Perfis de Acesso baseados em Tópicos para Simulação Distribuída HLA

Henrique O. Gressler [1], **Alexandre C. Brites** [2], **Raul Ceretta Nunes** [2]

[1]Centro de Desenvolvimento de Sistemas (CDS) – Exército Brasileiro (EB)
Brasília, DF – Brasil

[2]Centro de Tecnologia – Universidade Federal de Santa Maria (UFSM)
Santa Maria, RS – Brasil

gressler.henrique@eb.mil.br, {acbrites, ceretta}@inf.ufsm.br

Abstract. *One of the main characteristics of distributed simulations that use the IEEE 1516-2010 communication standard - High-Level Architecture (HLA) - is that all communicated information is accessible to all interested participants. This characteristic represents a security vulnerability, especially in simulation exercises involving multiple nations or distinct attack and defense teams, such as simulated military exercises. While HLA provides services that standardize and optimize data access, there is no standardized way to control access to sensitive data transmitted within the distributed simulation environment. This paper presents a new approach for implementing data access authorization in an HLA-based distributed simulation, where the use of topic-based access profiles in the HLA middleware message distribution is explored. Experiments conducted with the Portico open-source middleware demonstrate that the proposed approach ensures security and optimizes data access by limiting data delivery per profile through a pre-configured security policy.*

Resumo. *Uma das principais características das simulações distribuídas que utilizam o padrão de comunicação IEEE 1516-2010 - High Level Architecture (HLA) é a de que todas as informações comunicadas estão acessíveis a todos os participantes interessados. Essa característica representa uma vulnerabilidade de segurança, especialmente em exercícios de simulação envolvendo múltiplas nações ou times distintos de ataque e defesa, tal como em exercícios militares simulados. Embora o HLA forneça serviços que padronizam e otimizam o acesso aos dados, não há uma forma padronizada para controlar o acesso a dados sensíveis que trafegam no ambiente de simulação distribuída. Este trabalho apresenta uma nova abordagem para autorização de acesso a dados em uma simulação distribuída HLA, onde é explorada a utilização de perfis de acesso baseados em tópicos na distribuição de mensagens do middleware do HLA. Experimentos realizados com o middleware Portico (open source) demonstram que a abordagem proposta garante segurança e otimiza o acesso aos dados, limitando a entrega de dados por perfil via políticas de segurança.*

1. Introdução

A Simulação Distribuída (SD), também conhecida como *Distributed Simulation* (DS), é uma técnica em que múltiplos componentes ou simuladores, possivelmente dispersos

geograficamente, trabalham de forma coordenada para modelar sistemas ou fenômenos complexos [Taylor 2019]. No campo militar, em particular, essa estratégia se mostra fundamental para permitir cooperação entre diferentes forças, podendo envolver exércitos de múltiplas nações, equipes de ataque e defesa ou diversos órgãos governamentais. Nesse contexto, o padrão IEEE 1516-2010 - High Level Architecture (HLA) [IEEE 2010b] define uma infraestrutura que viabiliza essa integração. Assim, componentes executados em computadores diferentes mantêm a comunicação com os demais em um cenário de simulação compartilhado [Morlang and Strassburger 2022, Falcone et al. 2017]. No HLA, uma SD é chamada de federação e é composta por aplicativos de simulação chamados federados. Os federados interagem entre si, por meio da *Run-Time Infrastructure* (RTI), que implementa as especificações e regras da interface HLA, e funciona como um *middleware* de comunicação, assegurando a interoperabilidade entre os componentes da SD [Akram et al. 2019].

Entretanto, o HLA tem uma característica que gera preocupação do ponto de vista de segurança: todas as informações publicadas RTI podem ser potencialmente recebidas por qualquer federado que simplesmente as assine. Essa "abertura" contraria cenários em que dados sensíveis não devem ser revelados a todos os participantes, como em treinamentos militares conjuntos que envolvem informações classificadas (táticas, doutrinas, capacidades de armamento, entre outras). Na ausência de um mecanismo de segurança nativo, o risco de vazamento de informações aumenta, podendo comprometer o realismo ou mesmo a viabilidade de simulações que exigem restrições de acesso [Slaghenaufi et al. 2019, Möller et al. 2012].

Alguns serviços disponibilizados na RTI, como o *Declaration Management* (DM) e o *Data Distribution Management* (DDM) implementam técnicas para realizar a filtragem de dados. Esses serviços, no entanto, têm foco em reduzir o fluxo de dados entre os federados. Não há definições e implementações de segurança na versão atual do HLA [IEEE 2010b], que foi concebido para ser utilizado em um domínio seguro. A ausência de definições de segurança limita a capacidade de realizar simulações seguras em ambientes distribuídos, especialmente quando há requisitos técnicos de segurança [Falcone and Garro 2023].

