Arcabouço de Vigilância Inteligente para Operações de Compras Eletrônicas no Contexto de *Smart Cities*

Suzani Cristina Pereira dos Santos[1], Robson Gomes de Melo[1], Nivaldi Calonego Junior[1]

[1]Núcleo de Redes Inteligentes e Soluções Criativas (RISC) – Universidade do Estado de Mato Grosso (UNEMAT)
Av São João, S/N – Cáceres – MT – Brazil

Abstract. *Intelligent surveillance systems aim to identify suspicious activity beyond the observation of people and environments, as computer networks and computer systems remain vulnerable to malicious actions. The intelligent surveillance framework (Arcabouço de Vigilância Inteligente - AVI) uses the cognitive construction of a user profile and the recognition of devices for electronic purchases, aiming to ensure the authenticity of transactions for computer systems in networked interconnected. The AVI assessment shows that it is effective with respect to user authenticity and that the smart surveillance model in purchasing operations matches the expectation of vulnerability reduction.*

Resumo. *Sistemas de vigilância inteligentes almejam identificar atividades suspeitas, indo além da observação de pessoas e ambientes, dado que as redes de computadores e os sistemas computacionais continuam vulneráveis às ações maliciosas. O sistema Arcabouço de Vigilância Inteligente (AVI) utiliza a construção cognitiva de um perfil de usuário e o reconhecimento de dispositivos para realização de compras eletrônicas, objetivando assegurar a autenticidade das transações para sistemas computacionais em interligados em rede. A avaliação do AVI monstra que é eficaz em relação à autenticidade dos usuários e que o modelo de vigilância inteligente em operações de compras condiz com a expectativa de redução de vulnerabilidades.*

1. Introdução

Sistemas de vigilância inteligente (Smart Surveillance System - SSS) são parte das soluções para os problemas decorrentes das transformações sociais, objetivando detectar comportamentos anormais por meio da vigilância [Talari et al., 2017]. A vigilância automatizada deve ser aplicada em redes e sistemas computacionais, pois estes compõem a base das transformações das cidades para uma forma inteligente. As tecnologias utilizadas para tornar uma cidade inteligente são vulneráveis a vazamento de informações privadas e sujeitas à interferência por ataques externos [Zhang et al. 2017]. Com isso, ainda há desafios a serem superados, principalmente aqueles relativos a autenticidade durante o processo de compras eletrônicas. A autenticidade consiste em garantir que o autor é, de fato, quem se diz ser [Melo 2014]. Essa garantia é fundamental para a implantação da estratégia de cidade inteligente, carecendo de um arcabouço de vigilância inteligente.

O Arcabouço de Vigilância Inteligente (AVI) refere-se a uma estrutura que fundamenta a vigilância inteligente em operações de compras eletrônicas. O AVI é um modelo híbrido que combina o modelo baseado na construção de um perfil de usuário

com o modelo baseado no reconhecimento de dispositivos.

Um cenário de experimentação foi desenvolvido como forma de realizar uma prova de conceito e análise da eficácia do AVI. Um sistema WEB foi desenvolvido para representar de forma fidedigna uma operação de compra eletrônica em um ambiente de cidades inteligentes.

2. Trabalhos Correlatos

Os SSS almejam vigiar, por tempo, indeterminado ambientes, pessoas, redes e sistemas computacionais [Talari et al., 2017], sendo a utilização de câmeras e algoritmos de aprendizagem de máquina as mais usadas.

Patrick e Bourbakis compararam algumas implementações de vigilância de objetos em uma casa inteligente, em ambiente interno, baseado em câmeras, considerando, especificamente, as alterações de luminosidade no interior. As câmeras são espalhadas nos aposentos de forma a vigiar o ambiente como um todo e rastrear os objetos presentes. O trabalho tem como premissas os elementos considerados importantes para um sistema de vigilância, tais como: custo, área de alcance, tempo de vida, confiabilidade, entre outras. Por fim, constataram que nenhum sistema é ideal, dependendo do tamanho e formato do objeto procurado [Patrick and Bourbakis 2009].

Sidhu e Sharad trataram da automatização para a identificação de cenas de crimes interpessoais, tais como o *bullying*, assalto e assédio. Essa abordagem utiliza o processamento de áudios e imagens para realização de seus processos. Em ambos os casos o sistema emite um alerta quando o gatilho é ativado [Sidhu and Sharad 2016].

