Uma proposta de políticas de migração para sociedade de agentes

Vinicius Machado Pinto, Nicolas da Silva Jatoba, Nilson Mori Lazarin

[1]Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet/RJ)
Nova Friburgo, RJ – Brasil

{vinicius.pinto,nicolas.jatoba}@aluno.cefet-rj.br

nilson.lazarin@cefet-rj.br

Abstract. *A Multi-Agent System (MAS) is a society of agents that share the same environment and act autonomously to achieve their own goals, being able to cooperate or compete. Some of these societies may be open, and their agents may come and go freely. However, freely migrating agents can present security risks to the SMA, as an agent can be malicious. This work presents an approach that contributes to migration control, aiming to prevent communication or access by unauthorized agents. To this end, we propose an extension of the communicator agents architecture, implementing a firewall model for MAS.*

Resumo. *Um Sistema Multiagentes (SMA) é uma sociedade de agentes que compartilham um mesmo ambiente e agem de forma autônoma para atingir seus próprios objetivos, podendo cooperar ou competir. Essas sociedades podem ser abertas e seus agentes podem entrar e sair livremente. Entretanto, a livre migração de agentes pode apresentar riscos à segurança do SMA, visto que um agente pode ser mal-intencionado. Este trabalho apresenta uma abordagem para o controle migratório, visando impedir a comunicação ou acesso de agentes não autorizados. Para tal, propomos uma extensão da arquitetura dos agentes comunicadores, implementando um modelo firewall para SMA.*

1. Introdução

Sistemas Multiagentes (SMA) são uma classe de sistemas compostos por entidades autônomas, chamadas agentes, que compartilham um ambiente e interagem entre si para alcançar objetivos individuais ou coletivos. Esses agentes podem cooperar ou competir, criando uma dinâmica complexa e adaptativa dentro do SMA. No caso de SMA abertos, os agentes estão livres para se movimentar, criando desafios de segurança significativos para o SMA. A invasão de agentes maliciosos ou a ocorrência de acessos não autorizados podem comprometer o bom funcionamento do sistema e afetar a confiabilidade e integridade das interações entre os agentes [Hubner 1995, Alvares and Sichman 1997, Vila et al. 2007].

Este trabalho propõe uma abordagem para prevenir acessos indesejados e agentes maliciosos com base nas políticas de migração da sociedade dos agentes. Para isso, é proposta uma extensão para a arquitetura de *Agentes Comunicadores* [Jesus et al. 2018], através da implementação de um modelo de firewall para controlar a migração e a comunicação do agente para outro sistema multiagente.

O modelo proposto busca controlar a migração e a comunicação do agente para outro SMA, por meio de regras e políticas de segurança definidas. Dessa forma, o *Agente Comunicador* pode examinar e verifica a identificação da origem e seus privilégios, antes de permitir que eles entrem ou se comuniquem.

Este artigo está organizado da seguinte forma: na Seção 2 são apresentados os conceitos básicos necessários para o entendimento da proposta; na Seção 3 são apresentados e comentados alguns trabalhos relacionados; A metodologia proposta neste trabalho é apresentada na Seção 4; por fim, os resultados esperados são apresentados na Seção 5.

2. Fundamentação Teórica

Os denominados *Agentes Comunicadores* são uma extensão da arquitetura de agentes Jason [Bordini et al. 2007] capazes de se comunicar com outros SMA, além de permitirem a migração de agentes entre SMA distintos, através do ContextNet [Endler et al. 2011], um gateway IoT (*Internet of things*). Nesta arquitetura, os protocolos permitem migrar um SMA inteiro ou de agentes específicos conforme a relação que será estabelecida com o SMA de destino, sendo elas baseadas nas relações ecológicas: Inquilinismo, Mutualismo e Predatismo. No Inquilinismo, ocorre a transferência de um SMA inteiro para outro, visando se tornar apenas um com o destino; no Mutualismo, o objetivo é transmitir e obter novos conhecimentos e depois retornar ao SMA de origem; e no Predatismo, o intuito é dominar o SMA de destino, preservando seus agentes [Jesus et al. 2018].

Um *firewall* atua como uma espécie de barreira, deixando apenas determinadas comunicações seguirem, através das regras e politicas, previamente definidas. Um firewall podem ser baseado em hardware ou em software. Os baseados em hardware são dispositivos externos que atuam normalmente no ponto de conexão com a internet, podendo dar suporte a uma pequena rede local ou até mesmo em uma rede corporativa agindo como um concentrador/comutador (hub/switch) de rede. Um firewall baseado em software é normalmente projetado para trabalhar com sistemas operacionais específicos. Estes firewalls após a instalação normalmente vem com seu próprio conjunto de políticas predefinidas, políticas que permitem especificar qual nível de segurança se deseja obter [Ford 2002].

