Middleware Support for Non-repudiable Business-to-Business Interactions

Nick Cook
School of Computing Science, Newcastle University, UK

PhD Thesis Extended Abstract

The wide variety of services and resources available over the Internet presents new opportunities for organisations to collaborate to achieve common goals. For example, business partners wish to access each other's services and share information along the supply chain in order to compete more successfully in the delivery of goods or services to the ultimate customer. This can lead to the investment of significant resources by business partners in the resulting collaboration. In the context of such high value business-to-business interactions (B2B) interactions, it is desirable to regulate (monitor and control) the behaviour of business partners to ensure that they comply with agreements that govern their interactions. While cooperating on agreed undertakings, organisations will continue to act autonomously and are likely to privilege their own interests over those of their business partners. This can lead to tension between the need for cooperation and the need of each business partner to protect their own interests. In this context, we assume that each business partner has a set of local policies that they wish to enforce and that there are one or more agreements between partners for the conduct of their interactions. Examples of agreements include natural language contracts that govern business collaborations, agreements that specify acceptable service provision and usage, and the specification of the correct execution of cross-organisational processes or workflows to achieve some common goal. To resolve the tension between cooperation and autonomy, it is desirable to regulate B2B interactions so that they comply with the agreements between business partners. At the same time, businesses should be able to enforce their own policies. Such enforcement should include accountability for actions performed. That is, it should not be possible to subsequently deny having requested some service or having modified shared information. If actors are not accountable for their actions, then agreements are unenforceable. So, there are two aspects to achieving regulation in the context of high-value B2B interactions:

1. high level mechanisms to specify contractual rights and obligations and to derive an electronic embodiment of contractual conditions for the validation of observed behaviour, and
2. lower level mechanisms that record observed behaviour — generating a non-repudiable audit trail of an interaction and verifying that the observed behaviour is valid with respect to the electronic embodiment of interaction agreements.

The work presented in this dissertation addresses the latter aspect of regulation by providing support for the run-time validation and non-repudiation of B2B interactions. An interaction is non-repudiable if the parties to the interaction cannot subsequently deny their participation. A related concern is that well-behaved parties should not suffer disadvantage because of the misbehaviour, or non-cooperation, of their business partners. Thus, accountability can extend to supporting fair outcomes to parties who comply with agreements.

The main contribution of this work is the design and implementation of flexible middleware to support the non-repudiation and validation of B2B interactions. Two non-repudiation
services are defined — non-repudiable service invocation and non-repudiable information sharing — that address requirements in two domains for action: (i) over private resources that are exposed as services to business partners and (ii) over shared (or jointly owned) resources.

Non-repudiable service invocation

Figure 1 Service invocation

Figure 1 shows a typical two-party, client-server interaction. The client invokes a service by sending a request to the server. The server then issues a response. For non-repudiable service invocation, we wish to generate irrefutable evidence that the interaction took place and to validate both request and response with respect to contract (however defined). To this end, client and server execute non-repudiation protocol to exchange evidence of the interaction and to ensure that:

1. a request is only passed to the server if: (i) the client provides evidence for the non-repudiation of origin of the request (NROreq), (ii) the request is valid with respect to contract, as indicated by non-repudiation of validation of the request (NRVreq), and (iii) the server provides evidence for the non-repudiation of receipt of the request (NRRreq), and
2. a response is only passed to the client if: (i) the server provides evidence for the non-repudiation of origin of the response (NROresp), (ii) the response is valid with respect to contract, as indicated by non-repudiation of validation of the response (NRVresp), and (iii) the client provides evidence for the non-repudiation of receipt of the response (NRRresp).

Figure 2 Non-repudiable service invocation

Figure 2 is a logical view of the exchange of evidence that is achieved by the execution of an appropriate non-repudiation protocol. It shows the minimum requirements for the evidence that must be generated and exchanged during a request/response service invocation.