Wu discute um sistema de vigilância inteligente que utiliza câmeras com acesso remoto (do inglês, Pan–Tilt–Zoom câmera - PTZ), sensores no ambiente, dispositivos vestíveis e um servidor de vigilância para automatizar a identificação de eventos e de pessoas suspeitas. O sistema utiliza um algoritmo de aprendizagem para essa automatização. A localização e o tempo de execução são exibidos na sua interface quando uma situação de interesse ocorre [Wu et al. 2016].

Dubal trata da vigilância por meio de um robô mutável. Para isso, utilizaram um veículo aéreo sem tripulação (do inglês, Unmanned Aerial Vehicle - UAV) capaz de realizar a vigilância nos três meios de locomoção (ar, água e terra). Entretanto, as imagens capturadas por esse UAV carecem de análise humana para a constatação de alguma anormalidade [Dubal et al. 2016].

Navin propõe um programa de vigilância da saúde pública baseado na utilização de uma aplicação para celulares. Esse sistema permite que epidemiologistas enviem formulários de pesquisa à comunidade e armazenem as respostas em um banco de dados, que é analisado por técnicas de aprendizagem de máquina. Essas análises permitem a detecção de epidemias e a emissão de alertas. Essa forma de vigilância necessita de uma participação voluntária e sincera dos cidadãos [Navin et al. 2017].

A análise desses trabalhos mostra que os sistemas de vigilância inteligentes podem funcionar de forma colaborativa ou independente. Na forma colaborativa, pressupõe-se que a participação dos usuários é imprescindível para que seja feita a coleta de dados. Na forma independente, compreende-se que os atuantes na camada física são as câmeras e os sensores. Com isso, verifica-se que os trabalhos encontrados na literatura destacam a inteligência dos sistemas de vigilância voltados para pessoas e ambientes e não para as redes ou sistemas computacionais.

3. Arcabouço de Vigilância Inteligente

O Arcabouço de Vigilância Inteligente para ambiente de compras eletrônicas, no contexto de cidades inteligentes, baseia-se na construção de um perfil do usuário e no reconhecimento de dispositivos, criando meios para assegurar a legitimidade do usuário durante a utilização de um contato de crédito em operações de compras eletrônicas. O AVI ilustrado na Figura 1 está organizado em quatro elementos fundamentais: Módulo de Análise, Base de Reconhecimento, Módulo de Confirmação e Módulo de Autorização. As operações são vigiadas com base nas fórmulas numeradas de 3.1, até 3.9, que verificam a autenticidade de usuário, baseando-se no montante da transação e no identificador (ID) do dispositivo. O resultado da autenticidade do usuário é encaminhado para a operação de verificação de limite de crédito e outras operações financeiras.

$V_{médio} = \frac{1}{n} \cdot \sum_{i=1}^{n} m_i$; $V_{médio}$: Base de Reconhecimento sobre a média. (3.1)

$V_{max} = V_{médio} + L^+$; L^+: Limiar superior. (3.2)

$V_{min} = V_{médio} - L^-$; L^-: Limiar inferior. (3.3)

$V_{perfil} = \{x \mid V_{min} \leq x \leq V_{max}\}$; V_{perfil}: perfil do cliente. (3.4)

$D_{médio} = \{z \mid z.uso > \frac{1}{n} \cdot \sum_{i=1}^{n} d_i\}$; $D_{médio}$: Base de Reconhecimento. (3.5)

$D_{perfil} = \{y \mid y \in D \quad D_{medio}\}$; y: dispositivo. (3.6)

$m \in D_{perfil}$; m: Montante de entrada. (3.7)

$d \in D_{perfil}$ d: dispositivos compatíveis com o perfil. (3.8)

$D_{perfil}.d.uso{+}{+}$ Incremento do perfil de uso do dispositivo d.

$d \rightarrow D_{perfil}$; Insere o dispositivo d no perfil D (3.9)

