Multiagent Prototype with Sensors Fusion and Fuzzy Logic for Assessment of Security Systems Availability

Daniel Gleison M. Lira[1], **Marcial P. Fernández**[1], **Gustavo A. L. Campos**[1]

[1] Programa de Pós-Graduação em Ciência da Computação
Universidade Estadual do Ceará (UECE)
Fortaleza – CE – Brazil

daniel.gleison@aluno.uece.br,{marcial.fernandez,gustavo.campos}@uece.br

Abstract. *This work uses computational intelligence to mitigate the problem of monitoring the availability of security systems (videosurveillance, alarm detection, access control) in physical environments (banks, industries, hospitals). For that, a system with three smart agents was proposed: data fusion; fuzzy inference for creating the Physical Security Vulnerability Index (IVSF); monitoring and actions in the physical environment. In model validation, a prototype was implemented with devices and communication protocols based on the Internet of Things (IoT). The results of the proposed system were considered satisfactory, proving to be feasible for implementation in a real physical environment.*

Resumo. *Este trabalho utiliza inteligência computacional para mitigação do problema de monitoramento da disponibilidade de sistemas de segurança (videovigilância, detecção de alarme, controle de acesso) em ambientes físicos (bancos, indústrias, hospitais). Para tanto, foi proposto um sistema com três agentes inteligentes: fusão de dados; inferência fuzzy para criação do Índice de Vulnerabilidade de Segurança Física (IVSF); monitoramento e ações no ambiente físico. Na validação do modelo, foi implementado protótipo com dispositivos e protocolos de comunicação baseados em Internet das Coisas (IoT). Os resultados do sistema proposto foram considerados satisfatórios, mostrando-se viável para implementação em ambiente físico real.*

1. Introdução

A segurança física corresponde à constituição de barreiras físicas, recursos tecnológicos e procedimentos operacionais para dissuadir, impedir, dificultar, detectar e garantir uma resposta eficaz aos incidentes. É o ramo da segurança que visa a preservação da integridade das pessoas, patrimônio, imagem e demais ativos da organização [MARCONDES 2022].

Os recursos tecnológicos de segurança são compostos por sensores e equipamentos eletrônicos que compõem os sistemas de Circuito Fechado de TV (CFTV), detecção de alarme, controle de acesso, dentre outros, conforme Tabela 1. Os sistema de segurança podem ser aplicados em diversos ambientes físicos, a exemplo de agências bancárias, aeroportos, hospitais e indústrias.

No que tange ao segmento bancário, visando atendimento à Lei n° 7.102 [BRASIL 1983] e Portaria 3.233 [BRASIL 2012], os planos de segurança das instituições financeiras brasileiras são fiscalizados periodicamente pelo Departamento de Polícia Federal (DPF). Caso seja apurada irregularidade no funcionamento dos recursos de

Tabela 1. Subsistemas de segurança física

Subsistema de segurança	Tecnologias de sensores
Detecção de alarme	infravermelho, microondas, temperatura, fumaça, vibração
Controle de acesso	biometria, proximidade, bluetooth, rádio frequência
CFTV	câmeras analógicas e IP

segurança obrigatórios na Lei, a agência poderá ser multada e até sofrer interdição. Nesse mister, cumpre destacar a importância do monitoramento em tempo real da disponibilidade dos dispositivos de segurança, de modo que as eventuais falhas sejam identificadas e solucionadas.

De acordo com dados do 16º Anuário Brasileiro de Segurança Pública [FBSP 2022], a taxa de roubos em 2021 cresceu em vários segmentos, com destaque para alta de 11% em instituições financeiras, o que reforça a necessidade de investimentos em novas tecnologias de segurança. Mostrou-se, ainda, que todos os estados brasileiros investiram R$ 157,7 bilhões em segurança pública nos anos de 2020 e 2021, mas apenas R$ 1,9 bilhão foram destinados à inteligência e informação. Sendo assim, o Brasil investiu, nos últimos dois anos, apenas 1,2% do total gasto com segurança na área de inteligência e informação.

Não obstante ao esforço da comunidade acadêmica em disseminar a ciência de dados, inteligência computacional e IoT em soluções corporativas, existe uma lacuna para pesquisas que envolvam segurança de ambientes físicos, sobretudo em instituições financeiras.

A análise de vulnerabilidade de segurança física de uma agência bancária, por exemplo, é realizada de forma pontual, considerando aspectos de localização geográfica, histórico de incidentes, histórico de manutenção, sem considerar a situação instantânea de disponibilidade dos sistemas de segurança. A ponderação do nível de vulnerabilidade varia de acordo o tipo de dado recebido, então, é difícil abstrair uma correlação entre disponibilidade geral do sistema e a vulnerabilidade do ambiente físico. A disponibilidade de um subsistema específico pode ter prioridade sobre os demais sistemas, o que denota o grau de incerteza do trabalho e justifica a utilização da lógica fuzzy.

Diante do contexto, o problema de pesquisa é: Como realizar o monitoramento da disponibilidade de segurança em ambientes físicos através da inteligência computacional? Este trabalho tem por objetivo geral um sistema multiagente baseado em fusão de sensores para avaliação de disponibilidade dos sistemas de segurança e criação do Índice de Vulnerabilidade de Segurança Física (IVSF), visando a tomada de decisão na área de segurança, enquanto que os objetos específicos são: definir as funções dos agentes - fusão de dados, processamento e monitoramento; definir o IVSF; projetar o sistema de inferência baseado em em lógica *fuzzy*; implementar protótipo do sistema multiagente utilizando dispositivos IoT; e avaliar o desempenho do modelo proposto.

A estrutura do trabalho está dividida em 5 seções. Inicialmente, a Seção 1 apresenta a contextualização do problema e os objetivos do trabalho. A Seção 2 mostra os trabalhos relacionados ao tema do trabalho. A Seção 3 especifica a arquitetura do sistema proposto e a implementação do protótipo. A Seção 4 detalha os resultados obtidos e a

avaliação de desempenho da solução proposta. Por fim, a Seção 5 descreve as conclusões e os trabalhos futuros. Os códigos-fontes completos do protótipo, incluindo os resultados, gráficos e tabelas, estão disponíveis no repositório digital *Github* do autor. [1].

