CASHMERE: Context-based Authorization in Hypermedia Agent Environments

Alexandru Sorici[1,*], Adina Magda Florea[1]

[1]National University of Science and Technology POLITEHNICA Bucharest, 313 Splaiul Independentei, Bucharest, Romania

Abstract

Hypermedia Multi-Agent Systems (HMAS) promote an alignment between MAS engineering and the Web architecture to enable development of large, open, dynamic and long-lived interaction systems. HMAS environments exploit HATEOAS to facilitate the *discovery* of the resources whose affordances are required by agents. An insufficiently addressed issue in current HMAS frameworks is that of enabling *authorized* access to resources in a manner exploiting the *dynamics* of multi-agent environments. We propose a framework for *context-based* authorizations for access and discovery of resources in an HMAS, inspired by work on Attributed-Based Access Control and RDF Stream Reasoning. We detail the design of the framework functionality and the integration with current HMAS platforms, highlighting advantages and challenges of the approach.

Keywords

Hypermedia MAS, Web-of-Things, Context, RDF Stream Processing, Context-Based Access Control

1. Introduction

Hypermedia Multi Agent Systems (HMAS) are a design paradigm promoting MAS engineering that is aligned with the web architecture to enable large, open, dynamic and long-lived interaction systems [1]. HMAS use synergies between the *Agent and Artifacts* (A&A) meta-model [2] for agent environment programming and the Web-of-Things (WoT) W3C Thing Description (TD) specification [1], such that *artifacts*, organized into *workspaces* are represented on the web as resources having *properties* and affording *actions* and *event* notifications.

HMAS are characterized by an increased interaction dynamics, since agents can enter or exit an environment, can opt to change the *role* they play in a situation, can start or stop providing a service. This increased *logical mobility* of agents and the open and long-lived nature of HMAS create the need to apply *context-aware* boundaries to the interactions that take place. In turn, this requires a *dynamic control of authorized access* to the services provided by artifact resources in a hypermedia MAS environment.

A simple scenario exemplifies the matter: a research facility implementing a visual event notification system using smart lights in each lab. The smart lights are available as artifacts

ISWC 2023 Posters and Demos: 22nd International Semantic Web Conference, November 6–10, 2023, Athens, Greece

*Corresponding author.

alexandru.sorici@upb.ro (A. Sorici); adina.florea@upb.ro (A. M. Florea)

0000-0002-6850-0912 (A. Sorici); 0000-0001-7249-1871 (A. M. Florea)

[1]WoT Thing Description 1.1 specification: https://www.w3.org/TR/wot-thing-description/

in an HMAS environment and digital assistants of researchers can discover and use them. However, management requires that interaction with any smart light be allowed only for *employed personnel* who are *physically present* in the labs.

The dynamic access control issue remains insufficiently addressed (see preliminary design work on signifiers [3]) in the design of existing HMAS frameworks and is, thus, a focus of the current work, which we title CASHMERE. Concretely, we describe a solution to: *(i)* represent *context* information that is used in dynamic access authorization decision making, *(ii)* implement an RDF stream reasoning mechanism to identify situations of *shared interaction context*, which constitute ground for granting an authorization, *(iii)* represent and validate access authorizations using the SOLID Web Access Control (WAC) specifications [2], and *(iv)* describe the integration of the proposed solution with a hypermedia MAS (Yggdrasil [1]).

2. CASHMERE: Design and semantic web technologies in use

The CASHMERE context-based authorization mechanism (illustrated in Figure 1) exploits an opportunity cost of combining the following semantic web technologies.

Context Representation (Step 1 in Fig. 1). We interpret *context* as "any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves" [4]. To represent context information we employ the CONSERT Ontology [5], which uses reification to describe information in terms of *ContextAssertions* (denoting the *predicate*), which bind several *ContextEntities*. This form allows easy *annotations* of context information, particularly regarding time of assertion, temporal validity and provenance.

Shared Context Modeling (Step 2 in Fig. 1). The CONSERT Model identifies *ContextDimensions* and *ContextDomains* as means to manage and provision context information in a system [6]. *ContextDimenstions* provide *perspectives* of *logical partition* of information (e.g. based on location, based on activity, based on organizational relations). *ContextDomains* are *view instances* obtained from one or more *perspectives* (e.g. *employed* users physically present *in a research lab*, Teaching Activity X, membership relation Y). We define two entities as *sharing*