Figure 3 Interceptor-mediated service invocation

The aim of the proposed service for non-repudiable and validated service invocation is to preserve the abstraction shown in Figure 1 and at the same time generate and exchange the evidence shown in Figure 2. As shown in Figure 3, this is achieved by using middleware-provided interceptors on the invocation path between client and server.
Non-repudiable information sharing

The primary concern with respect to information sharing is the maintenance of the integrity information that is shared between application processes at two or more collaborating organisations. We wish to hold organisations to account for their actions with respect to shared information. As with service invocation, this leads to the need to collect non-repudiation evidence of those actions and their validity with respect to agreements that determine which actions are legitimate. Conceptually, shared information resides in a shared space. The members of the sharing group act upon the information in the shared space. They can observe each other's actions and subject those actions to validation. Thus, the shared space is an abstraction that presents the agreed view of the information.

Figure 4 Information sharing

Figure 4 shows three organisations (A, B and C) that have access to and can update information in a shared space. If A wishes to update the information, then, to meet regulatory requirements, they must reach agreement with B and C on the validity of their proposed update. For the agreement to be non-repudiable:

1. B and C require evidence that the update originated at A, and
2. A, B and C require evidence that, after reaching a decision on the update, all parties have the same (agreed) view of the state of the shared information.

The latter condition implies that there must be evidence that all parties received the update and that they all agreed to the update being applied to the information.

Figure 5 Non-repudiable information sharing

Figure 5 shows the exchange of evidence required to achieve the irrefutable, agreed transition from information state \( s \) to information state \( s+1 \). First A proposes an update to both B and C. As shown, A also provides evidence of the origin of the update (NRO). Then B and C each provide evidence of receipt of the update (NRR) and their non-repudiable decision on the validity of the update (NRV\(_B\) and NRV\(_C\), respectively). Finally, A relays the group decision to B and C by sending them the collected validation tokens and A's non-repudiation of receipt of the validation evidence (NRRV). If the validation tokens represent unanimous agreement to
the change, then the consistent shared view of the information after the exchange of evidence is that it is now in state \( s+1 \) (as shown in Figure 5). Otherwise, the update is considered invalid and the shared view of the information is that it is in state \( s \).

![Diagram of Interceptor-mediated information sharing](image)

**Figure 6 Interceptor-mediated information sharing**

The overall aim of the proposed service for non-repudiable and validated information sharing is similar to that for service invocation: to preserve the abstraction shown in Figure 4 and at the same time generate and exchange the evidence shown in Figure 5. As shown in Figure 6 middleware-provided interceptors are used to achieve this and to execute the necessary non-repudiation protocols.

**Summary of contributions**

The core of the work in the dissertation comprises:

1. the definition of the non-repudiation services based on fundamental work on protocols for the exchange of non-repudiation evidence,
2. the design and implementation of a generic framework for protocol execution, and
3. the demonstration of the practical implementation of the non-repudiation services using the protocol execution framework.

Taken together, this work addresses requirements for: non-repudiation, no unfair advantage, application-specific validation, flexibility and transactional information sharing. A notable feature of the approach taken is the careful separation of concerns. Application-level abstractions are maintained by the realisation of the non-repudiation services as middleware. The application-independent middleware itself is separated into three layers: a protocol-independent layer to address non-repudiation service specific issues, a layer for deployment of protocol implementations and a protocol-independent layer for B2B communications. This separation is fundamental to the flexibility of the middleware. Mechanisms to provide non-repudiation and validation of interactions are independent of the applications to which they apply and yet can be adapted to a specific application context. Protocol-specifcics do not leak into the abstractions provided by the non-repudiation services nor into the communications interface between organisations. Thus, different protocols can be deployed to suit different requirements. The separation of concerns is expressed in the middleware through the specification of APIs for interaction with and between the different middleware components. So, there is a well-defined interface between each middleware layer, including the
specification of self-describing protocol messages for processing by the middleware. A support service API isolates implementation detail of the necessary supporting infrastructure. A data-binding API supports the distinction between the local representation of data and its agreed representation in non-repudiation evidence and, in particular, as shared information. The definition of an API for validation and event listeners allows the application programmer to adapt the middleware to application-specific requirements and to customise the rules that are applied in different interaction contexts.

In summary, through a unified approach to the development of middleware support for non-repudiation and validation of B2B interactions, the thesis establishes:

1. that a set of middleware services can provide a flexible framework for protocol-based interaction,
2. that the framework can deliver non-repudiation services that are appropriate to the two domains for action — the private and the shared, and
3. that the services can be used to regulate B2B interactions and at the same time preserve application-level semantics.