2. Trabalhos Relacionados

Para a análise e seleção dos estudos primários, foram utilizadas como fontes de dados as bibliotecas digitais: *ACM Digital Library*, *IEEE Xplore Digital Library* e *ScienceDirect*, nas quais foram executadas as strings de busca no título, resumo e palavras-chaves, no período de 2010 a 2021, conforme Figura 1. Como resultado da análise, foram selecionados os trabalhos de [SIPELE et al. 2018], [ONOFRE et al. 2015], [DAKHLALLAH et al. 2011], [TEJEDOR et al. 2010] e [NETO 2018].

Figura 1. String de busca

```
("multi-agent") AND
("sensor fusion" OR "data fusion" ) AND
("security" OR "safety")
```

O artigo *"Advanced Driver's Alarms System through Multi-agent Paradigm"* [SIPELE et al. 2018] propõe uma arquitetura baseada no paradigma multiagente para projetar um sistema assistente de direção avançada através da fusão de dados. O objetivo principal é projetar um sistema hierárquico capaz de gerenciar o processo de aquisição de conhecimento de todos os aspectos envolvidos na cena de condução, como a ambiente, bem como o comportamento e estado do condutor, fornecendo suporte para construir e testar modelos de raciocínio.

O artigo *"Multi-sensor geo-referenced surveillance system"* [ONOFRE et al. 2015] descreve uma nova arquitetura de sistema de vigilância baseada em eventos georreferenciados de múltiplos sensores e no tratamento dinâmico de eventos. Este sistema pode contribuir para uma resposta eficiente a eventos sobre a localização de eventos e agentes de segurança, bem como reduzir as falhas do sistema com o uso de vários sensores. Uma das áreas de melhoria identificada foi a relação entre o perfil do agente e o desempenho nos tipos de eventos, que pode ser melhorada com o uso de lógica fuzzy.

O artigo *"Application of Sensor Similarity, Complementarity and Type-2 Fuzzy Logic to a Dynamic Security Monitoring System"* [DAKHLALLAH et al. 2011] foi concentrado em um conjunto efetivo de sensores complementares Laser (para medicação de velocidade), Sonar (para varredura espacial) e RF (para direitos de acesso)]. Um novo sistema multiagente foi obtido pela fusão dos tipos de dados sensoriais acima, tirando vantagens de similaridade e conceitos de complementaridade. O estado do sistema é transformado para poder tomar uma decisão de conscientização de segurança, usando lógica *fuzzy* tipo 2 para lidar com a incerteza de cenário de ativos sob vigilância.

Em *"Multi-agent Based Distributed Semi-automatic Sensors Surveillance System Architecture"* [TEJEDOR et al. 2010] é descrita uma arquitetura de monitoramento de

[1] https://github.com/danielgleison/dissertacao

sensores semiautomatizada e de suporte à decisão usada para desenvolver um sistema de monitoramento de sensores inteligentes. A arquitetura proposta é agrupada em três camadas de agentes: a camada de agentes de sensores, camada de agentes de processamento de sensores e, por fim, as camadas de agentes assistentes de suporte. Essa arquitetura propõe um sistema multiagente totalmente descentralizado usando a Linguagem de Comunicação de Agente FIPA.

Por fim, o artigo "*A Multi-agent System Using Fuzzy Logic Applied to eHealth*" [NETO 2018] propõe uma abordagem de sistema multiagente que utiliza dispositivos IoT para captar os sinais cardíacos dos pacientes e, usando processo de lógica *fuzzy*, estima o nível de hipertensão, considerando a pressão sistólica, pressão diastólica, idade e índice de massa corporal. Foram utilizadas informações de 768 pacientes obtidos de um banco de dados público para avaliação do desempenho apresentado no modelo de lógica *fuzzy*. Os resultados foram comparados com avaliação feita por enfermeiros credenciados, alcançando 94,40% de acerto no diagnóstico.

Conforme comparativo da Tabela 2, dos cinco trabalhos relacionados, todos propõem modelos de sistemas multiagentes, três trabalhos utilizam técnicas de fusão de dados, dois trabalhos com processamento de lógica *fuzzy*, apenas um trabalho com protótipo IoT e quatro são aplicados à area de segurança. Diferentemente dos trabalhos relacionados, a proposta deste trabalho abrange todos os tópicos avaliados, ou seja, dispõe de arquitetura multiagente com fusão de dados, lógica *fuzzy* e protótipo IoT, além da aplicabilidade na área de segurança.

Tabela 2. Comparativo entre os trabalhos relacionados

Trabalho	Multiagente	Fusão	Fuzzy	IoT	Área
Advanced Driver's Alarms System through Multi-agent Paradigm	Sim	Sim	Não	Não	Segurança
Multi-sensor geo-referenced surveillance system	Sim	Sim	Não	Não	Segurança
Application of Sensor Similarity, Complementarity and Type-2 Fuzzy Logic to a Dynamic Security Monitoring System	Sim	Sim	Sim	Não	Segurança
Multi-agent Based Distributed Semi-automatic Sensors Surveillance System Architecture	Sim	Não	Não	Não	Segurança
A Multi-agent System Using Fuzzy Logic Applied to eHealth	Sim	Não	Sim	Sim	Saúde
Este	**Sim**	**Sim**	**Sim**	**Sim**	**Segurança**

3. Arquitetura do sistema multiagente para avaliação da disponibilidade de sistemas de segurança

Este trabalho utiliza os conceitos de inteligência computacional e IoT para mitigação do problema de monitoramento da disponibilidade de segurança física de ambientes. Para tanto, foi proposto um sistema multiagente para realização das seguintes funções:

1. Aquisição e fusão de dados de disponibilidade dos sistemas de segurança;
2. Predição do nível de vulnerabilidade baseada em lógica *fuzzy*;
3. Tomada de decisão em tempo real baseada em regras condição-ação.

