Controle de acesso adaptativo através do monitoramento do ambiente

G. M. Toschi[1], C. E. Cugnasca[2]

***Abstract* — This paper presents the proposal of computer system model for the control of people access in buildings and facilities through adaptive techniques to make it sensitive to the context and take into account the history of the environment. Adaptive techniques have been incorporated into two parts of this process, at the monitoring of the environment for the calculation of the level of threat, and at the calculation of levels of access of each room of a building. In this work we propose, the union of these processes to compose a broader, more flexible and safer system.**

***Keywords* — monitoring, inbound and outbound flow of people, access control, adaptive techniques.**

I. Introdução

Os sistemas de controle de acesso (SCA) vem sendo utilizados há muito tempo, inicialmente com o controle sendo realizado por um porteiro. Trata-se de uma forma pouco eficiente, de baixa segurança e dependente da habilidade e competência de uma pessoa.

Com o intuito de melhorar esse processo, sistemas automatizados foram gradualmente introduzidos em função da tecnologia disponível em cada época. Atualmente busca-se automatizar cada vez mais o sistema de acesso, conseguindo maior eficiência e segurança.

O controle de acesso as instalações vem se tornando cada vez mais importante para a segurança. Contudo, em função das particularidades de cada local, há a necessidade de adaptações, de forma que uma característica desejável nos sistemas de controle é a flexibilidade, viabilizando a implantação de sistemas mais eficazes e seguros.

Diversos modelos de controle de acesso têm sido estudados, um exemplo são os tradicionais, que são independentes de contexto. Atualmente , novos modelos estão surgindo como o de autorização contextual, na qual variáveis de ambiente alteram o comportamento do sistema. Um outro modelo é o controle de acesso baseado em papéis (CABP) [5]. O *National Institute of Standards and Technology* (NIST) propõe um padrão para o CABP, que estabelece um modelo referencial de autorização contextual.

Em [5] descreve-se uma especialização desse modelo, que foi aplicado no controle de acesso sensível ao contexto aplicado no Instituto do Coração do Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo (InCor).Formas de fazer esse controle de acesso se tornar cada vez mais dinâmico estão em estudo, com o objetivo de fazer com que ele se adapte às condições do ambiente para proporcionar maior segurança.

Para que o SCA se adapte ao ambiente, este deve possuir um sistema de monitoramento, que prove a capacidade de coletar e processar informações sobre o ambiente e sobre as pessoas que nele circulam.

Encontram-se disponíveis no mercado sistemas de monitoramento baseados em diversas tecnologias e sensores [1], destinados a coletar os dados do ambiente. Um exemplo é o monitoramento do centro de Londres, que é feito por câmeras espalhadas com movimento rotacional e *zoom* para seguir automaticamente o foco de atividades suspeitas durante a noite. Técnicas de inteligência artificial são utilizadas para classificar movimentações com características suspeitas, alertando os operadores, que são os responsáveis pela confirmação da identificação e ações a realizar em cada caso.

O objetivo deste trabalho é apresentar uma proposta de evolução para o modelo de SCA utilizando técnicas adaptativas para torna-lo mais sensível ao contexto através do ajuste dinâmico dos intervalos de cálculo do nível de ameaça do ambiente. A seção II discute o nível de segurança e ameaça e como o cálculo deste pode ser realizado de forma adaptativa. A seção III descreve o processo de controle de acesso predial de acordo com a patente americana em [6], enquanto a seção IV apresenta um modelo de controle de acesso adaptativo. A seção V apresenta futuras simulações utilizando a ferramenta AdapTools [9], enquanto a seção VII discute os resultados e apresenta as conclusões. Por fim, a última seção apresenta a lista de referências.

II. Nível de Ameaça/Segurança

Um sistema de monitoramento predial consegue calcular o nível de ameaça referente ao ambiente por meio das variáveis monitoradas, um processo denominado *multisensor* [1], que rastreia os usuários durante sua permanência dentro do prédio, registrando todos os seus movimentos e ações. Por exemplo, o sensor de luminosidade pode indicar o período noturno, no qual o índice de ocorrências de furtos ou roubos é mais elevado. Configurando-se convenientemente as regras de interpretação dos sinais dos sensores, pode-se calcular o nível de ameaça em cada instante.