Nesse contexto, este trabalho apresenta o *Topic-Based Access Profile* (TBAP) como uma abordagem capaz de incorporar políticas de controle de acesso diretamente na infraestrutura de simulação HLA. Inspirada nos modelos de controle de acesso baseados em papéis (*Role-Based Access Control*, ou RBAC) [Sandhu 1998] e em tópicos (*Topic-Based Access Control*, ou TBAC) [Nakamura et al. 2018], a solução consiste em associar cada federado a um perfil de acesso que descreve, de forma granular, quais dados (tópicos) podem ser publicados ou assinados. Uma vez que o TBAP filtra internamente as chamadas e as entregas de dados na RTI, os federados só recebem (ou podem publicar) informações condizentes com suas permissões.

A principal contribuição do trabalho é demonstrar que o TBAP viabiliza um mecanismo de autorização no âmbito de uma mesma federação HLA, sem exigir modificações nos federados ou adoção de ferramentas externas, diferentemente de soluções que atuam como pontes (bridge) [Slaghenaufi et al. 2019] entre federações ou que demandam proxies [Andrews et al. 2008] intermediários. Os experimentos de funcionalidade realizados com o Portico [OpenVLC 2016] – uma RTI de código aberto – evidenciam a praticidade

dessa solução, embora métricas de desempenho (tempo, memória, escalabilidade) sejam objeto de trabalhos futuros.

Este artigo está organizado como segue: na Seção 2, são apresentados conceitos fundamentais para compreensão do trabalho. Os trabalhos relacionados são discutidos na Seção 3. A Seção 4 descreve em detalhes a proposta do TBAP, incluindo sua definição, mapeamento de tópicos e forma de integração à RTI. Na Seção 5, são apresentados experimentos de funcionalidade que demonstram a eficácia do TBAP no controle do fluxo de dados. Por fim, a Seção 6 traz as considerações finais, discutindo limitações, aplicações práticas e extensões futuras do trabalho.

2. Referencial

Nesta seção, são apresentados os conceitos essenciais para compreender o desenvolvimento da abordagem de controle de acesso em simulações distribuídas usando o padrão HLA. Primeiramente, descreve-se a ideia geral de Simulação Distribuída e suas aplicações. Em seguida, discute-se o funcionamento do padrão HLA, com ênfase nos serviços de comunicação que permitem a interação entre simuladores (federados). Por fim, são abordadas questões relacionadas à segurança, incluindo a limitação dos recursos nativos de controle de acesso do HLA, bem como a importância de mecanismos adicionais para proteger dados sensíveis.

2.1. Simulação Distribuída

A SD consiste em integrar diversos componentes de simulação que, embora possam ser executados em locais distintos ou em diferentes computadores, compartilham um cenário comum. Cada componente (ou "simulador") é responsável por parte do ambiente, como o comportamento de entidades, regras de física ou modelos de eventos. Quando esses simuladores trocam dados em tempo real (ou quase real), cria-se uma visão unificada do sistema ou fenômeno em estudo [Taylor 2019].

No contexto militar, a Simulação Distribuída é usada para exercícios que envolvem múltiplas forças, simulando ações de ataque e defesa em cenários complexos. Em vez de concentrar toda a lógica em um único supercomputador, divide-se a simulação em vários módulos, cada um desempenhando um papel específico. Esse método aumenta a escalabilidade e a flexibilidade, permitindo que novas entidades ou cenários sejam adicionados sem grandes alterações na arquitetura [Slaghenaufi et al. 2019, Möller et al. 2012].

2.2. O Padrão HLA

O High Level Architecture (HLA) é uma arquitetura genérica voltada a promover interoperabilidade e reusabilidade em simulações distribuídas, padronizada pelo IEEE inicialmente em 2000 e revisada na versão IEEE 1516-2010 [Taylor 2019]. O padrão HLA fornece um modelo de referência que permite que diferentes aplicações de simulação trabalhem de forma conjunta dentro de um ambiente compartilhado. Esse padrão inclui: a definição do *framework* e suas regras [IEEE 2010b], a especificação da interface [IEEE 2010a], as definições de dados [IEEE 2010c], além de um processo de desenvolvimento [IEEE 2022], revisado em 2022.