O Módulo de Análise é o ponto de entrada do AVI, onde são tratados o valor de entrada e o dispositivo em uso na operação, sendo esses dados usados na lógica de *controle* baseada em perfil. Considera-se: que o perfil do usuário é dinâmico, havendo a necessidade de refinamentos baseados em cálculos de uso de valor médio; que o usuário pode trocar de dispositivo, provocando a necessidade de refinamento no uso dispositivos; o dispositivo pode não pertencer à lista. Realiza-se a inserção do mesmo e incrementa-se o seu contador de quantidade de uso; o dispositivo pertence à lista. Realiza-se a ação de incremento de seu uso; o término desse processamento ativa o Módulo de Autorização, indicando que o usuário está apto a realizar a operação. Quando o montante não é parte do perfil, ocorre a verificação de reconhecimento do dispositivo utilizado. Em caso positivo, incrementa-se o uso e aciona-se o Módulo de Autorização caracterizando a autorização do usuário. Em caso negativo, o Módulo de Confirmação envia uma mensagem para que seja feita a identificação da legitimidade do usuário. Ao ser confirmado, o valor do montante e a identificação do dispositivo são armazenados na Base de Reconhecimento. Além disso, o Módulo de Confirmação dá sequência indicando para o Módulo de Autorização que o usuário pode ser autorizado. Entretanto, caso não haja a confirmação, indica-se a não autorização do usuário. O procedimento de Refinamento ocorre periodicamente sobre a Base de Reconhecimento. Isso é feito como forma de ajuste no tempo, em intervalo compatível com o perfil do usuário e a lista dos dispositivos considerados confiáveis. Essa técnica viabiliza o

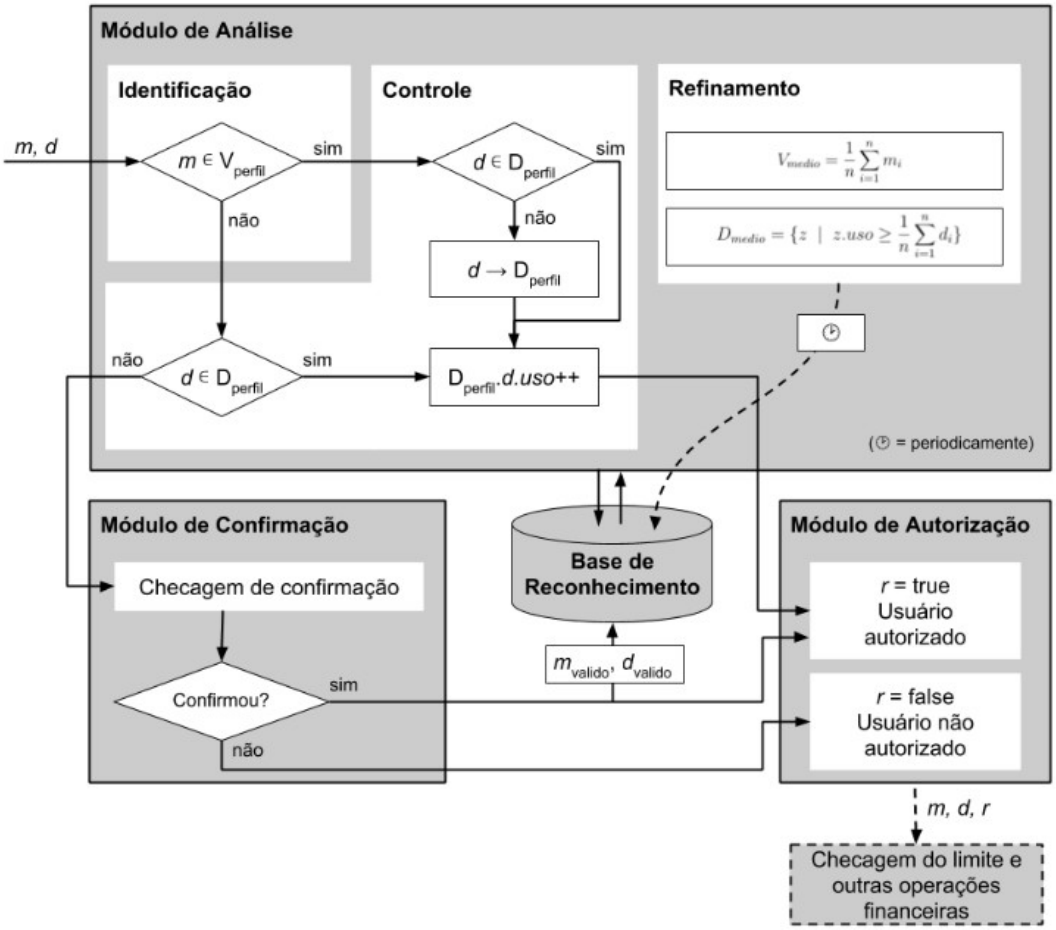


Figura 1 - Diagrama de fluxo operacional do AVI.

aperfeiçoamento do reconhecimento do perfil do usuário e a remoção dos dispositivos pouco utilizados.