Os sistemas de segurança física foram divididos em subsistemas, de acordo com o ambiente físico: Sistema de Circuito Fechado de TV (CFTV), Sistema de Controle de Acesso Físico (SCAF) e Sistema de Alarme (SA). A disponibilidade de segurança é representada por indicadores obtidos a partir da fusão dos sensores dos sistemas de segurança física.

O cálculo dos indicadores de disponibilidade dos sistemas de CFTV, SCAF e SA é realizado pela Equação 1.

$$Disponibilidade(Sistema) = \frac{\sum SensoresAtivos(Sistema)}{\sum SensoresMonitorados(Sistema)} \quad (1)$$

Com base nos indicadores de disponibilidade de cada subsistema de segurança, realiza-se a inferência *fuzzy* para obtenção do nível de vulnerabilidade estimado do ambiente. Referido índice de vulnerabilidade, denominado Índice de Vulnerabilidade de Segurança Física (IVSF), foi criado nesta pesquisa para subsidiar a tomada de decisão no segmento de segurança física. De acordo com regras estabelecidas em função da vulnerabilidade, o sistema especialista executa ações no ambiente físico.

Geralmente, os critérios de tomada de decisão em segurança física são definidos através de métodos tradicionais de análise de riscos que utilizam grades de probabilidade qualitativa. Nesse cenário, caso a empresa não tenha um histórico de falhas, o cálculo será feito com base em dados e avaliações subjetivas, a exemplo dos Métodos de Mosler e William T. Fine. O método de Mosler serve de base para a identificação, análise e evolução dos fatores que podem influir na manifestação e concretização da ameaça, projetando o impacto causado em caso de sucesso do ataque pela classe e dimensão de cada risco, enquanto que o método de William T. Fine estabelece prioridade nas ações de gestão da segurança da corporação, integrando o grau de risco com a limitação econômica [PEIXOTO 2006].

Com o IVSF proposto, a tomada de decisão é realizada com base da avaliação da disponibilidade do sistemas de segurança do ambiente, utilizando inteligência computacional *fuzzy*. Para validação da proposta, foi desenvolvido protótipo do sistema multiagente, incluindo dispositivos IoT (Raspberry e ESP8266), softwares embarcados (Python e C++), protocolo de comunicação (MQTT) e plataforma de monitoramento (Node-Red). O fluxograma do modelo proposto, contendo as funções e dados gerados de cada agente, está definido na Figura 2.

3.1. Agente de Fusão de Dados

No agente de fusão de dados é realizada a aquisição e fusão de dados dos sensores de monitoramento, bem como a geração das informações de disponibilidade dos sistemas de segurança. Nessa etapa inicial são utilizados dispositivos IoT para captura do nível de disponibilidade dos subsistemas de videovigilância (CFTV), controle de acesso físico (SCAF) e alarme (SA) que compõem o sistema de segurança física.

A fusão dos dados dos 3 subsistemas é realizada de forma quantitativa complementar (nível 2), onde são combinadas informações de sensores digitais de subsistemas diferentes, permitindo uma visão mais abrangente da situação de vulnerabilidade do ambiente físico. Na Figura 3 está representada a fusão nível 2, sendo que os sensores S1 a S10 monitoram o subsistema CFTV, S11 a S20 o subsistema SCAF, e S21 a S30 o subsistema SA.

3.2. Agente de Processamento

No agente de processamento ocorre o processamento dos dados do agente de fusão de dados para predição do nível de vulnerabilidade, cujos resultados são utilizados para geração

Figura 2. Fluxograma do modelo proposto

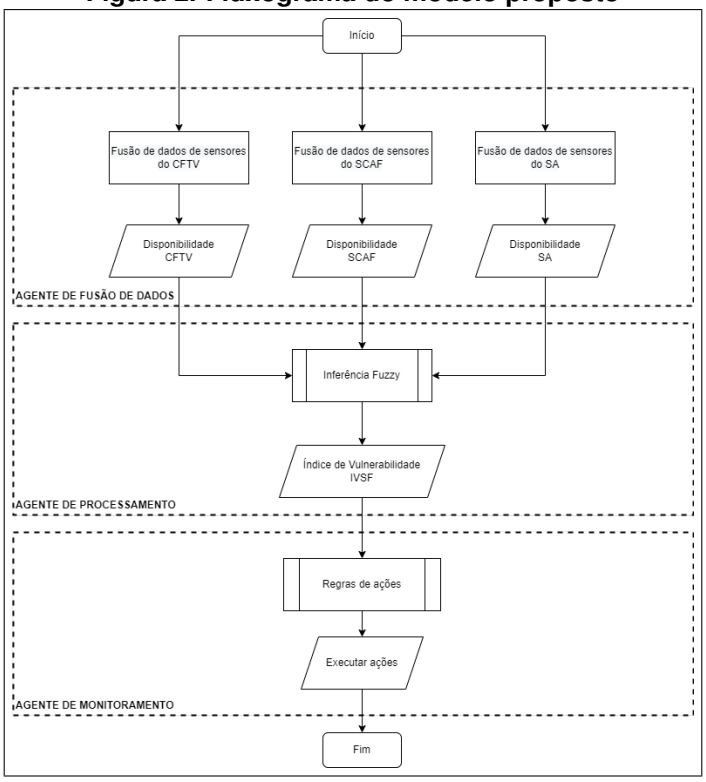
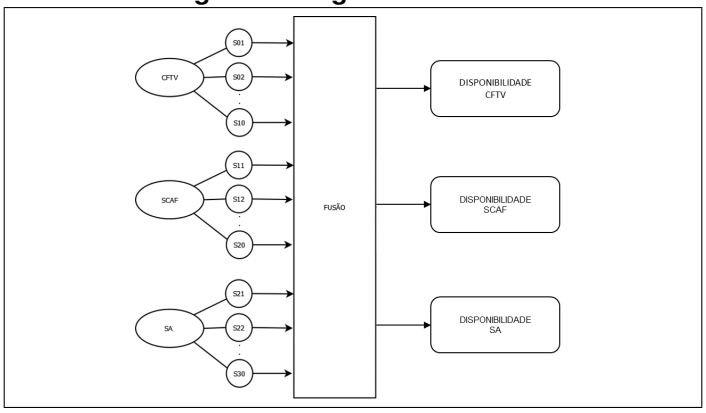


Figura 3. Diagrama de Fusão



do IVSF. Ressalta-se que as informações processadas podem ser criptografadas e armazenadas em banco de dados, porém não fazem parte do escopo deste trabalho.