[1] Eng. Eletricista, Mestrando, Escola Politécnica da Universidade de São Paulo.
[2] Eng. Eletricista, Mestre, Doutor e Livre-Docente, Professor Associado 3, Escola Politécnica da Universidade de São Paulo.

Esse exemplo evidencia que é possível identificar padrões de comportamentos a partir com os dados coletados e, utilizando-se as regras contextuais de autorização do processo de CABP, pode-se fazer o cálculo do nível de ameaça [5].

A. Modelo adaptativo para o cálculo de ameaça

Uma das formas de aplicação do modelo adaptativo no controle de acesso consiste em mudar o intervalo de amostragem das variáveis do ambiente, utilizadas para o cálculo do nível de ameaça. Para o controle dessa frequência é proposto um Autômato Adaptativo (AA) [10] descrito a seguir que foi adaptado de [9].

Definem-se limites para o nível de ameaça, e quando algum dos valores amostrados das variáveis monitoradas ultrapassá-los, a frequência de amostragem é alterada. Dessa forma, quando esse nível ultrapassar um limite superior, a frequência aumenta; ao retornar a um valor inferior a um dos limites, a frequência volta a diminuir.

A Figura 1 mostra um exemplo de frequência de cálculo do nível de ameaça ao longo do tempo, no qual o nível de ameaça é calculado a partir de amostragens das variáveis de um ambiente. Foram definidos somente dois limites, mas podem ser definidas varias faixas de valores, definidas por dois limites, dentro dos quais a frequência terá um valor específico. A frequência dessas amostragens e do cálculo depende do nível calculado: quando esse nível sai da região de normalidade (faixa definida por a e b). o intervalo entre uma amostra e outra é aumentado, alterando a frequência do cálculo.

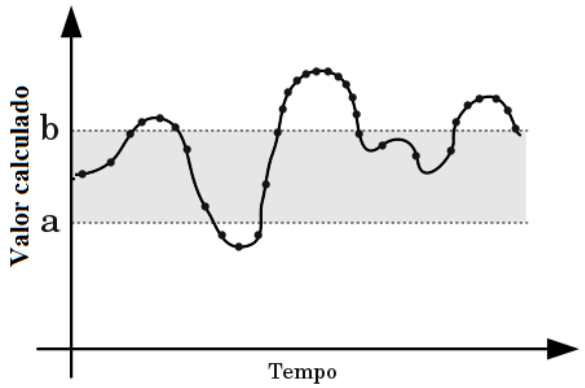

Figura 1 - Exemplo de uma sequência de cálculo do nível de ameaça ao longo do tempo. Adaptado de [9]

III. Controle de Acesso

O processo de controle de acesso consiste basicamente em identificar a pessoa que está se movimentando, validar suas permissões e responder com a liberação ou negação do seu acesso dessa pessoa ao ambiente controlado, e eventualmente acionando outras medidas de segurança para proteger o ambiente.

A Figura 2 mostra o fluxograma base da patente americana de um sistema de segurança para o controle de acesso predial [6]. Esse processo tem entradas de variáveis, por exemplo, a luminosidade do ambiente, e essas variáveis são utilizadas para controle do ambiente externo, como acender a luz quando estiver escuro. Porém a validação de acesso é independente das condições do ambiente.