Nesta proposta, iremos implementar um firewall baseado em software, onde o firewall fará parte da própria arquitetura do *Agente Comunicador*, dado que ele recebe todas as comunicações, seja transferência ou apenas uma mensagem, assim fazendo o controle conforme as regras e políticas definidas.

3. Trabalhos relacionados

Em [Chebout et al. 2016], embora não mencione explicitamente *firewalls*, é proposta uma abordagem baseada em aspectos para o controle preventivo em sistemas multiagentes abertos, mediante uma observação dos movimentos dos agentes, interceptando todas as solicitações externa e em seguida é realizada uma análise para verificar se o agente possui ou não determinado recurso para poder prosseguir com sua solicitação, tendo um certo custo de processamento, que leva mais tempo dado que é feito toda uma análise antes de liberar o acesso ou bloqueá-lo. Diferentemente, em nossa abordagem, propomos a criação de regras e políticas para verificação se o agente pode ou não se comunicar, ou realizar transferências.

Em [Gupta et al. 2017], é abordado o paradigma de Internet das Coisas (IoT) e a quantidade de dados em nuvem que são sensíveis a ataques, podendo ser comprometidos. O trabalho propõe uma solução baseada em firewall, embarcado em um Raspberry Pi que protege a comunicação com o banco de dados localizado na nuvem. Através da instalação desse firewall em determinada rede, o trabalho pôde analisar e proteger cada pacote entrando e saindo da mesma. Diferentemente o nosso trabalho, propõe a criação de um modelo de firewall baseado em software para controlar o acesso e a comunicação extra-SMA que podem estar hospedados na mesma rede ou computador.

Em [Vila et al. 2007] são apresentados os desafios existentes na busca de soluções dos problemas de segurança em sistemas multiagentes baseados no framework JADE. Dentre das soluções apresentadas destaca-se a autenticação de usuários por criptografia e a autorização do acesso a serviços por determinado grupo de usuários. O gerenciamento apresentado conseguiu garantir que os dados não fossem acessados por usuários sem permissão. Diferentemente, este trabalho propõe a extensão da arquitetura de agente especialista capaz de gerenciar a movimentação e a comunicação entre diferentes SMA baseados em JASON.

4. Proposta

Buscando adicionar uma camada de segurança e possibilitar o controle de comunicação e acesso ao SMA, propomos a utilização de políticas e regras. Para isso, será necessário estender a arquitetura do *Agente Comunicador*, adicionando ações internas capazes de analisar os cabeçalhos da comunicação KQML [Finin et al. 1994] e da migração Bio-Inspirada [Souza de Jesus. et al. 2021]. No contexto deste trabalho definimos regras e políticas como:

Regra:KQML *Critérios tais como origem, tipo de interação, força ilocucionária ou protocolo que definem se uma comunicação e/ou migração deve ser permitida ou negada.*

Política: *Define os critérios para permitir ou negar uma comunicação e/ou uma migração de agentes, caso não exista uma regra que se aplique à comunicação*

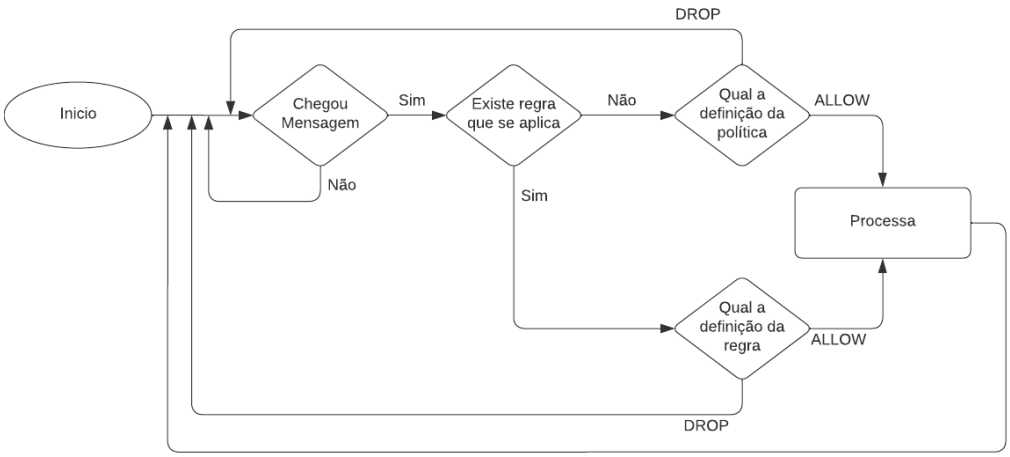

Figura 1. Fluxograma de análise de comunicação KQML de entrada ou saída do SMA.