Como forma de validação do AVI foi desenvolvido um sistema WEB que representa um cenário de compras eletrônicas. Esse sistema foi utilizado para a prova de conceito e análise de eficácia da proposta apresentada. Esse ambiente representa um contexto real de uma compra eletrônica em um ambiente de cidades inteligentes.

4. Resultados obtidos

Para verificar a completude da compra, é definida a função lógica f: ExE→ E; onde E é o conjunto booleano E= {V, F}; sendo V: verdade e F: Falso; x, y ϵ E; f(x, y) = x or y, ou seja, f é uma disjunção lógica.

O modelo do sistema de vigilância dos correios eletrônicos se baseia no dispositivo utilizado. Nesse modelo, os dispositivos, quando passam pela confirmação de autenticidade, são adicionados ao reconhecimento. A função teórica desse modelo é ilustrada na Figura 3 (a). Entretanto, devido ao seu procedimento de refinamento, o AVI deixa de confiar em dispositivos pouco utilizados, conforme a função teórica do gráfico na Figura 3 (b).

O modelo dos contatos de créditos se baseia na construção do perfil de usuário. Levando em consideração a demora para determinar um perfil válido para o cliente sustentado em seus gastos, as compras iniciais não garantem a autenticidade do cliente.

A função teórica desse modelo é ilustrada na Figura 4 (a). O AVI é capaz de estabelecer um intervalo de valores compatíveis com o usuário mais rapidamente do que as iniciativas atuais, conforme a função teórica ilustrada na Figura 4 (b).

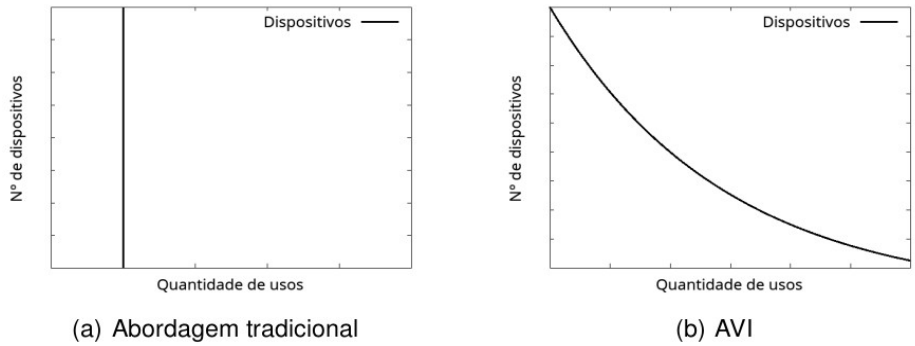


Figura 3 - Função teórica do modelo baseado em reconhecimento de dispositivo

O modelo que se baseia em perfil necessita de um certo período de tempo para que o sistema complete a construção do mesmo. Desse modo, verifica-se que, inicialmente, o sistema não possui nenhum reconhecimento do usuário com base em perfil. Assim, toda compra realizada nesse período inicial é aceita, mesmo sem garantir a autenticidade do usuário. No caso do AVI, o intervalo de gasto pertencente ao perfil do usuário ajusta-se em menos tempo, pois depende exclusivamente da quantidade de vezes em que o contato de crédito é utilizado, independente do tempo.

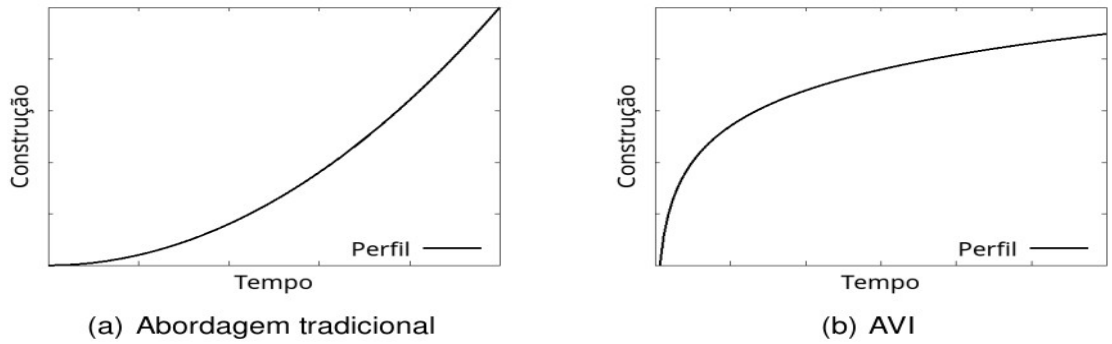
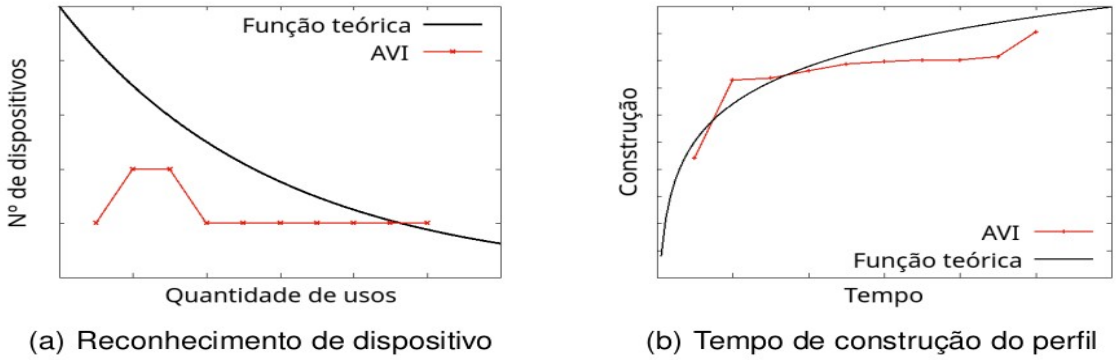