No HLA, cada aplicação participante é denominada federado, enquanto o conjunto desses federados forma uma federação. Para viabilizar o intercâmbio

de dados entre esses federados, o HLA define a *Run-Time Infrastructure* (RTI) [Morlang and Strassburger 2022, IEEE 2010a], que atua como um *middleware* de comunicação. A RTI oferece diversos serviços classificados em grupos, como:

- ***Federation Management***: criar ou destruir federações, além de gerenciar a participação de cada federado.
- ***Declaration Management* (DM)**: possibilita que cada federado anuncie quais dados deseja publicar ou assinar.
- ***Object Management***: permite gerenciar as instâncias de objetos compartilhados na federação (criação, atualização, remoção).
- ***Ownership Management***: controla quem "detém" a capacidade de atualizar certos atributos de objeto.
- ***Time Management***: coordena o avanço de tempo lógico entre federados, útil em cenários onde a ordem de eventos é crítica.
- ***Data Distribution Management* (DDM)**: oferece meios de filtrar o envio de dados, aliviando a carga de rede em simulações de grande porte.

A comunicação segue o paradigma *publish/subscribe*, ou seja, um federado publica dados que podem ser assinados (subscritos) por outros. Essa comunicação baseia-se em duas formas principais de dados [IEEE 2010c]:

- **Classes de objeto**: entidades persistentes, com atributos que podem ser atualizados ao longo do tempo (por exemplo, aeronaves, veículos terrestres, sensores).
- **Classes de interação**: eventos efêmeros, que transportam parâmetros no momento em que ocorrem (por exemplo, lançamento de míssil ou mudança de estado operacional).

Todas essas definições ficam documentadas em um arquivo chamado *Federate Object Model* (FOM), que descreve cada classe de objeto, cada interação e os respectivos atributos e parâmetros [IEEE 2010c].

A versão IEEE 1516-2010 do HLA não define mecanismos nativos de autenticação ou autorização de federados, assumindo que todos operam em um "domínio seguro". Essa suposição nem sempre condiz com cenários reais, principalmente em simulações militares conjuntas. Pesquisas a respeito da nova versão "HLA 4" [Möller et al. 2021] indicam que recursos de segurança para autorização de federados serão incluídos. No entanto, embora o HLA 4 tenha sido aprovado pela IEEE em fevereiro de 2025 [SISO 2025], um anúncio oficial ainda é aguardado e a versão amplamente utilizada ainda é a IEEE 1516-2010, também conhecida como HLA Evolved.

Como consequência, se um federado assina um atributo de determinada classe de objeto, ele passa a receber todas as atualizações dos atributos de todas as instâncias daquela classe, mesmo que parte dessas instâncias não devesse ser de seu conhecimento. Embora esse seja o comportamento esperado para o HLA, gera riscos em exercícios que envolvem dados sensíveis, como informações sobre capacidades de armamentos, doutrinas de emprego ou posicionamento de tropas [Slaghenaufi et al. 2019].

2.3. Mecanismos de Filtragem: DM e DDM

Para reduzir o volume de dados trafegados, o HLA traz os serviços de *Declaration Management* (DM) e *Data Distribution Management* (DDM) [IEEE 2010a]:

- **DM** permite que cada federado declare apenas as classes de objeto e classes de interação que deseja publicar ou assinar, reduzindo o envio de dados irrelevantes.
- **DDM** oferece uma filtragem mais detalhada, baseada em valores de atributos ou parâmetros. Ele permite especificar "regiões" numéricas, de modo que o envio de dados ocorra apenas quando há sobreposição de regiões definidas pelos publicadores e assinantes.

Esses recursos melhoram a escalabilidade e o desempenho, mas não solucionam o problema de "quem pode ver o quê" em termos de confidencialidade. Eles focam em eficiência, não em segurança.

2.4. Segurança de Dados Sensíveis

O uso de simulações militares conjuntas exemplifica por que a segurança é crucial. Tais cenários podem envolver múltiplas nações ou forças, cada qual com níveis distintos de classificação de informação. Alguns dados podem ser amplamente compartilhados (ex.: posição básica de tropas amigas), enquanto outros devem ficar restritos (ex.: estratégias de ataque, capacidades de armamentos). Em exercícios de treinamento, mesmo dados aparentemente "inocentes" podem revelar doutrinas ou capacidades reais, se analisados em conjunto [Möller et al. 2012].