O mecanismo de inferência é baseado na lógica de conjuntos *fuzzy*, cujas variáveis de entrada são obtidas através da fusão de informações dos dispositivos IoT associados a cada subsistema de segurança física, enquanto que a variável de saída é o índice de vulnerabilidade estimado da agência bancária.

Para tornar a modelagem mais eficiente e equilibrar a quantidade de regras do sistema de inferência, uma estratégia recomendada na literatura consiste em utilizar três termos para as variáveis linguísticas de entrada e cinco termos para a variável linguística de saída (ALTROCK, 1995), conforme Tabela 3.

Tabela 3. Variáveis de Entrada e Saída do Sistema *fuzzy*

Variável Real	Tipo	Universo	Variável Linguística
Disponibilidade CFTV (VE1)	Entrada	[0, 100] (%)	Baixa, Média, Alta
Disponibilidade SCAF (VE2)	Entrada	[0, 100] (%)	Baixa, Média, Alta
Disponibilidade SAI (VE3)	Entrada	[0, 100] (%)	Baixa, Média, Alta
Índice de Vulnerabilidade (VS)	Saída	[0, 100] (%)	Muito Baixo, Baixo, Médio, Alto, Muito Alto

No mecanismo de inferência *fuzzy* deste trabalho utilizou-se das funções de pertinência triangular para os valores intermediários e trapezoidal para os valores linguísticos extremos da faixa de trabalho escolhida. Assim como em [NASCIMENTO 2020], a escolha foi fundamentada pelo fato dos conjuntos extremos serem regiões onde a incerteza é menor, já nos conjuntos intermediários foram considerados regiões de maior incerteza. As funções triangulares e trapezoidais, além de serem bastante simples, geralmente apresentam bons resultados, conforme verificado por [BARUA et al. 2014].

Na lógica *fuzzy*, as variáveis de entrada do sistema são mapeadas em variáveis linguísticas, as quais são utilizadas na definição de regras para o processamento da variável de saída. Considerando que não existe conjunto de dado disponível para o aprendizado supervisionado do problema em questão, a base de conhecimento do sistema de inferência foi gerada a partir de regras condicionais (se-então) definidas por especialista do domínio de aplicação. A base de regras está disponível na Tabela 4. Segundo [AYYUB and KLIR 2006], o especialista é uma pessoa que possui domínio sobre determinado assunto. Desta forma, selecionaram-se cinco especialistas que possuíam mais de 10 anos de experiência na área citada previamente, atenddendo à quantidade proposta por [G.J. and B. 1995].

Na saída do controlador *fuzzy* tem-se o Índice de Vulnerabilidade de Segurança Física (IVSF) que representa a previsibilidade de risco operacional do sistema de segurança física observado, com faixa de trabalho de 0 a 100%.

O modelo do protótipo baseia-se no sistema de controle *fuzzy* com o método de inferência de Mamdani. As variáveis de entrada consideradas são: disponibilidade de CFTV, disponibilidade do SCAF e disponibilidade do SA. A variável de saída é o IVSF. Para essas variáveis, atribuiu-se termos linguísticos, e cada um deles com funções de pertinência dos tipos triangular e trapezoidal. Por meio da análise do conjunto dos dados envolvendo as variáveis mencionadas, pode-se estabelecer uma base de conhecimento com regras linguísticas, relacionado-as a fim de se estimar o valor do IVSF, sendo esse estimado pelo método de defuzzificação do Centro de Gravidade (COG), Bissetor de Área (BOA), Média dos Máximos (MOM), Menor dos Máximos (SOM) e Maior dos Máximos (LOM).

No protótipo foi adotado o sistema de inferência *fuzzy* especificado na Tabela 5. Os intervalos e funções foram definidos pelo autor e podem ser ajustados em posterior processo de otimização. Na Figura 4 tem-se a representação gráfica das funções de pertinência das variáveis de entrada que representam os índices de disponibilidade dos sistemas de CFTV, SCAF e SA, bem como a funções de pertinência da saída correspondentes ao Índice de Vulnerabilidade de Segurança Física (IVSF). As funções de pertinência e o valor da saída *fuzzy* dos Cenários 1 a 4 estão representados na Figura 5.

Tabela 4. Base de Regras do Sistema *fuzzy*

Regra	SE			ENTÃO
	Disponibilidade CFTV	Disponibilidade SCAF	Disponibilidade SA	Vulnerabilidade
R01	Baixa	Baixa	Baixa	Alta
R02	Baixa	Baixa	Média	Alta
R03	Baixa	Baixa	Alta	Alta
R04	Baixa	Média	Baixa	Alta
R05	Baixa	Média	Média	Média
R06	Baixa	Média	Alta	Média
R07	Baixa	Alta	Baixa	Alta
R08	Baixa	Alta	Média	Média
R09	Baixa	Alta	Alta	Média
R10	Média	Baixa	Baixa	Média-Alta
R11	Média	Baixa	Média	Média
R12	Média	Baixa	Alta	Média
R13	Média	Alta	Baixa	Média
R14	Média	Alta	Média	Média
R15	Média	Alta	Alta	Média-Baixa
R16	Média	Média	Baixa	Média
R17	Média	Média	Média	Média
R18	Média	Média	Alta	Média
R19	Alta	Baixa	Baixa	Média-Alta
R20	Alta	Baixa	Média	Média
R21	Alta	Baixa	Alta	Média-Baixa
R22	Alta	Média	Baixa	Média
R23	Alta	Média	Média	Média
R24	Alta	Média	Alta	Baixa
R25	Alta	Alta	Baixa	Média-Baixa
R26	Alta	Alta	Média	Baixa
R27	Alta	Alta	Alta	Baixa