[2]SOLID Web Access Control specifications: https://solidproject.org/TR/wac

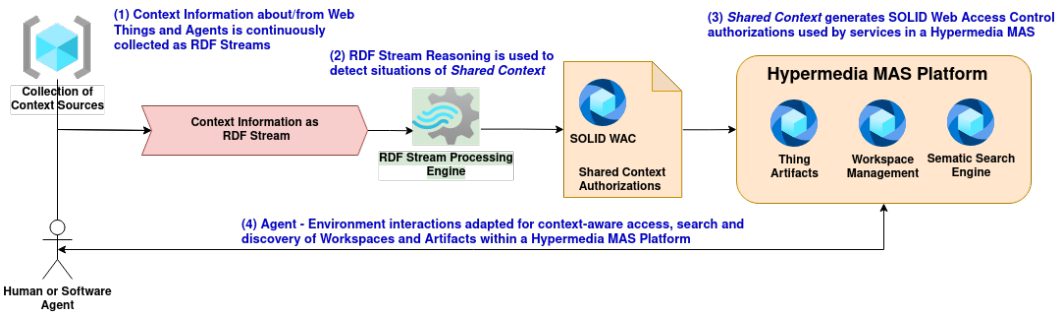

Figure 1: General overview of the information and interaction flow that integrates the CASHMERE context-aware access functionality into a HMAS platform.

context within an application domain if a subset of context information *from* or *about* them is included in at least one *ContextDomain* of the application. The *shared context* relation is formalized as a *group membership* whereby entities that share context belong to the same *ContextDomain Group*.

RDF Stream Processing for Shared Context Identification (Step 2 in Fig. 1). Context information can change in time (e.g. due to agent mobility, changes in current activity) and this requires reasoning methods which can manage such changes. We identify conditions for *shared context* by using RDF Stream processing (RSP) frameworks. Specifically, we use the newest C-SPARQL [7] iteration which follows the RSP-QL [8] semantics of interpreting *time-varying* RDF graphs. RSP-QL introduces new SPARQL operators which (i) define the duration and trigger conditions for *evaluation windows* and (ii) describe the semantics of evaluation output (either as new streams or a snapshot output). In CASHMERE, a *ContextDomain Group* runs C-SPARQL queries to output streams that indicate membership *acceptance* (using CONSTRUCT ISTREAM operators) or membership *revocation* (using CONSTRUCT DSTREAM operators) with respect to the agents and artifacts that are bound by the RDF stream processing query.

SOLID Web Access Control Authorizations (Step 3 in Fig. 1). CASHMERE uses WAC specifications and the ACL ontology to transform the identified shared *ContextDomain* membership into an actionable authorization mechanism. Authorized agents are identified by a WebID [3]. An artifact in an HMAS advertises its list of authorizations using a `rel=acl` Link header. Authorizations provide `Read, Write, Append` or `Control` access. The `acl:agentGroup` mode of identifying authorization subject is used in CASHMERE, describing an instance of a `vcard:Group` which can contain individual agents as members. This maps directly to the mechanism of *ContextDomain* membership CONSTRUCT outputs.

The novelty of our work lies in *reasoning about context information* itself as the main conditioning factor to grant authorizations, leading to a very flexible and extensible method of defining situations that *count as* an *interest* and *legitimate ground for* a human or software agent to access data and services in a hypermedia environment.

3. Overview of HMAS Integration

Figure 2 shows the extension of element types (Artifacts, Workspaces, Environments, Search Services) of the Yggdrasil HMAS platform [1] with their typical WAC authorizations. The service running C-SPARQL inferences to produce membership instances is `Lab308CtxDomainGroup`, outputting them as triples of form `Lab308CtxDomain vcard:hasMember ex:agent` (see Listing 1 as an example inference). The body of the query in Listing 1 distinguishes three context information input sources (different SPARQL graphs), depending on the mode of acquisition: *static assertions* (which identify the agent - line 11), *profiled assertions* (the employment status of the agent - lines 12-20) and a named window defining the stream of sensed `PersonLocated` *ContextAssertion* instances (lines 21-25). Notice that, since the `precis:WorksAt` *ContextAssertion* instance is a profiled one, it is interrogated for its `TemporalValidityAnnotation` (lines 17-19), which is then used to check validity of the employment status (line 27).

[3]WebID specifications: https://www.w3.org/2005/Incubator/webid/spec/

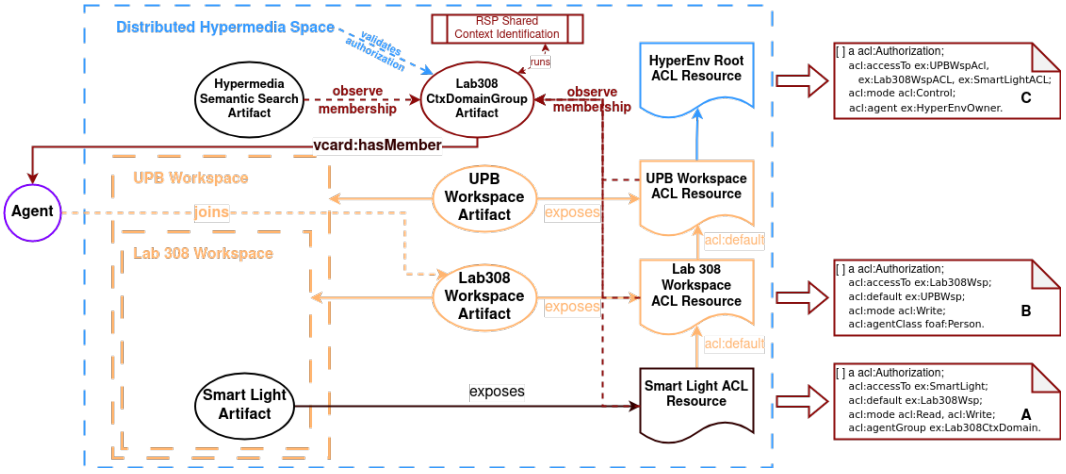

Figure 2: Summarized view of WAC usage based on shared *ContextDomain* for typical artifact instances - Thing, Workspace, Semantic Search Engine - encountered in a Hypermedia MAS Environment.