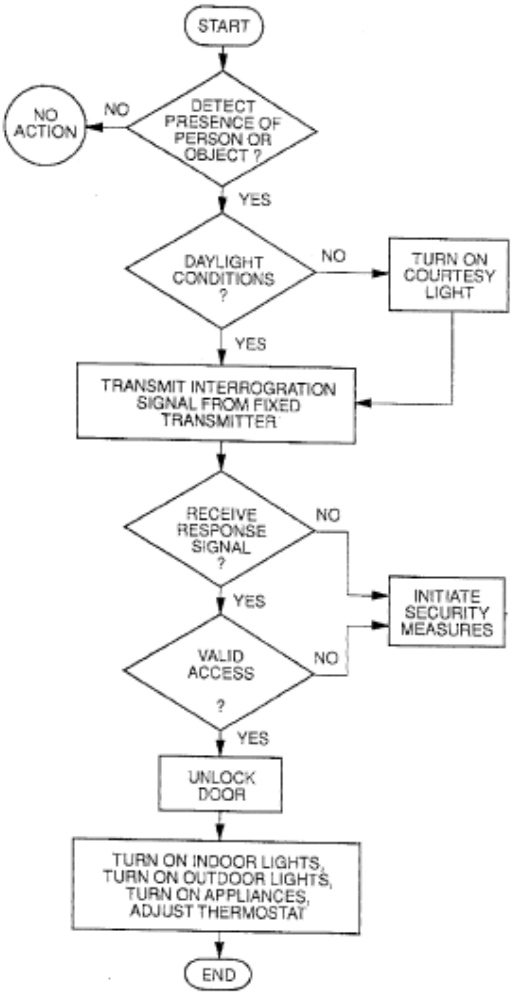

Figura 2 - Fluxograma de controle de acesso extraído de [6]

IV. Modelo de Controle de Acesso Adaptativo

O modelo de controle de acesso da Figura 2 foi estendido para um modelo de controle de acesso adaptativo, baseado no nível de ameaça calculado. Para isso a etapa de validação de acesso do usuário foi modificada para torná-la adaptativa ao nível de ameaça calculado.

A. Cálculo da autorização de acesso

O cálculo da autorização de acesso pode ser feito utilizando-se duas variáveis:

- Nível de permissão do usuário;
- Nível de permissão do ambiente.

Para um usuário ter acesso a um ambiente, seu nível de permissão deve ser maior ou igual ao do ambiente. Dessa forma o nível de permissão do ambiente torna-se o limite inferior para a permissão de acesso do usuário.

Na Figura 3 podem-se visualizar os níveis de acesso fixos, não adaptativos. Um ambiente que tenha nível de acesso 4, por exemplo, sempre exigirá um nível de permissão do usuário maior ou igual a 4 independentemento do contexto.

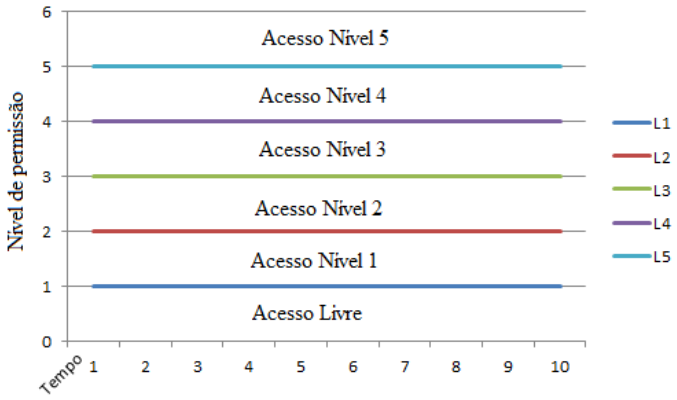

Figura 3 - Níveis de acesso estáticos

B. *Calculo da autorização de acesso adaptativo*

Para tornar o controle de acesso mais seguro, pode-se fazer o cálculo da autorização de acesso de modo adaptativo. Dependendo do nível de ameaça do ambiente, calculado pelo sistema de monitoramento, o grau de permissão dos ambientes pode aumentar, diminuir ou podem ser criados novos níveis de permissão intermediários para melhor se adequar à situação do prédio. O nível de acesso é composto por um nível base, *offset*, somado a um variável proposcional ao nível de ameaça calculado. A formula a seguir representa esse modelo:

Nível de Permissão = offset + c*(Nível de Ameaça)

Na Figura 4 podem-se observar os limites dinâmicos dos diferentes níveis de acesso. No Instante de Tempo 2 algum evento externo ocorreu, modificanto o nível de ameaça calculado, e assim, os limites para os diferentes níveis de acesso são alterados dinamicamente. Cada ambiente pertence a um nível de acesso e, portanto, somente os usuários com nível de permissão maior ou igual aos limites estabelecidos para acesso em determinado momento serão autorizado a entrar no ambiente.