Tabela 5. Funções de pertinência das váriáveis do sistema *fuzzy*

Tipo	Variável Linguística	Universo	Intervalos		Função
Entrada	Disponibilidade CFTV	[0,100]	Baixa Média Alta	[0, 0, 25,50] [25,50,75] [50,75,100,100]	Trapezoidal Triangular
Entrada	Disponibilidade SCAF	[0,100]	Baixa Média Alta	[0, 0, 25,50] [25,50,75] [50,75,100,100]	Trapezoidal Triangular
Entrada	Disponibilidade SA	[0,100]	Baixa Média Alta	[0, 0, 25,50] [25,50,75] [50,75,100,100]	Trapezoidal Triangular
Saída	IVSF	[0,100]	Baixa Média-Baixa Média Média-Alta Alta	[0, 0, 12.5, 25] [12.5, 25, 50] [25, 50, 75] [50, 75, 87.5] [75, 87.5, 100, 100]	Trapezoidal Triangular

O valor estimado de IVSF utilizando o método de defuzzificação COG é obtido pela Equação 2, onde x_i indica o número de amostras, $\mu(x_i)$ é a função de pertinência e

Figura 4. Funções de Pertinência de Entrada (CFTV, SCAF e SA) e Saída (IVSF)

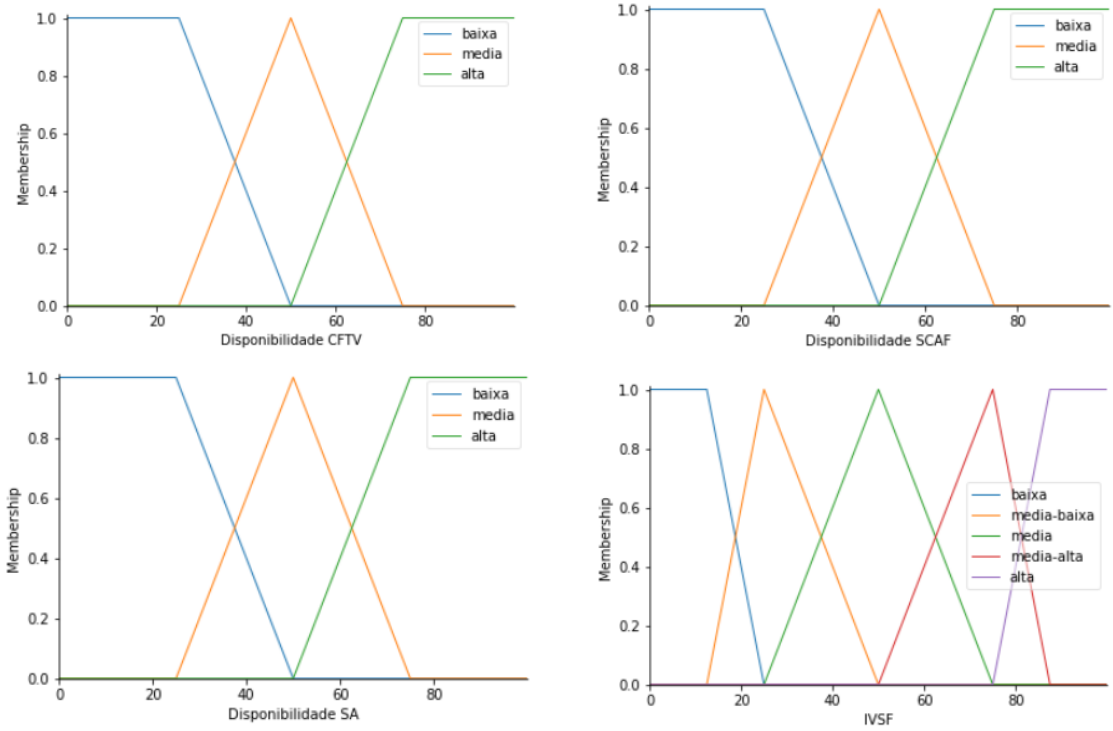
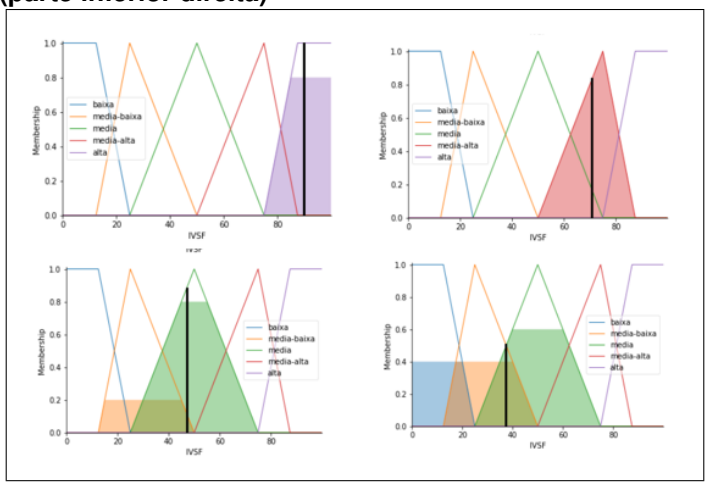


Figura 5. Gráficos de Defuzzificação Mandani COG - Cenário 1 (parte superior esquerda), Cenário 2 (parte superior direita), Cenário 3 (parte inferior esquerda) e Cenário 4 (parte inferior direita)

