution (e.g. service substitution) or action parametrization (e.g. Routing/encryption algorithm replacement). This may be the case when it is necessary to enforce lighter security mechanisms (e.g. Shorter key length or selection of pre-shared symmetric keys instead of key negotiation), or shape user data (e.g. Message payload reduction or message drop). Even in the simplified scenario of a routing decision request from a deployed Messaging_service to the Routing_service, the getNextHop() admission has distinct policy requirements for QoS and security.

In a more specific scenario though, if the message is already protected by integrity mechanisms, it cannot be modified without breaking message integrity. Thus, payload reduction must be removed from the available adaptations. In another scenario of interoperability goals, QoS aware routing should be enriched with intrusion detection information for the avoidance of compromised nodes, based on dynamic trust management information. Additionally, the selected QoS and security related actions must be prioritised (e.g. Message modification before integrity and encryption).

Thus, the interoperability requirements should be achieved, while security and QoS maintain their corresponding decision focus, allowing transparency for the reconciliation of their distinct decisions. This reconciliation is to occur in a small number of discrete steps allowing partial re-use of reasoning structures, where each domain must apply pre-configured relaxations until requirements are satisfied or an empty resolution is obtained.

V. TACTICS TSI and Decision Subsystem

The overarching goal of TACTICS is to define the reference architecture of the TSI, as a middle-ware placed between the IS (Information System) and the radio, transparently given the utilization of standard tactical radio equipment. The TSI concept architecture divided the middle-ware into two vertical stacks, as presented in figure 1. The Controller holds the whole *intelligence* and supervises the functionality of particular processing layers of the TSI. The second, acts as the Processing Pipeline, which processes messages coming from the IS down to the bearer (radio access level) at three horizontal layers, namely Service, Message and Packet.

The Processing pipeline handles sessions, processes messages, cuts them into packets and sends them out through the radio (or other network interfaces). Each of the three layers has means to enforce QoS mechanisms adapting the traffic

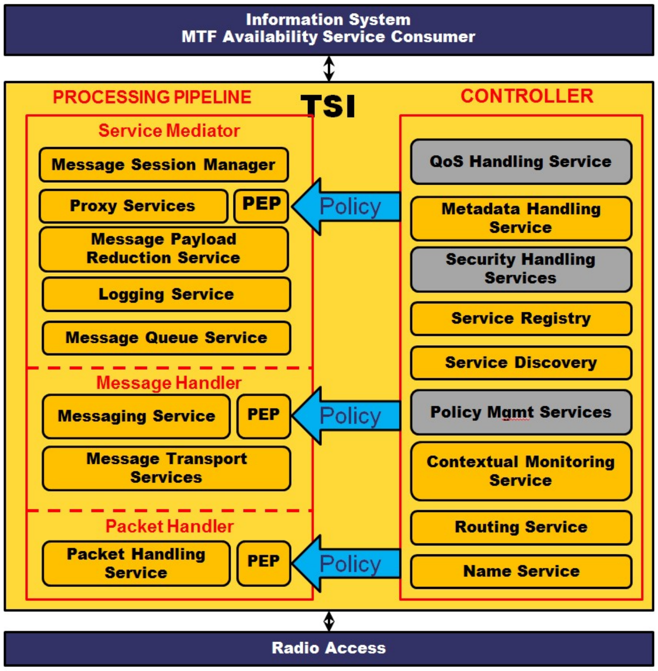

Fig. 1. Processing pipeline and controller in the TSI architecture.

to the current network conditions and device status, as well as security mechanisms supporting confidentiality, integrity and access control (so called PEP, Policy Enforcement Point). These mechanisms are triggered by actions, the activation of which is decided in the Controller (see chapter VII). The Controller collects the aforementioned cross-layer information and on the basis of that, enforces policies which configure the Processing Pipeline. Such an approach makes the controlling process independent of singular messages coming to the TSI node. Thus, the PEPs are governed by the policies defined within the Controller referring to security and QoS mechanisms on the particular level. It is worth mentioning that the Controller is able to continuously adapt its decision-making process based on the feedback received through the cross-layer information, after the completion of an action (e.g. Successful message transmission or deletion, intrusion detection etc)

VI. Ontology and Policy Framework

The distinct security and QoS domains and capabilities can be defined as a cohesive group of elements (e.g. Enforcement mechanisms, observable objects and actions) aiming to the fulfilment of the aforementioned discrete goals. Each domain is responsible for the collection of subset environmental parameters, and the management of suitable enforcement mechanisms by taking decisions from its own perspective, for the governance of required actions. Each domain is branched into corresponding sub-domains (e.g. Security - protection, detection, diligence, planning, response // QoS - resource reservation, congestion management, traffic admission, service level agreements). Even though TACTICS requires from each domain to maintain its own decision focus, both QoS and Security may impact each other and enforce contradictory decisions. TACTICS harmonizes both decisions under the frame of a common interoperability goal.