Figura 4 - Função teórica do modelo baseado em construção do perfil.

Como forma de validar o AVI sobre as funções teóricas, foram simuladas 50 (cinquenta) compras através da utilização de uma ferramenta de automatização de testes chamada Selenium (2019). O procedimento de refinamento foi realizado a cada 5 (cinco) compras, totalizando 5 (dez) execuções. Durante sua execução, foi coletada a quantidade de dispositivos considerados confiáveis, ou seja, a confirmação da compra sem a necessidade de verificação de autenticidade, e também o valor médio pertencente ao perfil do usuário. Com isso, chegou-se à representação ilustrada na Figura 5.

A análise da Figura 5(a) mostra que a quantidade de dispositivos considerados confiáveis foi reduzida conforme o esperado. Neste caso, assume-se que o AVI assegura a autenticidade do usuário confiando em poucos dispositivos, eliminando, assim, a vulnerabilidade que é criada na abordagem tradicional. Além disso, a construção do perfil se comportou segundo a função teórica, conforme ilustrado na Figura 5(b). A partir da segunda execução do refinamento, o AVI já foi capaz de obter o intervalo de valores mais compatíveis com o perfil do usuário.

O AVI é um modelo híbrido, que se baseia na construção de um perfil e no



(a) Reconhecimento de dispositivo (b) Tempo de construção do perfil

Figura 5 - Testes do AVI associados com a função teórica.

reconhecimento de dispositivo, buscando assegurar a autenticidade dos usuários. A partir de um cenário de simulação de compras eletrônicas para a prova de conceito, os resultados indicaram que o AVI foi eficaz naquilo que se propõe a realizar. Isto é, o AVI garante a autenticidade dos usuários em uma compra eletrônica quando utilizado um contato de crédito.

5. References

Dubal, S. et al. (2016) “Smart aero-amphibian surveillance system”. IEEE International Conference Workshop on Electronics Telecommunication Engineering, p. 111–116.

Melo, R. G. de. (2014) “Gerenciamento de conectividade segura e contínua em redes de acesso heterogêneas”. Tese (doutorado) – Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-Graduação em Informática, p. 144–155.

Navin, K.; Krishnan, M. M.; Lavanya, S. (2017) “A mobile health based smart hybrid epidemic surveillance system to support epidemic control programme in public health informatics”. IEEE International Conference on IoT and Application (ICIOT).

Patrick, R.; Bourbakis, N. (2009) “Surveillance systems for smart homes: A comparative survey”. 2009 21st IEEE International Conference on Tools with Artificial Intelligence, p. 248–252.

Selenium. (2019) “Gerador de teste”. https://www.seleniumhq.org/. Acesso aos 14/09/2019.

Sidhu, R. S.; Sharad, M. (2016) “Smart surveillance system for detecting interpersonal crime”. 2016 IEEE International Conference on Communication and Signal Processing, p. 2003–2007.

Talari, S. et al. (2017) “A review of smart cities based on the internet of things concept”. Energies, v. 10.

Wu, K.-R. et al. “Smart surveillance with context and location sensitivity and quality control”, IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems, p. 363–364, 2016.

Zhang, K. et al. (2017) “Security and privacy in smart city applications: Challenges and solutions”, IEEE Communications Magazine, v. 55, p. 122–129.