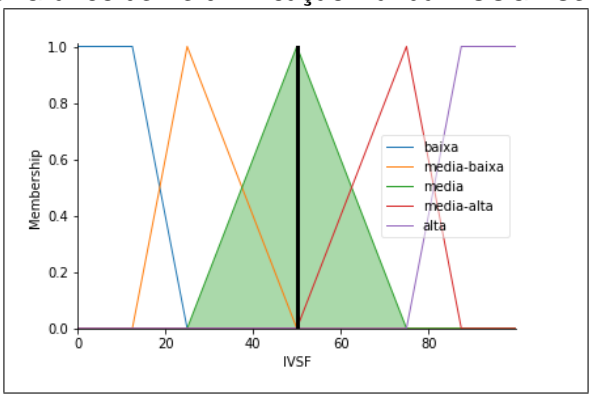


n representa o número de elementos da amostra.

$$X^* = \frac{\sum_{i=1}^{n} x_i \mu(x_i)}{\sum_{i=1}^{n} \mu(x_i)} \tag{2}$$

Para avaliar a desempenho do método proposto foi realizada a análise entre os resultados do IVSF Estimado e IVSF Médio, adotando-se as métricas do *Mean Absolute*

Figura 6. Gráfico de Defuzzificação Mandani COG - Cenário 10



Percentage Error (MAPE) e *Coefficient of Determination* (R^2). As fórmulas de cálculo estão definidas nas Equações 3 e 4, onde $\widehat{x}(t)$ é o IVSF Estimado, $\widetilde{x}(t)$ é o IVSF Médio, $\overline{x}$ refere-se aos valores médios dos registros, e N é o número de pontos do conjunto de dados. Em geral, valores menores de MAPE e valores maiores de R^2 indicam melhor desempenho de previsão [XU et al. 2019].

$$MAPE = \frac{1}{N-p+1} \sum_{p+1}^{N} \left| \frac{\widetilde{x}(t) - \widehat{x}(t)}{\widehat{x}(t)} \right| \tag{3}$$

$$R^2 = 1 - \frac{\sum_{t=p+1}^{N} (\widetilde{x}(t) - \widehat{x}(t))^2}{\sum_{t=p+1}^{N} (\widetilde{x}(t) - \overline{x})^2} \tag{4}$$

3.3. Agente de Monitoramento

O agente de monitoramento executa ações de acordo com o monitoramento dos níveis de vulnerabilidade do agente de processamento. De acordo com a faixa do IVSF extraído, realizar-se-á a tomada de decisão por meio de alertas e ações automáticas visando a mitigação, em tempo real, dos riscos envolvidos. Na Tabela 6 encontram-se as ações executadas pelo sistema proposto, as quais foram definidas pelo autor e podem se adaptar a cada ambiente físico.

Tabela 6. Tomada de Decisão do Sistema *fuzzy*

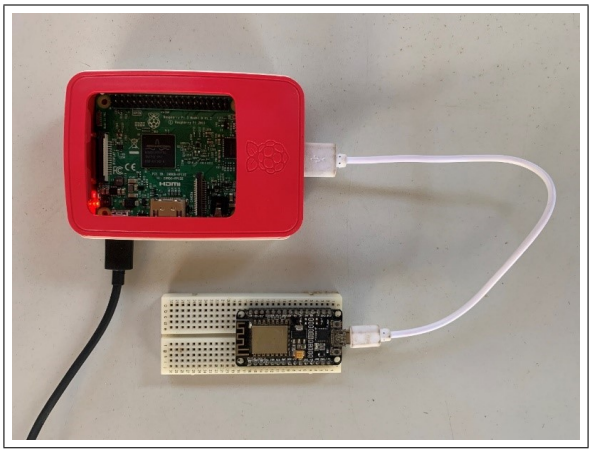
Decisão	IVSF	Ação
D01	0 - 30 (%)	Enviar alerta para a central de operação
D02	31-60 (%)	Enviar alerta para a central de manutenção
D03	61-80 (%)	Ligar a sirene
D04	81-100 (%)	Enviar alerta para a central de segurança

4. Implementação do protótipo do sistema multiagente

Neste trabalho foi realizada a implementação dos três agentes do sistema proposto. As funções dos agentes de fusão de dados e monitoramento foram implementadas no dispositivo ESP8266. O agente de processamento foi implementado no Raspberry, utilizando modelo de inferência *fuzzy* Mandani e biblioteca *Python Scikit-Fuzzy*. Os indicadores de

disponibilidade de CFTV, SA e SCAF da Tabela 7 foram obtidos a partir da simulação de 1.000 sensores de cada sistema. A Figura 7 mostra os dispositivos NodeMCU ESP8266 e *Raspberry* Pi 3, ambos com conexão wi-fi, que foram utilizados no desenvolvimento do protótipo.

Figura 7. *Hardware* do protótipo (Raspberry na parte superior e ESP8266 na parte inferior)



Nesta pesquisa, o protocolo MQTT (Message Queuing Telemetry Transport) foi adotado para interação entre os agentes do modelo proposto, conforme tela do cliente web MQTTBox [MQTTBox 2022] da Figura 8. Para o serviço de broker MQTT, foi utilizado o mesmo Raspberry do agente de processamento. As funções de publicação e assinatura MQTT estão integradas nos códigos de cada agente.

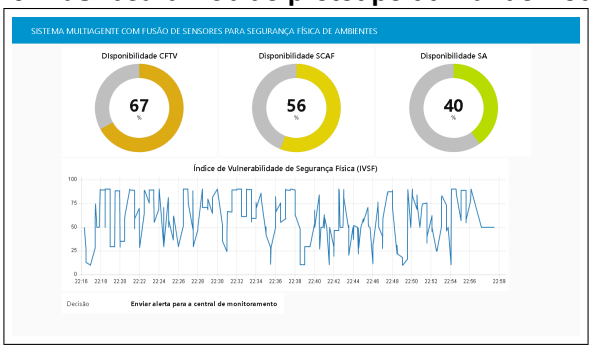
Figura 8. Comunicação MQTT dos agentes

A plataforma Node-Red [NODE-RED 2022] foi utilizada como interface operacional do protótipo para visualização das informações entre os agentes, conforme Figura 9. Node-Red é um ambiente de desenvolvimento baseado em JavaScript que faz uso de Node.js. É usado para desenvolvimento de sistemas IoT conectando *Application Programming Interface* (API), dispositivos de hardware e serviços online e foi desenvolvido pela IBM [FERENCZ and DOMOKOS 2020].