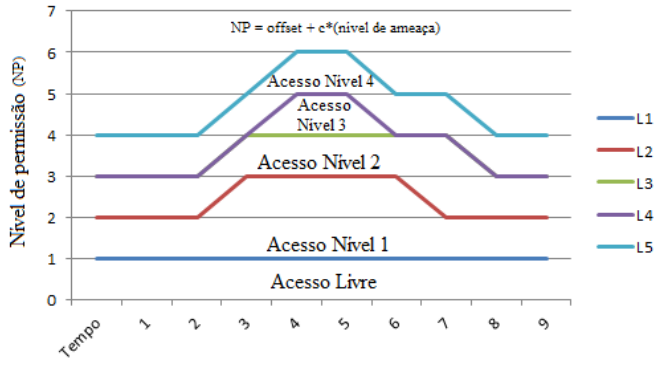

Figura 4 - Níveis de acesso adaptativos

Podem-se observar que o acesso Nível 3 somente surge em um momento específico, Instante de tempo 3, para suprir uma necessidade momentânea, sendo depois descartado, quando a situação volta ao normal.

C. *Controle de acesso adaptativo*

A Figura 6 apresentado a extensão do passo de validação de acesso, apresentado na Figura 5, que será substituido no fluxograma de controle de acesso apresentado na Figura 2. O processo de validação de acesso é baseado no cálculo da autorização de acesso adaptativo da Figura 4.

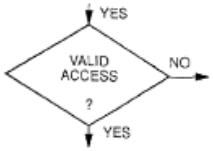

Figura 5 - fluxograma de controle de acesso original retirado de [6]

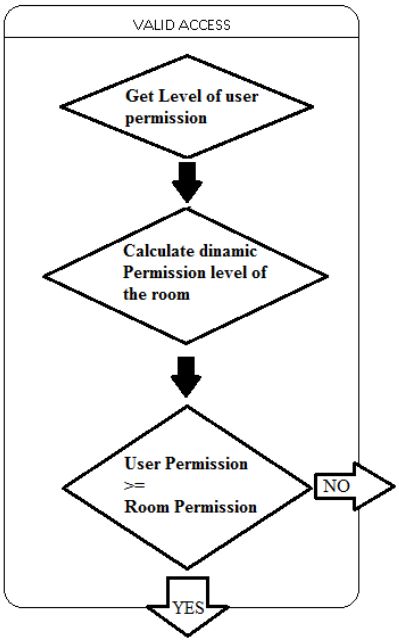

Figura 6 - fluxograma de controle de acesso adaptativo

Utilizando-se a nova forma de cálculo, o controle de acesso se torna adaptativo às condições do ambiente.

Os sensores espalhados pelo prédio se tornam entradas de dados do sistema. A entrada de dados é adaptativa em relação às condições do ambiente, variando a frequência de amostragem de acordo com o nível de ameaça calculado.

A partir deste nível calculado podem-se definir dinamicamente as faixas de permissão de cada ambiente do prédio. Dessa forma as faixas de permissão se tornam adaptativas às condições do ambiente também.

A utilização de técnicas adaptativas para o controle de acesso tem como objetivo tornar mais seguro esse processo, de forma a garantir a integridade do prédio que tem um sistema inteligente e adaptativo.

V. Simulações Futuras

A ferramenta AdapTools [8] pode ser utilizada para realização de simulações computacionais de um modelo adaptativo. O AA descrito anteriormente será construído no AdapTools para gerar a simulação. A partir dessa simulação pode-se validar a utilização desse AA para o calculo do nível de ameaça e do controle de acesso de ambientes.

Em uma primeira etapa de simulação pode-se utilizar o modelo adaptativo de cálculo de ameaça com apenas uma variável de ambiente para simplificação da simulação. Em

seguida, utiliza-se esse nível de ameaça calculado para a verificação da autorização de acesso adaptativo. Dessa forma pode-se visualizar como a alteração de uma variável do ambiente interfere em ambos os cálculos, e diretamente influenciar o acesso de um usuário ao ambiente controlado.

Em uma segunda etapa pode-se adicionar múltiplas variáveis de ambiente, que são alteradas para simular as condições do ambiente de um prédio. Assim, pode-se analisar a simulação de forma mais próxima de um sistema em ambiente real.