This chapter gives basis to the formal definition of a *TACTICS common policy model*, in the sense that such policy model should support a multi-domain decision environment. The policy model should be comprehensive enough to allow negotiation/deconflictation of QoS and Security cross-layer decisions. Equally important is the notion of policy dynamicity, which refers to the on-line adaptation of security and QoS policies due to alteration of contextual parameters. The notion of dynamicity is incorporated across two distinct dimensions. Initially, the use of ontological structures facilitates the refined capturing of dynamic attributes, across a detailed description of the deployed tactical system in a distributed, prioritized and aggregated manner. Additionally, the alterations of such dynamic attributes is addressed not only by their monolithic incorporation across policy decisions, but in a layered manner by the definition of prioritized rule-sets for each of the expected actions/ interoperability goals.

In respect to the *observable objects*, each domain is responsible for the collection of subset environmental parameters, for the population of the local knowledge base. The *TACTICS common ontology* is defined as a knowledge base, where the T-Box is a set of classes, properties and axioms, while the Abox is a set of individual terms and assertion sentences. The TBox terms are divided into three basic sets, namely Core, QoS and Security, where:

Core: Elements related to common and generic classes, such as:

- User
- Service
- Device
- Radio network
- Information
- Topology

and properties, such as:

- Service invokes service
- Service is deployed on device
- Network is accessed by user
- Network uses radio
- User accesses network
- Device is located at

Each of these elements within the core is further specialized. Thus, Core:Information may be specialized as Core:Message and further as Core:User Message or Core:Signalling Message. Similarly the security and QoS sets are constructed, according to the corresponding domain specific requirements, as presented at figure 2. It must be noted that the construction and deployment of the defined policies is conducted at the mission preparation stage, where no computational or other constraints are present. At this stage optimal solutions are approximated with the incorporation of mission specific operational requirements and the use of computational intelligence methods.

The aforementioned *enforcement mechanisms* refer to security and QoS dedicated services, capable of enforcing the policy decisions in respect to the questioned actions. The defined enforcement mechanisms include, but are not limited to:

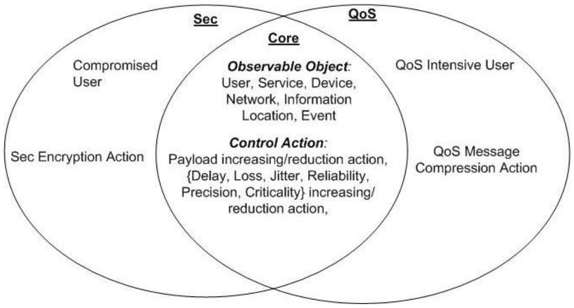
Sec
QoS
Core
Compromised User
Observable Object:
User, Service, Device, Network, Information Location, Event
QoS Intensive User
Sec Encryption Action
Control Action:
Payload increasing/reduction action, {Delay, Loss, Jitter, Reliability, Precision, Criticality} increasing/ reduction action,
QoS Message Compression Action

Fig. 2. Simplified example of Multi-domain ontology construction.

- Session manager
- Service registry
- Message queue
- Trust management
- Encryption
- Intrusion detection
- Service choreography
- Routing
- Traceability
- Message adaptation

VII. Interoperability of Security and QoS

The Tactical Service Infrastructure Reference Architecture (TRA) created within TACTICS, has been modelled in accordance to the NATO Architecture Framework 3.1. The elements of the TSI architecture aiming to facilitate the interoperability of security and QoS mechanisms are:

Action requester: A service that initiates an action request. It can be either the Security Handler or the QoS Handler, which monitoring network parameters identify the requirement for a specific action/adaptation. Each of these elements can additionally incorporate precomputed or generic policy decisions, which are enforced by the corresponding Policy Enforcement Points (PEP) without invoking the Policy Manager. This mechanism is integrated for optimization purposes in case or constrained reasoning resources.