5. Resultados

Na Tabela 7 encontram-se os resultados estimados do IVSF utilizando o modelo Mandani e método defuzzificação COG, considerando os 10 cenários de disponibilidade de CFTV,

Figura 9. Dashboard web do protótipo utilizando Node-Red



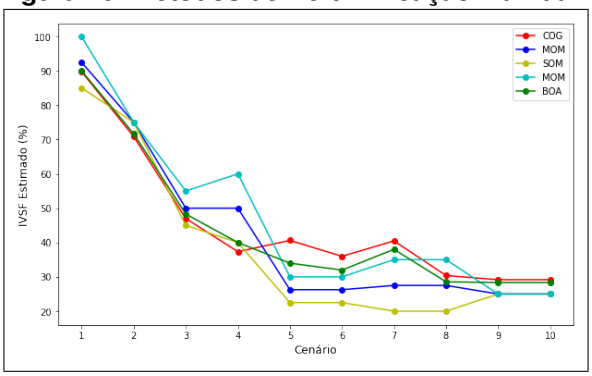
SCAF e SA. Os ambientes físicos com baixa disponibilidade nos sistemas de segurança, possuem alto índice de vulnerabilidade.

Tabela 7. Resultados do sistema *Fuzzy* Mandani COG

Cenário	Disponibilidade CFTV (%)	Disponibilidade SCAF (%)	Disponibilidade SA (%)	IVSF (%)
1	10.00	30.00	10.00	89.74
2	25.00	50.00	50.00	70.83
3	55.00	50.00	50.00	46.99
4	60.00	60.00	50.00	37.32
5	90.00	50.00	45.00	40.61
6	70.00	50.00	50.00	35.98
7	65.00	50.00	50.00	40.46
8	60.00	70.00	50.00	30.37
9	50.00	50.00	90.00	29.17
10	50.00	50.00	80.00	29.17

Na Figura 10, temos a comparação gráfica dos valores de saída IVSF entre os métodos de defuzzificação COG, BOA, MOM, SOM e LOM. Decorrida a estimação da saída *fuzzy*, o modelo realizará automaticamente a tomada de decisão de acordo com as faixas de IVSF e ações estabelecidas. Observa-se que, quanto maior for o IVSF, maior será a criticidade da ação a ser tomada.

Figura 10. Metódos de Defuzzificação Mamdani



Considerando que não existe a informação experimental ou base de conhecimento sobre o IVSF dos cenários de simulação, adotamos a Equação 5 para obtenção do IVSF Médio em função da média da disponibilidade dos sistemas de CFTV, SCAF e SA.

$$\text{IVSF Médio (\%)} = 100 - \text{Disponibilidade Média (\%)} \quad (5)$$

O gráfico da Figura 11 mostra a dispersão entre os valores resultantes do IVSF Médio e IVSF Estimado de cada cenário de simulação. Na Tabela 8 encontram-se os valores de erro MAPE e R^2 do IVSF estimado nos métodos de defuzzificação COG, BOA, MOM, LOM e SOM em relação ao IVSF Médio, obtido a partir da média da disponibilidade dos 10 cenários de simulação. Sobre os resultados, podemos observar que o método de defuzzificação Mamdani COG (Centro de Gravidade) obteve melhor desempenho, apresentado menor erro MAPE (0.150) e maior coeficiente R^2 (0.669) sobre os outros métodos avaliados.

Figura 11. Gráfico de dispersão entre IVSF Estimado e IVSF Médio

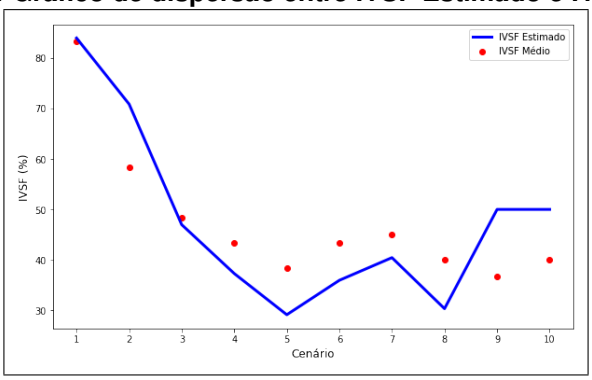


Tabela 8. Comparativo do erro entre o IVSF Estimado e o IVSF Médio por método de defuzzificação Mamdami

Erro	COG	BOA	MOM	LOM	SOM
MAPE	0.150	0.172	0.269	0.309	0.257
R^2	0.669	0.564	0.049	-0.351	0.084

Os tempos de resposta das tarefas do agente de processamento do protótipo, implementado no Raspberry Pi 3, estão indicados na Tabela 9. Os tempos obtidos são referentes a cada processamento do IVSF no sistema *fuzzy*, independentemente da quantidade de sensores monitorados de cada sistema de segurança. Considerando que os sensores dos sistemas de segurança foram simulados, não foi possível obter o tempo total de reposta do agente de fusão de dados.

Tabela 9. Tempos de resposta do agente de processamento

Tarefa	Tempo de Processamento
Assinatura MQTT do agente de fusão de dados	0,174 s
Inferência *fuzzy* do IVSF	2,852 s
Publicação MQTT no agente de monitoramento	0,023 s
Tempo Total	3,049 s

Considerando os valores apurados de erro entre o IVSF estimado no sistema *fuzzy* e o IVSF de referência, mostra-se viável a utilização do modelo proposto para tomada de

decisão em tempo real de acordo com o nível de vulnerabilidade de segurança. Com base nos tempos de processamento dos agentes e no baixo custo de implantação, o protótipo desenvolvido com dispositivos IoT e comunicação MQTT tem potencial para instalação em ambiente real com pontos de monitoramento distribuídos, a exemplo de agências bancárias.