2.5. Modelos de Controle de Acesso

Para criar uma camada de segurança dentro do ambiente HLA, pode-se recorrer a modelos de controle de acesso consolidados:

- ***Role-Based Access Control* (RBAC)** [Sandhu 1998]: privilegia a ideia de "papéis" (ou perfis). Um usuário herda direitos conforme o papel que desempenha na organização. É muito usado em sistemas corporativos, onde "Administrador", "Analista" ou "Usuário" definem concessões de acesso.
- ***Topic-Based Access Control* (TBAC)** [Nakamura et al. 2018]: pensado para sistemas *publish/subscribe*. Em vez de papéis, define "tópicos" como base de autorização. Esse modelo é útil em arquiteturas de mensageria, pois cada tópico corresponde a um canal de informação específico.

Esses modelos de controle de acesso fornecem uma base conceitual sólida para soluções que demandam gerenciamento flexível e granular de permissões em ambientes distribuídos.

2.6. Considerações finais

Esta seção apresentou uma visão geral da Simulação Distribuída, detalhou o funcionamento do HLA e suas limitações de segurança, além de descrever os mecanismos de filtragem e os modelos de controle de acesso que servem de base para o TBAP. Essas discussões demonstram a necessidade de uma camada adicional de controle de acesso na federação, que será explorada na proposta do TBAP.

3. Trabalhos relacionados

A crescente necessidade de segurança em SD, especialmente em treinamentos militares conjuntos, envolvendo diferentes nações foi abordada por [Slaghenaufi et al. 2019], onde

foi proposta uma arquitetura de segurança que combina uma ponte, que conecta duas federações, e um filtro, que sanitiza dados classificados antes de sua transmissão. O filtro proposto opera em dois níveis. O primeiro deles é relacionado ao *Federation Object Model* (FOM), modelo que define as classes de objetos e classes de interações que a simulação deve utilizar. Diferentes federações podem usar uma combinação de diferentes FOM. Dessa forma, o primeiro filtro garante que apenas dados acordados e reconhecidos por ambas as federações possam ser enviados. O segundo nível do filtro atua sobre atributos e parâmetros que podem conter informações classificadas ou sensíveis. Para as federações envolvidas, a ponte-filtro é vista como um federado que subscreve dados e os publica em outra federação (após o filtro), ou um federado que publica dados que subscreveu em outra federação. Enquanto a solução ponte-filtro oferece uma abordagem para evitar o vazamento de dados entre federações distintas, o TBAP proposto neste trabalho implementa um mecanismo de controle de acesso aos dados pelos federados, no âmbito de uma federação, diretamente na RTI, permitindo criar regras que restringem o envio e o recebimento de dados em uma simulação distribuída HLA.

Ao utilizar tópicos como unidade lógica de interesse, [Falcone and Garro 2023] apresentaram o *Topic-Based Publish-Subscribe Messaging System* (TBMS), concebido para otimizar o serviço de DDM do HLA. O TBMS substitui a verificação tradicional de sobreposição de regiões por um algoritmo de correspondência baseado em tópicos, o *Topic-Based Matching* (TBM), que canaliza as publicações para filas intermediárias e as distribui por meio de um *exchange* (componente responsável pelo encaminhamento). O trabalho evidenciou que o particionamento por tópicos é útil não apenas para melhorar o desempenho, mas também para decidir o encaminhamento dos dados. Essa constatação serviu de inspiração direta para o mecanismo proposto neste artigo: se tópicos permitem identificar quem requer determinado dado, eles também podem fundamentar regras que definam quem pode recebê-lo. Assim, o TBAP herda do TBMS a ideia de organizar o fluxo de informações em tópicos e estende-a com políticas de autorização que restringem publicações e assinaturas de forma granular.

Com o objetivo de oferecer controle de acesso em sistemas *publish/subscribe* (PS), especialmente no contexto de *peer-to-peer* (P2P), [Nakamura et al. 2018] propuseram o modelo TBAC. Neste modelo, as permissões são gerenciadas com base em tópicos específicos, que são os temas ou categorias de informação que os *peers* podem publicar ou assinar. No TBAC, cada *peer* tem direitos de acesso que determinam quais tópicos eles podem acessar e quais operações podem executar. O modelo é bastante útil em ambientes em que há muitos publicadores e assinantes, pois permite controle detalhado sobre quem pode acessar quais informações.

Neste trabalho, os conceitos do modelo TBAC foram adaptados para a arquitetura do HLA. O perfil é definido como um conjunto de regras de acesso e, tal como no modelo RBAC em que uma *role* pode ser atribuída a um usuário, no TBAP um perfil pode ser atribuído a um federado. O controle do fluxo das mensagens fica a cargo do *middleware* que implementa o TBAP, neste caso, o RTI da arquitetura HLA.