Security/QoS PEP: A service that incorporates the required mechanisms or knowledge, for the enforcement of any generated or precomputed policy decision.

Policy manager: A service that transfers the decision request to the Security/QoS Policy Decision Points (PDP) and the Metadata Handler. Additionally, the policy manager is responsible for the deconflictation of the PDPs decisions.

Security/QoS PDP: A service that contains the policy rules for the available action requests for instance identification. Multiple rules are constructed for each action request, incorporating static and dynamic attributes regarding services, information, nodes, radios, networks and subjects. The rules corresponding to each action request, are prioritized and utilized for deconflictation purposes between the security and QoS domains.

Metadata Handler: An ontologically constructed knowledge-base that incorporates static and dynamic attributes required for policy decisions. These attributes may refer to services, information, nodes, radios, networks and subjects. Metadata Handler constructs a static copy of the ontological structure (snapshot) at the initiation of an access request, which is maintained until the successful generation of a valid/deconflicted policy decision. Reasoning for a given action request is achieved with the use of this dedicated static copy and the policy rules included at the PDPs

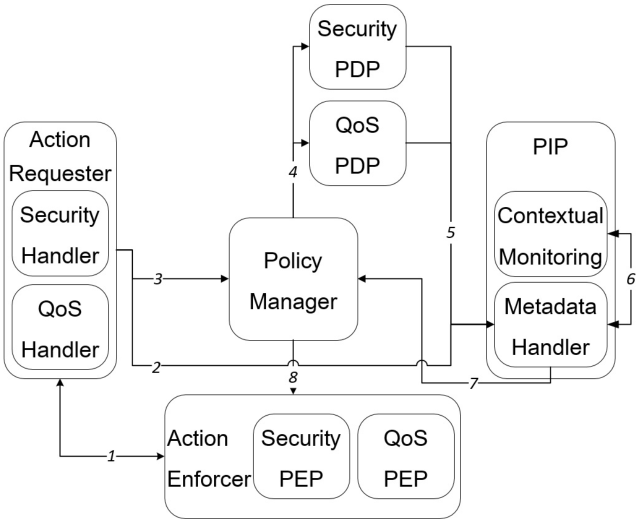

Fig. 3. Elements and flows involved into policy decisions.

Contextual monitoring: A service that periodically monitors the dynamic attributes, while it also incorporates mechanisms for the computation of statistical and aggregated values. These attributes are incorporated into policy rules, for optimization purposes in cases or constrained reasoning resources.

A. Analytical scenario

The interconnectivity of the defined elements is presented at figure 3, while the functionalities of the numbered interactions can be described with the use of a simplified message prioritization scenario. Assuming that a message labelled as *"Alert"* arrives at the Message Queue (MQ), the MQ operating as action solution requester transfers an Action Solution Request (ASR) to the QoS Handler (QH). Concurrently the following functionalities occur, as depicted at figure 3.

- **Functionality 1, Interaction 1:** QH seeks locally stored precomputed solution in cooperation with the Security Handler (SH), to be transferred directly for enforcement to QoS PEP. (For the purpose of the scenario, no solution if found at this stage. If a precomputed solution is found at this stage, the procedure is completed successfully.)
- **Functionality 2, Interaction 2:** QH requests ASR dedicated snapshot of Metadata Handler (MH) at time T0. This message initiates the AReS (Action Request Session) with a dedicated Action Request Session ID (AReS.ID).
- **Functionality 3, Interaction "Self":** QH locally resolves the ASR, generating QoS oriented list of prioritised Action Solutions (AS).
  - Note 1: AS computation is based on partial information (e.g. Limitations of routing protocol)
  - Note 2: Computation at the level of the Action Requester (AR) may rely on lookup tables, partial

knowledge bases, or algorithmic solutions which are defined at the mission preparation stage.

  - Note 3: The computed AS refer to the message type of the examined message, based on predefined attributes and has the prioritised form:
    AS1 = MessageTypeX.priority(High)
    AS2 = MessageTypeX.priority(Medium).