The logical hierarchy of an A&A based HMAS straightforwardly facilitates the WAC *effective authorization* determination mechanism. Workspaces enable inclusive access (any agent having a FOAF profile) by default (item B. in Fig 2), while individual artifacts dynamically restrict access based on ContextDomain membership (item A. in Fig 2). Control for change in access control policies is defined at HMAS environment level (item C. in Fig 2). The HMAS platform facilitates the *validation* of a context-based authorization for all HMAS resources that use a context-based access. It does so by running a federated SPARQL query against all *ContextDomain Groups* observed by a HMAS resource).

```
PREFIX ...
REGISTER STREAM <SharedLab308Context> AS
CONSTRUCT ISTREAM {
    precis:lab308group vcard:member ?agent .
}
FROM NAMED :staticAssertions
FROM NAMED :profiledAssertions
FROM NAMED WINDOW :pLoc [RANGE PT10S STEP PT10S] ON STREAM :PersonLocated
WHERE
{
    GRAPH :staticAssertions { ?agent rdf:type foaf:Person . }
    GRAPH :profiledAssertions {
        ?worksAssertion a precis:WorksAt ;
            consert:assertionSubject ?agent ;
            consert:assertionObject precis:upb ;
            ann:hasAnnotation ?validAnn .
        ?validAnn a ann:TemporalValidityAnnotation ;
            ann:startTime ?employmentStart ;
            ann:endTime ?employmentEnd .
    }
    WINDOW :pLoc {
        ?persLocAssertion a precis:LocatedAt;
            consert:assertionSubject ?agent ;
            consert:assertionObject precis:lab308 .
    }
    BIND (xsd:dateTime(NOW()) AS ?date)
    FILTER (?date > ?employmentStart && ?date < ?employmentEnd)
}
```

Listing 1: Demonstrator scenario shared context identification query

4. Conclusion

CASHMERE exploits a technological fit to offer a modular solution for context-based access authorization in A&A HMAS platforms, using a flexible context-representation method (CONSERT), a time-aware *shared context* identification method (RSP using C-SPARQL) and an authorization representation and validation mechanism following SOLID WAC specifications.

Acknowledgments

This work has been supported by funding under grant agreement PN-III-P1-1.1-PD-2021-0756 from the Romanian National Research, Development and Innovation Plan.

References

[1] A. Ciortea, O. Boissier, A. Ricci, Engineering world-wide multi-agent systems with hypermedia, in: Engineering Multi-Agent Systems: 6th International Workshop, EMAS 2018, Stockholm, Sweden, July 14-15, 2018, Revised Selected Papers 6, Springer, 2019, pp. 285–301.

[2] A. Ricci, M. Piunti, M. Viroli, Environment programming in multi-agent systems: an artifact-based perspective, Autonomous Agents and Multi-Agent Systems 23 (2011) 158–192.

[3] D. Vachtsevanou, A. Ciortea, S. Mayer, J. Lemée, Signifiers as a first-class abstraction in hypermedia multi-agent systems, arXiv preprint arXiv:2302.06970 (2023).

[4] A. K. Dey, Understanding and using context, Personal and ubiquitous computing 5 (2001) 4–7.

[5] A. Sorici, G. Picard, O. Boissier, A. Zimmermann, A. Florea, Consert: Applying semantic web technologies to context modeling in ambient intelligence, Computers & Electrical Engineering 44 (2015) 280–306.

[6] A. Sorici, G. Picard, O. Boissier, A. Florea, Multi-agent based flexible deployment of context management in ambient intelligence applications, in: Advances in Practical Applications of Agents, Multi-Agent Systems, and Sustainability: The PAAMS Collection: 13th International Conference, Proceedings 13, Springer, 2015, pp. 225–239.

[7] D. F. Barbieri, D. Braga, S. Ceri, E. D. VALLE, M. Grossniklaus, C-sparql: a continuous query language for rdf data streams, International Journal of Semantic Computing 4 (2010) 3–25.

[8] D. Dell'Aglio, E. Della Valle, J.-P. Calbimonte, O. Corcho, Rsp-ql semantics: A unifying query model to explain heterogeneity of rdf stream processing systems, International Journal on Semantic Web and Information Systems (IJSWIS) 10 (2014) 17–44.