4. Topic-Based Access Profile - TBAP

Nesta seção apresentamos o TBAP, uma abordagem para implementar autorização de acesso a dados em uma simulação distribuída HLA. A principal motivação para o desen-

volvimento do TBAP é a necessidade de oferecer controle de acesso granular aos dados compartilhados entre os federados em um ambiente de simulação distribuída, onde, no modelo tradicional HLA, todos os participantes têm acesso a todos os dados, bastando para isso, assiná-los. Essa característica pode ser vista como uma vulnerabilidade de segurança, especialmente quando diferentes federados pertencem a diferentes entidades ou têm papéis distintos, como em simulações militares envolvendo equipes de ataque e defesa, ou exercícios militares de cooperação entre nações. O TBAP foi projetado para resolver esse problema, proporcionando uma maneira de limitar o acesso aos dados a apenas aqueles federados que têm permissão para acessá-los, utilizando perfis de acesso configurados previamente em políticas de segurança.

4.1. Definição formal do TBAP

Formalmente, o TBAP pode ser definido da seguinte maneira:

Seja $OP = \{pb, sb\}$ o conjunto das operações, onde pb refere-se à operação de publicação de dados e sb refere-se à operação de subscrição de dados em tópicos específicos. Seja $T = \{t_0, t_1, ..., t_n\}$ o conjunto de tópicos e $F = \{f_0, f_1, ..., f_n\}$ o conjunto de federados em uma simulação HLA. Cada federado pode publicar ou subscrever dados relacionados a um ou mais tópicos.

Chamamos o par $\langle t, op \rangle$ de direito de acesso, e a um conjunto de direitos de acesso, damos o nome de perfil. Quando um perfil é atribuído a um federado f, temos um conjunto de regras de acesso do tipo $\langle f, t, op \rangle$. Essas regras são utilizadas pelo TBAP para definir a política de acesso do federado e filtrar as mensagens trocadas com a RTI, garantindo que cada federado f execute uma operação op em um tópico t apenas se existir uma regra $\langle f, t, op \rangle$ previamente definida em sua política de acesso.

4.2. Arquitetura e configuração do TBAP

A arquitetura tradicional do HLA (sem o TBAP) pode ser visualizada na Figura 1. Nela, cada federado interage com a RTI diretamente por meio dos componentes Embaixador do Federado e Embaixador da RTI, sem nenhum mecanismo intermediário de controle de acesso.

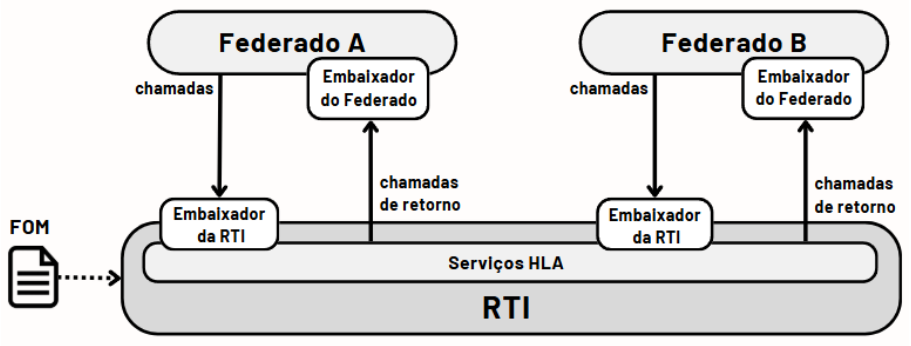


Figura 1. Arquitetura tradicional do HLA. Fonte: o autor.

Com o TBAP, introduzimos uma camada intermediária dentro da RTI, que monitora as chamadas dos federados para a RTI e as respectivas respostas. Essa camada é responsável por verificar as permissões dos federados segundo uma política de segurança

definida em um arquivo XML denominado `RTIPolicy.xml`, ilustrado na Figura 2. O arquivo especifica claramente quais federados são autorizados, quais perfis existem e como eles estão associados a cada federado. Além disso, para garantir a integridade da política, o *hash* (SHA256) desse arquivo é validado no momento da conexão dos federados.

```
<RTIpolicy name="NomeDaPolicy">
    <Federation name="NomeDaFederacao">
        <!-- Federados autorizados -->
        <allowedFederate name="NomeDoFederado1" />
        <allowedFederate name="NomeDoFederado2" />

        <!-- Perfis de acesso -->
        <federateProfile name="NomeDoPerfil1">
            <accessRight topic="HLAobjectRoot.Classe.*" op="pb" />
            <accessRight topic="HLAinteractionRoot.Interacao.*" op="sb" />
        </federateProfile>
        <federateProfile name="NomeDoPerfil2">
            <accessRight topic="HLAobjectRoot.Classe.*" op="pb,sb" />
            <accessRight topic="HLAinteractionRoot.Interacao.*" op="pb,sb" />
        </federateProfile>

        <!-- Atribuição de perfis -->
        <profileAssign federate="NomeDoFederado1" profile="NomeDoPerfil1" />
        <profileAssign federate="NomeDoFederado2" profile="NomeDoPerfil2" />
    </Federation>
</RTIpolicy>
```