- **Functionality 4, Interaction 3:** QH transfers an Action Request (ARe) to the Policy Manager (PM). The ARe is formed as a bundle, including the optimal AS and the dedicated AReS.ID, which is bound to the dedicated MH snapshot.
  - Note 1: There is an one to one mapping between the ARes.ID and the Snapshot ID (Sn.ID)
  - Note 2: ARe has the form: ARe=(AReS.ID, AS1)
- **Functionality 5, Interaction 4:** PM transfers the ARe to the security and QoS PDPs.
- **Functionality 6, Interaction "Self":** The two PDPs identify the dedicated sets of rules for the examined ARe (MessageTypeX, prioritization), based on their decision contexts and the common interoperability goal.
  - Note 1: The rules are in the form of prioritized queries.
  - Note 2: Identification is achieved with the use of lookup tables, which are constructed at the mission preparation stage.
- **Functionality 7, Interaction 5:** The set of first priority rules (one from Security and one from QoS) are transferred to the MH. The messages carry the predefined AReS.ID as:
  QoS: (AReS.ID, QoS_Rule1)
  Security: (AReS.ID, Security_Rule1)
- **Functionality 8, Interaction 6:** MH reasons for the examined session, given the session dedicated copy of the ontology (Sn.ID) and the received set of rules. The MH returns:
  Allow acknowledgement: If instances have been identified on a query.
  Not allow acknowledgement: If no instances have been identified.
- **Functionality 9, Interaction 7:** MH transfers the query responses to the PM.
- **Functionality 10, Interaction 8:** PM evaluates the responses and if they are not contradictory AS1 is transferred to the QoS PEP for enforcement. Possible contradictions are resolved with the use of the aforementioned deconflictation mechanisms (In a least constrained scenario, this can be achieved with an examination of secondary rules and AS).

VIII. Conclusion

The attainment of interoperability across the security and QoS requirements of constraint tactical networks imposes multiple challenges. Under this scope, this article presents the designed mechanisms for that purpose, within the project TACTICS. The identified constraints and requirements have been presented along with the architecture of the decision subsystem. Additionally, an insight has been provided over the utilised ontology and policy framework, focusing on the developed interoperability mechanism. Our future work will focus on the refinement of the presented framework, according to the requirements of tactical networks.

Acknowledgements

The results described in this work were obtained as part of the EDA project TACTICS. The TACTICS project is jointly undertaken by Patria(FI), Thales Communications & Security(FR), FKIE(DE), Thales Deutschland(DE), Leonardo(IT), Thales Italia(IT), NTNU(NO), ITTI(PL), MCI(PL), and their partners, supported by the respective national Ministries of Defence under EDA Contract No. B 0980.

References

[1] M. Manso, J. M. A. Calero, C. Barz, T. H. Bloebaum, K. Chan, N. Jansen, F. T. Johnsen, G. Markarian, P.-P. Meiler, I. Owens, *et al.*, "Soa and wireless mobile networks in the tactical domain: Results from experiments," in *Military Communications Conference, MILCOM 2015-2015 IEEE*, pp. 593–598, IEEE, 2015.

[2] A. Aloisio, M. Autili, A. D'Angelo, A. Viidanoja, J. Leguay, T. Ginzler, T. Lampe, L. Spagnolo, S. D. Wolthusen, A. Flizikowski, and J. Sliwa, "TACTICS: TACTICal Service Oriented Architecture," *CoRR*, vol. abs/1504.07578, 2015.

[3] T. A. Lampe, C. Prasse, A. Diefenbach, T. Ginzler, J. Sliwa, and S. McLaughlin, "TACTICS TSI Architecture," *International Conference on Military Communications and Information Systems ICMCIS*, 2016.

[4] V. Gkioulos and S. D. Wolthusen, "Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks," *Norwegian Information Security Conference 2015 (NISK-2015).*

[5] V. Gkioulos and S. D. Wolthusen, "Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures," *Advances in Networking Systems Architectures, Security, and Applications - of Springer's Advances in Intelligent Systems and Computing*, 2015.