Esta abordagem visa garantir que apenas agentes confiáveis ingressem na sociedade de agentes. Para isso, propomos um mecanismo para restringir ou permitir a comunicação entre agentes com base em políticas de segurança estabelecidas. Seu objetivo é garantir que sejam processadas pelo agente Comunicador apenas comunicações KQML autorizadas, o acesso não autorizado é impedido. Na Figura1 é apresentado o fluxograma de análise da comunicação KQML.

4.1. Ações Internas propostas

Em resumo, a abordagem proposta neste trabalho inclui estender a arquitetura dos *Agentes Comunicadores*, adicionando ações para gerenciar políticas e regras de encaminhamento de mensagens e agentes móveis, contribuindo com o aumento da segurança de SMA Abertos. Esse agente irá analisar o cabeçalho que chegará na tentativa de comunicação, definindo qual será a ação a ser realizada, sem considerar a mente do agente. Abaixo é apresentada uma ilustração, figura 2, sobre o modelo de plano de ação de um agente Comunicador, definindo a política e as regras para comunicação KQML externa ao SMA.

```
+!firewall <-
    .policy(TIPO,ABRANGÊNCIA,FORÇA|PROTOCOLO,DETERMINAÇÃO);
    .rule(TIPO,ABRANGÊNCIA,ORIGEM,DESTINO,FORÇA|PROTOCOLO,DETERMINAÇÃO).
```

Figura 2. Uma proposta de plano para gerenciamento do *firewall*

Nas políticas, temos que definir os parâmetros Tipo, Abrangência, Força ou Protocolo e a determinação, a tabela abaixo ilustra a definição de cada parâmetro e seus possíveis valores.

Nas regras, será necessário definir os parâmetros tipo, abrangência, origem, destino, força ou Protocolo e a determinação, a tabela abaixo ilustra a definição de cada parâmetro e seus possíveis valores.

- **Tipo:** define se a regra ou política se aplica à entrada ou saída $(input|output)$;
- **Abrangência:** define se a regra ou política se aplica a comunicação, transferência ou ambos $(all|communication|migration)$;
- **Origem:** define a qual SMA ou agente origem a regra se aplica $(source)$;
- **Destino:** define a qual SMA ou agente de destino a regra se aplica $(destination)$;
- **Força/protocolo:** define qual é a força da mensagem ou o protocolo de transferência $(all|illocutionary_{force}|BioInsp_{protocol})$;
- **Determinação:** determina se a regra ou política irá liberar, ou bloquear todos os acessos $(accept|drop)$.

4.2. Cenário comparativo

A proposta do nosso trabalho pode ser comparada o funcionamento de um condomínio, onde esse ocupa o lugar do SMA e o agente comunicador atua como telefonista e porteiro desse sistema. O telefonista do condomínio ao atender uma ligação, ele identifica a origem e para qual morador, a ligação é destinada. Em seguida, ele verifica se existe alguma anotação que seja aplicável a ligação. Por exemplo, algum morador pode estar aguardando essa ligação ou informar que não quer receber a ligação. Caso não exista anotação

específica, o telefonista irá seguir as recomendações gerais do condomínio sobre encaminhamento de ligações. Por exemplo, podem existir regras gerais sobre encaminhamento de telemarketing ou horários de não perturbe.

No caso de migração entre sistemas, dentro do cenário comparativo proposto, uma pessoa, ao chegar até a portaria do condomínio, primeiro o porteiro irá verificar através da identificação dessa pessoa se ela é moradora, caso seja, ela tem sua entrada liberada. Se for um visitante, o porteiro irá verificar se existe alguma anotação sobre entrada pré-autorizada. Caso contrário, o porteiro irá seguir as regras do condomínio, negando a entrada, por exemplo.

5. Resultados Esperados

Este trabalho propõe uma abordagem e espera-se que a políticas de migração e controle de acesso para sociedades de agentes, contribua para fortalecer a segurança de SMA Abertos. Alguns resultados esperados incluem:

- Prevenção de acessos não autorizados: A implementação do modelo de firewall permitirá o controle da migração de agentes para uma sociedade de agentes, evitando a entrada de agentes maliciosos ou não confiáveis. Isso ajudará a proteger o SMA contra invasões e ameaças à segurança.
- Mitigação de riscos de segurança: A definição de políticas de migração permitirá que a sociedade de agentes estabeleça critérios para permitir ou negar a migração de agentes. Essas políticas podem incluir a verificação de credenciais do agente, tipo de comunicação ou transferência de dados e a força da mensagem. Com isso, espera-se reduzir os riscos de agentes maliciosos comprometerem a integridade e confiabilidade das interações no SMA.
- Fortalecimento da confiabilidade de SMA Aberto: Com a implementação das políticas de migração e controle de comunicação, espera-se fortalecer a confiabilidade dos sistemas multiagentes como um todo. Agentes maliciosos terão maior dificuldade em penetrar no sistema, garantindo a integridade das interações entre agentes confiáveis e evitando a interferência de atores não autorizados.
- Melhoria da segurança global: A abordagem proposta visa aprimorar a segurança global dos sistemas multiagentes abertos, considerando a livre circulação de agentes. Ao adotar políticas de migração e controle de comunicação, o SMA estará mais preparado para lidar com riscos de segurança, garantindo a confidencialidade, integridade e disponibilidade das interações entre os agentes.

Em resumo, a implementação da abordagem baseada em políticas de migração e controle de comunicação espera fortalecer a segurança de sistemas multiagentes abertos, reduzir riscos de acessos não autorizados, mitigar ameaças de agentes maliciosos, controlar a comunicação entre SMAs e melhorar a confiabilidade global do sistema. Esses resultados contribuirão para a criação de ambientes mais seguros e confiáveis para o desenvolvimento de sociedades de agentes.

Além disso, será necessário para a validação do modelo, uma análise do custo computacional adicionado no processo de comunicação. Será necessário comparar a taxa de transferência e migração entre agente comunicador padrão, agente comunicador estendido, sem regras e com política padrão *accept* e agente comunicador com regras de controle de acesso.

Referências

Alvares, L. O. and Sichman, J. S. (1997). Introdução aos sistemas multiagentes. In *Jornada de Atualização em Informática*. UnB.

Bordini, R. H., Hübner, J. F., and Wooldridge, M. (2007). *Programming Multi-Agent Systems in AgentSpeak Using Jason (Wiley Series in Agent Technology)*. John Wiley Sons, Inc., Hoboken, NJ, USA.

Chebout, M. S., Mokhati, F., Badri, M., and Chaouki Babahenini, M. (2016). Towards preventive control for open mas. ICINCO 2016, page 269–274, Setubal, PRT. SCITEPRESS - Science and Technology Publications, Lda. https://doi.org/10.5220/0006005602690274.

Endler, M., Baptista, G., Silva, L. D., Vasconcelos, R., Malcher, M., Pantoja, V., Pinheiro, V., and Viterbo, J. (2011). Contextnet: Context reasoning and sharing middleware for large-scale pervasive collaboration and social networking. In *Proceedings of the Workshop on Posters and Demos Track*, PDT '11, New York, NY, USA. ACM. https://doi.org/10.1145/2088960.2088962.

Finin, T., Fritzson, R., McKay, D., and McEntire, R. (1994). KQML as an agent communication language. In *Proceedings of the Third International Conference on Information and Knowledge Management*, CIKM '94, page 456–463, New York, NY, USA. ACM. https://doi.org/10.1145/191246.191322.

Ford, J. L. (2002). Manual completo de firewalls pessoais: tudo o que você precisa saber para proteger o seu computador. Pearson.

Gupta, N., Naik, V., and Sengupta, S. (2017). A firewall for internet of things. In *2017 9th International Conference on Communication Systems and Networks (COMSNETS)*, pages 411–412. https://doi.org/10.1109/COMSNETS.2017.7945418.

Hubner, J. F. (1995). *Migração de agentes em sistemas multi-agentes abertos*. Dissertação (Mestrado, Universidade Federal do Rio Grande do Sul. Instituto de Informática. Curso de Pós-Graduação em Ciência da Computação., Porto Alegre. https://lume.ufrgs.br/handle/10183/25032.

Jesus, V., Manoel, F., Pantoja, C. E., and Viterbo, J. (2018). Transporte de agentes cognitivos entre sma distintos inspirado nos princıpios de relaçoes ecológicas. In *Workshop-Escola de Sistemas de Agentes, seus Ambientes e apliCações—XII WESAAC*, pages 179–187.

Souza de Jesus., V., Pantoja., C. E., Manoel., F., Alves., G. V., Viterbo., J., and Bezerra., E. (2021). Bio-inspired protocols for embodied multi-agent systems. In *Proceedings of the 13th International Conference on Agents and Artificial Intelligence - Volume 1: ICAART*, pages 312–320. INSTICC, SciTePress. https://doi.org/10.5220/0010257803120320.

Vila, X., Schuster, A., and Riera, A. (2007). Security for a multi-agent system based on jade. *Computers Security*, 26(5):391–400. https://doi.org/10.1016/j.cose.2006.12.003.