Figura 2. Arquivo de configuração da política de acesso. Fonte: o autor.

A Figura 3 ilustra a nova arquitetura do HLA com o TBAP integrado. Observa-se claramente que a camada adicional do TBAP é posicionada estrategicamente entre o Embaixador do Federado e o Embaixador da RTI, interceptando e analisando todas as comunicações.

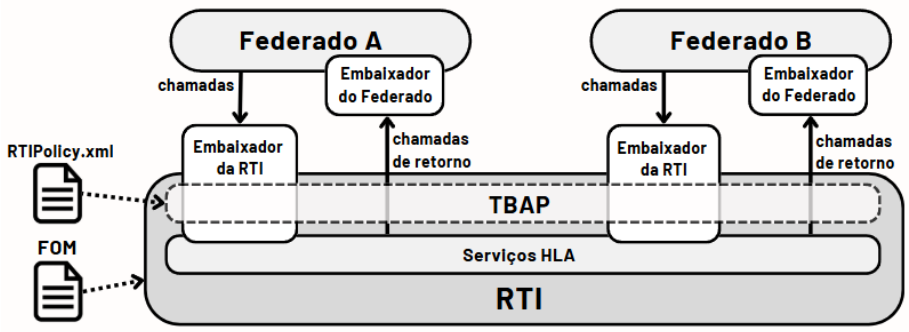


Figura 3. RTI HLA com TBAP implementado. Fonte: o autor.

4.3. Integração do TBAP a Portico

O TBAP foi implementado no Portico, uma RTI de código aberto compatível com o padrão HLA e distribuída sob a licença CDDL[1]. O processo de integração baseou-se na modificação interna da biblioteca do Portico, permitindo a inclusão de verificações antes da entrega das atualizações de atributos e interações aos federados.

A integração técnica ocorreu da seguinte forma:

[1]A *Common Development and Distribution License* (CDDL) é uma licença de código aberto criada originalmente pela Sun Microsystems, sendo aprovada pela *Open Source Initiative* (OSI). Ela permite modificação e redistribuição do software.

- O TBAP foi implementado por meio da criação das classes responsáveis por carregar e gerenciar os perfis definidos no arquivo `RTIPolicy.xml`.
- As classes utilizam estruturas internas baseadas em mapas (*hashMaps*) para indexar rapidamente quais federados possuem permissão para publicar ou subscrever determinados tópicos.
- O núcleo do TBAP foi integrado às chamadas internas do Portico, particularmente aos métodos responsáveis por publicar e distribuir atualizações de atributos e interações (interface RTIambassador) e métodos responsáveis por acionar as *callbacks* (interface FederateAmbassador).
- Durante a execução da simulação, o TBAP intercepta as mensagens e avalia o conteúdo confrontando com o perfil do federado. Caso uma solicitação viole a política definida, a RTI simplesmente não entrega os dados ao federado solicitante, sem impactar os demais federados autorizados.

Essa integração transparente garante que os federados não necessitem de qualquer modificação para usufruir dos benefícios do TBAP. Além disso, promove fácil adoção em federações já existentes, apenas pela modificação pontual da biblioteca Portico.

5. Experimentos

Para demonstrar a funcionalidade e eficácia do TBAP, foi conduzido um conjunto de experimentos utilizando a RTI Portico com a implementação proposta (RTI-TBAP). Esta seção descreve o experimento principal, que ilustra o controle granular do fluxo de dados, além de testes adicionais que verificam o comportamento da RTI-TBAP em cenários não autorizados ou mal configurados.

5.1. Experimento principal: Filtragem por perfil de acesso

No experimento principal, uma federação foi configurada com quatro federados identificados como A, B, C e D. Cada federado tinha funções e direitos distintos:

- Federado A: Publica atributos de 8 veículos em movimento, assina atributos da estação de Comando e Controle (C2) e publica/assina interações;
- Federado B: Publica atributos da estação C2, assina atributos dos veículos e publica/assina interações;
- Federados C e D: Assinam atributos dos veículos, da estação C2 e interações da federação, porém com restrições diferentes impostas pelo TBAP.