[6] V. Gkioulos and S. D. Wolthusen, "Reconciliation of Ontologically Defined Security Policies for Tactical Service Oriented Architectures," *International Conference on Future Network Systems and Security 2016 (FNSS 2016).*

[7] V. Gkioulos and S. D. Wolthusen, "Securing Tactical Service Oriented Architectures," *2nd International Conference on Security of Smart cities, Industrial Control System and Communications (SSIC 2016).*

[8] V. Gkioulos and S. D. Wolthusen, "A Security Policy Infrastructure for Tactical Service Oriented Architectures," *2nd Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems (CyberICPS 2016).*

[9] D. Nogalski and A. Najgebauer, "Semantic mediation of NATO C2 systems based on JC3IEDM and NFFI ontologies," in *NATO RTO symposium on Semantic and Domain based Interoperability*, November 2011. Reference RTO-MP-IST-101 AC/323(IST-101)TP/426.

[10] D. Nogalski, R. Ford, S. Kuehne, B.-J. Hansen, D. Hanz, M. Last, V. Mojtahedzadeh, G. Scamarcio, F. Tuncer, and M. Wunder, "Framework for Semantic Interoperability," Tech. Rep. STO-TR-IST-094 AC/323(IST-094)TP/525, NATO Science and Technology Organisation, 2014. Reference STO-TR-IST-094 AC/323(IST-094)TP/525.

[11] D. Nogalski, R. Ford, S. Kuehne, B.-J. Hansen, D. Hanz, M. Last, V. Mojtahedzadeh, L. Santos, F. Tuncer, and M. Wunder, "Bridging Semantic Interoperability gaps with SILF," in *International Conference on Military Communications and Information Systems (ICMCIS)*, pp. 1–11, May 2015.

[12] T. Yu, Y. Zhang, and K.-J. Lin, "Efficient Algorithms for Web Services Selection with End-to-End QoS Constraints," *ACM Transactions on the Web*, vol. 1, pp. 1–26, May 2007.

[13] M. Alrifai, T. Risse, P. Dolog, and W. Nejdl, “A Scalable Approach for QoS-Based Web Service Selection,” in *Proceedings of the Fourth International Workshop on Engineering Service-Oriented Applications (ICSOC 2008)* (G. Feuerlicht and W. Lamersdorf, eds.), vol. 5472 of *Lecture Notes in Computer Science*, (Sydney, Australia), pp. 190–199, Springer-Verlag, Dec. 2009.

[14] N. Ben Mabrouk, S. Beauche, E. Kuznetsova, and V. I. Nikolaos Georgantas, “QoS-Aware Service Composition in Dynamic Service Oriented Environments,” in *Proceedings of the 2009 10th International ACM/IFIP/USENIX Middleware Conference (Middleware 2009)* (J. M. Bacon and B. F. Cooper, eds.), vol. 5896 of *Lecture Notes in Computer Science*, (Urbana-Champaign, IL, USA), pp. 123–142, Springer-Verlag, Dec. 2009.

[15] G. Li, L. Liao, D. Song, and Z. Zheng, “A Fault-Tolerant Framework for QoS-aware Web Service Composition via Case-Based Reasoning,” *International Journal of Web and Grid Services*, vol. 10, pp. 80–99, Jan. 2014.

[16] S.-C. Lin and K.-C. Chen, “Cognitive and Opportunistic Relay for QoS Guarantees in Machine-to-Machine Communications,” *IEEE Transactions on Mobile Computing*, vol. 3, pp. 599–609, Mar. 2016.

[17] Y. Al Ridhawi and A. Karmouch, “Decentralized Plan-Free Semantic-Based Service Composition in Mobile Networks,” *IEEE Transactions on Services Computing*, vol. 8, pp. 17–31, Jan./Feb. 2015.

[18] D. Lin, C. Shi, and T. Ishida, “Dynamic Service Selection Based on Context-Aware QoS,” in *Proceedings of the IEEE Ninth International Conference on Services Computing (SCC 2012)* (L. Moser, M. Parashar, and P. Hung, eds.), (Honolulu, HI, USA), pp. 641–648, IEEE Press, June 2012.

[19] C. Zhou, L.-T. Chia, and B.-S. Lee, “Web Services Discovery with DAML-QoS Ontology,” *International Journal of Web Services Research*, vol. 2, pp. 43–66, Apr. 2005.

[20] F. Zeshan, R. Mohamad, and M. N. Ahmad, “Quality of Service Ontology Languages for Web Services Discovery: An Overview and Limitations,” in *Proceedings of the 15th International Conference on Human Interface and the Management of Information (HCI International 2013)* (S. Yamamoto, ed.), vol. 8016 of *Lecture Notes in Computer Science*, (Las Vegas, NV, USA), pp. 400–407, Springer-Verlag, July 2013.