V. VI. Comentários e Discussões

Este artigo apresentou o estudo do processo de monitoramento adaptativo para o calculo do nível de ameaça. Em seguida apresentou o estudo do processo de controle de acesso adaptativo que utiliza os dados do processo de monitoramento para calcular os níveis de acesso dinamicamente e assim tornando-se sensível as condições externas do ambiente.

A integração desses dois processos em um único sistema proporcionou maior flexibilidade para adaptação as políticas de controle de acesso mais complexas que se moldam ao contexto, para garantir um melhor e mais efetivo controle de monitoramento do ambiente.

A abordagem utilizada neste artigo para tornar o controle de acesso adaptativo também pode ser utilizada em ambientes virtuais. Da mesma forma que o processo de controle de acesso valida o acesso de um usuário à um ambiente de modo adaptativo, como foi descrito neste artigo, o processo de controle de acesso virtual pode determinar as permissões de acesso, leitura, escrita e de execução de um usuário, ou um grupo de usuários, em um ambiente virtual. Por exemplo, em um ambiente corporativo, este processo pode determinar se um usuário poderá se conectar ou não em um servidor dependendo das variáveis externas amostradas. Usuários de um grupo de baixo nível de permissão só podem se conectar aos servidores corporativos durante o dia estando dentro da empresa, por exemplo.

Nesse ambiente virtual as variáveis podem ser físicas, lidar no ambiente externo, ou variáveis virtuais, por exemplo, o volume de usuários conectados no servidor ou se o servidor está sendo alvo de um ataque *hacker*.

Dessa forma o ambiente virtual também pode se tornar mais seguro através do controle adaptativo de acesso.

Referências

[1] L. Osadciw, P. Varshney, e K. Veeramachaneni, “Improving personal identification accuracy using multisensor fusion for building access control applications”, in Information Fusion, 2002. Proceedings of the Fifth International Conference on, 2002, vol. 2, p. 1176–1183.

[2] C. Neves, L. Duarte, N. Viana, e V. Ferreira, “Os dez maiores desafios da automação industrial: as perspectivas para o futuro”, in II Congresso de Pesquisa e Inovacao da Rede Norte Nordeste de Educa\ccao Tecnológica, Joao Pessoa, Paraıba, Brasil, 2007.

[3] E. Oliveira, V. Nogueira, e S. Brito, “Controle de fluxo de automóveis com RFId”.

[4] Prof. Dr. A. R. Hirakawa e Prof. Dr. J. S. C. Martini, “SIGINURB – Sistema de Gestão da Infraestrutura Urbana”, Escola Politécnica da Universidade de São Paulo

[5] G. Motta e S. S. Furuie, “Um modelo de autorização contextual para o controle de acesso baseado em papéis”, in II Workshop em Segurança de Sistemas Computacionais (WSeg2002), 2002, p. 137–144.

[6] D. C. Duhame e D. V. Meyvis, “Security system for controlling building access”, U.S. Patent 5,541,585jul-1996.

[7] N. T. Nguyen, S. Venkatesh, G. West, H. H. Bui, e A. Perth, “Multiple camera coordination in a surveillance system”, Acta Automatica Sinica, vol. 29, no 3, p. 408–422, 2003.

[8] L. D. JESUS, D. G. D. SANTOS, A. A. D. CASTRO, H. PISTORI. WTA 2007 - II.2 - “AdapTools 2.0: Implementation and Utilization Aspects.” IEEE Latin Am. Trans. 5, 527-532 (2007).

[9] SANTOS, I. M. ; CUGNASCA, C. E. Autômato Adaptativo para definição autônoma do intervalo de amostragem de dados em Rede de Sensores Sem Fio. In: VI Workshop de Tecnologia Adaptativa, 2012, São Paulo. Memória do VI Workshop de Tecnologia Adaptativa 2012. São Paulo: Ed. USP, 2012.

[10] J. J. Neto. “Adaptive rule-driven devices – general formulation and case study” *Revised Papers from the 6th International Conference on Implementation and Application of Automata*, *CIAA 2001*, London, UK: Springer-Verlag, 2002, pp. 234-250, ISBN 3-540-00400-9.