6. Conclusões e Trabalhos Futuros

Para avaliação da disponibilidade de sistemas de segurança, a exemplo do CFTV, SCAF e SA, foi criado o Índice de Vulnerabilidade de Segurança Física (IVSF) a partir de um sistema multiagente com fusão de dados e lógica fuzzy. Nesta pesquisa, o SMA foi estruturado com três agentes: fusão de dados, processamento e monitoramento. Para a estimação do IVSF, utilizou-se o sistema de inferência baseado em lógica *fuzzy*, onde foram definidas as funções de pertinência, regras de condição e métodos de defuzzificação.

Os resultados obtidos pelo sistema *fuzzy* para estimação do IVSF foram considerados satisfatórios. Para fins de comparação, foi aplicada a média dos índices de disponibilidade, sendo que o MAPE e o R^2 foram de 0,15 e 0,67, respectivamente, para o método de defuzzificação COG que obteve o melhor desempenho em relação aos outros métodos avaliados. Na validação do sistema, foi criado protótipo baseado em IoT com sistema de inferência *fuzzy* e comunicação MQTT, cujo tempo total de processamento, de 3,05s, foi considerado satisfatório. Para tanto, foram utilizados os dispositivos Raspberry (controlador *fuzzy* e *broker* MQTT) e ESP8266 (sensores/atuadores), além do software Node-Red (*dashboard web*). Ressalta-se que, para os sensores dos sistemas de segurança, foi utilizada simulação para obtenção dos valores de disponibilidade.

Ademais, o IVSF estimado no modelo proposto pode ser agregado a outros indicadores associados à segurança dos ambientes, a exemplo do risco operacional, histórico de incidentes e criminalidade da região, para obtenção de novo indicador macro de segurança.

Diante do exposto, entendemos que os objetos desta pesquisa foram atingidos e que a implementação do modelo proposto em ambiente físico real tem potencial para suportar a tomada de decisão em situações de vulnerabilidade de segurança.

Por fim, a presente pesquisa pode ser ampliada com os trabalhos futuros relacionados a seguir:

- agregar o IVSF com índices existentes para criação de novos indicadores de segurança;
- comparar o modelo proposto com sistemas de inferência neuro-*fuzzy*;
- implementar o modelo em sistemas com processamento distribuído para redução do tempo de resposta;
- comparar o desempenho do sistema com outros protocolos de comunicação, a exemplo do HTTP REST;
- implementar protótipo com tecnologias móveis, a exemplo do 5G;
- utilizar o modelo com dados de processamento de imagens e visão computacional.

Referências

AYYUB, B. M. and KLIR, G. J. (2006). *Uncertainty Modeling and Analysis in Engineering and the Sciences*. Chapman Hall/CRC.

BARUA, A., MUDUNURI, L., and KOSHELEVA, O. (2014). Why trapezoidal and triangular membership functions work so well: Towards a theoretical explanation. *Journal of Uncertain Systems*, 8:164–168.

BRASIL (1983). Lei n° 7.102, de 20 de junho de 1983. Dispõe sobre a segurança para estabelecimentos financeiros. *Diário Oficial da República Federativa do Brasil*.

BRASIL (2012). Portaria 3.233/2012 - DG/DPF, de 10 de dezembro de 2012. *Diário Oficial da República Federativa do Brasil*.

DAKHLALLAH, T., ZOHDY, M., and SALIM, O. (2011). Application of sensor similarity, complementarity and type-2 fuzzy logic to a dynamic security monitoring system.

FBSP (2022). Anuário brasileiro de segurança publica 2022. `https://forumseguranca.org.br/wp-content/uploads/2022/06/anuario-2022.pdf`.

FERENCZ, K. and DOMOKOS, J. (2020). Using node-red platform in an industrial environment.

G.J., K. and B., Y. (1995). *Fuzzy sets and fuzzy logic: theory and applications*. Prentice Hall.

MARCONDES, J. S. (2022). Vulnerabilidade de segurança: O que é, classificação, exemplos. `https://gestaodesegurancaprivada.com.br/vulnerabilidade-de-seguranca-o-que-e-classificacao-exemplos`.

MQTTBox (2022). Mqttbox. `(https://chrome.google.com/webstore/detail/mqttbox/kaajoficamnjijhkeomgfljpicifbkaf)`.

NASCIMENTO, L. R. D. S. (2020). Proposta fuzzy para avaliação do desenvolvimento sustentável: um estudo de caso para o brasil. Mestrado, Universidade Estadual Paulista Júlio de Mesquita Filho, Sorocaba.

NETO, A. B. L. (2018). A multi-agent system using fuzzy logic applied to e-health in order to monitor hypertension. Mestrado, Universidade Estadual do Ceará, Fortaleza.

NODE-RED (2022). Node-red. `https://nodered.org/`.

ONOFRE, S., SOUSA, P., and PIMENTÃO, J. P. (2015). Multi-sensor geo-referenced surveillance system. In *2015 10th International Symposium on Mechatronics and its Applications (ISMA)*, pages 1–6.

PEIXOTO, M. C. P. (2006). *Engenharia social Segurança da informação na gestão corporativa*. Brasport.

SIPELE, O., ZAMORA, V., ESPINO, A., and MIGUEL, A. (2018). Advanced driver's alarms system through multi-agent paradigm.

TEJEDOR, J., PATRICIO, M. A., and MOLINA, J. M. (2010). Multi-agent based distributed semi-automatic sensors surveillance system architecture. In de Leon F. de Carvalho, A. P., Rodriguez-Gonzalez, S., De Paz Santana, J. F., and Rodriguez, J. M. C., editors, *Distributed Computing and Artificial Intelligence*, pages 317–324, Berlin, Heidelberg. Springer Berlin Heidelberg.

XU, W., HU, H., and YANG, W. (2019). Energy time series forecasting based on empirical mode decomposition and frbf-ar model. *IEEE Access*, 7:36540–36548.