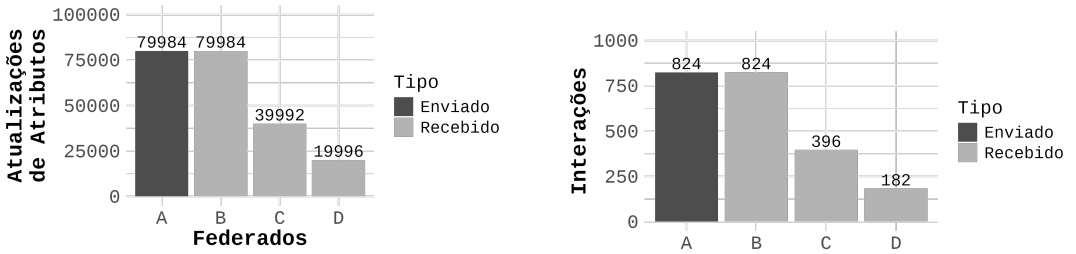
Em uma simulação HLA tradicional, todos os federados assinantes receberiam as mesmas quantidades de dados publicados. Ao utilizar o TBAP, perfis distintos foram definidos:

- Federados A e B receberam perfis com acesso completo aos dados de veículos e estação C2;
- Federado C recebeu acesso limitado a dados de apenas 4 dos 8 veículos simulados;
- Federado D recebeu acesso limitado a dados de apenas 2 veículos.

A política detalhada utilizada pode ser consultada em `https://bit.ly/4aN287a`.

A Figura 4a mostra que o Federado A enviou um total de 79.984 atualizações de atributos para a RTI, majoritariamente posições de veículos. O Federado B recebeu todas

as atualizações (79.984), enquanto os Federados C e D receberam apenas as quantidades de atualizações relativas aos veículos permitidos por seus perfis, ou seja, 39.992 e 19.996 atualizações, respectivamente. Este resultado confirma a eficácia do TBAP na filtragem por perfil.



(a) Atualizações de atributo enviadas e recebidas.

(b) Interações enviadas e recebidas.

Figura 4. Comparação do número de atualizações de atributos e interações enviadas e recebidas pelos federados. Fonte: o autor.

De maneira semelhante, a Figura 4b apresenta as interações enviadas pelo Federado A (824) e recebidas integralmente pelo Federado B. Os Federados C e D receberam apenas 396 e 182 interações, respectivamente, demonstrando também o controle granular sobre interações via TBAP.

5.2. Experimentos adicionais: Casos não autorizados

Para verificar a robustez do TBAP, foram conduzidos testes adicionais focados em cenários nos quais um federado tenta ingressar na federação sem estar previsto na política ou usando configurações incorretas. Os casos avaliados foram:

1. **Federado não autorizado:** Um federado foi inicializado com nome não listado na política de acesso. O resultado obtido foi uma exceção lançada pela RTI-TBAP, impedindo o ingresso do federado na federação.
2. **Federação não autorizada:** Um federado tentou ingressar em uma federação não prevista na política configurada. A RTI-TBAP retornou uma exceção também impedindo o ingresso.
3. **Configuração inconsistente:** Um federado utilizou um arquivo de configuração `RTIPolicy.xml` diferente daquele utilizado para inicializar a federação. A RTI-TBAP identificou a inconsistência por meio da validação do *hash* SHA256 do arquivo e lançou uma exceção rejeitando a conexão do federado.

Esses testes adicionais confirmaram que o TBAP atua de maneira proativa, evitando que federados mal configurados ou não autorizados possam acessar dados sensíveis da federação.

5.3. Considerações sobre os experimentos

Os experimentos conduzidos confirmam que o TBAP fornece um mecanismo eficaz para controle granular de acesso a dados em simulações distribuídas HLA. Além disso, os testes de robustez demonstram que a solução previne conexões inadequadas ou não autorizadas, fortalecendo a segurança da infraestrutura de simulação.

6. Considerações finais

Este trabalho apresentou o TBAP como uma solução para implementar uma camada adicional de segurança em simulações distribuídas baseadas no padrão HLA. Os experimentos realizados comprovaram a eficácia do TBAP na implementação de perfis de acesso, permitindo controlar de forma granular quais dados cada federado pode receber. Ao contrário da abordagem tradicional do HLA, onde todos os participantes têm acesso irrestrito às atualizações de atributos e interações publicadas, bastando para isso assiná-las, o TBAP garante que os federados recebam apenas os dados autorizados por seus perfis.