[21] L.-L. Qu and Y. Chen, “QoS ontology based efficient web services selection.,” in *International Conference on Management Science and Engineering (ICMSE)*, pp. 45–50, IEEE, 2009.

[22] a. A. E. Duygu Çelik, “Ontology-Based QoS Queuing Model for Selection of Web Services Servers.,” in *IEEE 34th Annual Computer Software and Applications Conference Workshops (COMPSACW)*, pp. 7–12, IEEE, 2010.

[23] A. Alnahdi, S.-H. Liu, and A. Melton, “Enhanced Web Service Matchmaking: A Quality of Service Approach,” in *IEEE World Congress on Services (SERVICES)* , pp. 341–348, IEEE, 2015.

[24] G. Dobson and A. Sanchez-Macian, “Towards unified QoS/SLA ontologies,” in *Services Computing Workshops IEEE*, pp. 169–174, IEEE, 2006.

[25] V. Xuan, “WS QoSOnto: a QoS ontology for web services,” in *IEEE International Symposium on Service-Oriented System Engineering, (SOSE)*, pp. 233–238, IEEE, 2008.

[26] S. Baccar, M. Rouached, and M. Abid, “A user requirements oriented semantic web services composition framework.,” in *IEEE Ninth World Congress on Services (SERVICES)*, pp. 333–340, IEEE, 2013.

[27] H. Yang, X. Chen, and S. Liu, “Research and implementation on QoS ontology of web service-oriented composition,” in *2nd International Symposium on Information Engineering and Electronic Commerce (IEEC)* , pp. 1–4, IEEE, 2010.

[28] A. Kim, J. Luo, and M. Kang, “Security Ontology to Facilitate Web Service Description and Discovery,” in *Journal on Data Semantics IX* (S. Spaccapietra, P. Atzeni, F. Fages, M.-S. Hacid, M. Kifer, J. Mylopoulos, B. Pernici, P. Shvaiko, J. Trujillo, and I. Zaihrayeu, eds.), vol. 4601 of *Lecture Notes in Computer Science*, (Heidelberg, Germany), pp. 167–195, Springer-Verlag, July 2007.

[29] G. Di Modica and Tomarchino, “Semantic Security Policy Matching in Service Oriented Architectures,” in *Proceedings of the 2011 IEEE World Congress on Services* (D. S. Milojicic and M. Kirchberg, eds.), (Washington D.C., USA), pp. 399–405, IEEE Press, July 2011.

[30] M. Ben Brahim, T. Chaari, M. Ben Jemaa, and M. Jmaiel, “The SemSPM Approach: Fine Integration of WS-SecurityPolicy Semantics to Enhance Matching Security Policies in SOA,” *Service Oriented Computing and Applications*, vol. 10, pp. 1–28, Feb. 2016. *(in press)*.

[31] A. Tolk and J. Muguira, “The Levels of Conceptual Interoperability Model (LCIM),” in *Proceedings of the Fall Simulation Interoperability Workshop*, 2003.

[32] V. Srivastava and M. Motani, “Cross-layer design: a survey and the road ahead,” *IEEE Communications Magazine*, vol. 43, pp. 112–119, Dec 2005.

[33] R. Levenshteyn and I. Fikouras, “Mobileman: design, integration, and experimentation of cross-layer mobile multihop ad hoc networks,” *IEEE Communications Magazine*, vol. 44, pp. 80–85, July 2006.

[34] P. Seymer, A. Stavrou, D. Wijesekera, and S. Jajodia, “Qop and qos policy cognizant module composition.,” in *IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY)* , pp. 77–86, IEEE, 2010.

[35] NSO, “STANAG 5066 C3B (Edition 3) - Profile for HR radio data communications,” March 2015.

[36] MIP, “Joint Command and Control Information Exchange Data Model,” 2014.

[37] Z. Shen and J. P. Thomas, “Security and QoS Self-Optimization in Mobile Ad Hoc Netwroks,” *IEEE transactions on mobile computing*, vol. 7, sep 2008.

[38] Y. Wu and S. Hu, “Optimal policies based on QoS for adaptive communication system with Markov Decision Process,” in *Anti-counterfeiting, 2nd International Conference on Security and Identification (ASID)*, pp. 114–119, IEEE, 2008.