Além disso, os testes adicionais demonstraram que o TBAP é robusto e eficaz em prevenir a conexão de federados não autorizados ou com configurações incorretas. Tal característica reforça a segurança operacional e protege a federação contra acessos não autorizados ou potenciais vazamentos de dados sensíveis.

Como resultado, o TBAP se mostra uma abordagem flexível, prática e eficiente para garantir a segurança em simulações distribuídas, especialmente em cenários militares ou em exercícios envolvendo múltiplas organizações com níveis variados de restrição de acesso a informações. Como trabalhos futuros, destaca-se a importância de investigar o impacto dessa camada de segurança sobre o desempenho da RTI, avaliando aspectos como latência, escalabilidade e consumo de recursos em simulações de larga escala.

7. Agradecimentos

Agradecemos ao Exército Brasileiro e ao seu Programa Estratégico do Exército ASTROS pelo apoio financeiro através do projeto SIS-ASTROS GMF (Convênio 898347/2020 e TED 20-EME-003-00).

Referências

Akram, A., Sarfraz, M., and Shoaib, U. (2019). Hla run time infrastructure: A comparative study. *Mehran University Research Journal of Engineering and Technology*.

Andrews, D., Wharington, J., and Stratton, D. (2008). Secproxy-a proposed security architecture for the hla. In *Simulation Technology and Training Conference Proceddings*. Citeseer.

Falcone, A. and Garro, A. (2023). A topic-based data distribution management for hla. In *Proceedings of the 13th International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH 2023)*, pages 186–193.

Falcone, A., Garro, A., Anagnostou, A., and Taylor, S. J. (2017). An introduction to developing federations with the high level architecture (hla). In *2017 Winter Simulation Conference (WSC)*, pages 617–631. IEEE.

IEEE (2010a). Ieee standard for modeling and simulation (m&s) high level architecture (hla)– federate interface specification. *IEEE Std 1516.1-2010 (Revision of IEEE Std 1516.1-2000)*, pages 1–378.

IEEE (2010b). Ieee standard for modeling and simulation (m&s) high level architecture (hla)– framework and rules. *IEEE Std 1516-2010 (Revision of IEEE Std 1516-2000)*, pages 1–38.

IEEE (2010c). Ieee standard for modeling and simulation (m&s) high level architecture (hla)– object model template (omt) specification. *IEEE Std 1516-2010 (Revision of IEEE Std 1516.2-2000)*, pages 1–110.

IEEE (2022). Ieee recommended practice for distributed simulation engineering and execution process (dseep. *IEEE Std 1730-2022 (Revision of IEEE Std 1730-2010)*, pages 1–74.

Möller, B., Croom-Johnson, S., Hartog, T., Huiskamp, W., Verkoelen, C., Jones, G., and Bennett, M. (2012). Security in nato collective mission training-problem analysis and solutions. In *Spring Simulation Interoperability Workshop 2012, 2012 Spring SIW, 26-30 March 2012, Orlando, FL, USA*, page 217.

Möller, B., Karlsson, M., Herzog, R., and Wood, D. (2021). Security in simulation-new authorization opportunities in hla 4. In *Proceedings of the 2021 Virtual Simulation Innovation Workshop*.

Morlang, F. and Strassburger, S. (2022). On the role of hla-based simulation in new space. In *2022 Winter Simulation Conference (WSC)*, pages 430–440. IEEE.

Nakamura, S., Ogiela, L., Enokido, T., and Takizawa, M. (2018). An information flow control model in a topic-based publish/subscribe system. *Journal of High Speed Networks*, 24(3):243–257.

OpenVLC (2016). The portico project. `http://porticoproject.org/`. Acessado em 22/03/2025.

Sandhu, R. S. (1998). Role-based access control. In *Advances in computers*, volume 46, pages 237–286. Elsevier.

SISO (2025). Hla 4 approved by ieee – simulation interoperability standards organization. `https://www.sisostandards.org/news/695782/HLA-4-Approved-by-IEEE.htm`. Acessado em 22/03/2025.

Slaghenaufi, X., Amaral, R. P., and Nunes, R. C. (2019). A combined structure for security in distributed simulation. In *2019 9th Latin-American Symposium on Dependable Computing (LADC)*, pages 1–4. IEEE.

Taylor, S. J. E. (2019). Distributed simulation: state-of-the-art and potential for operational research. *Eur. J. Oper. Res.*, 273:1–19.