Lógica Nebulosa Aplicada a um Sistema de Detecção de Possíveis Invasões na Rede de Computadores

Eduarda Elger
Centro de Ciências Exatas e Tecnológicas
Universidade Estadual do Oeste do Paraná
Cascavel, Paraná, Brasil
eduarda.elger@unioeste.br

Ellen Carine Bonafin Marques
Centro de Ciências Exatas e Tecnológicas
Universidade Estadual do Oeste do Paraná
Cascavel, Paraná, Brasil
ellen.marques1@unioeste.br

Heloisa Aparecida Alves
Centro de Ciências Exatas e Tecnológicas
Universidade Estadual do Oeste do Paraná
Cascavel, Paraná, Brasil
heloisa.alves@unioeste.br

1. Introdução

Redes de computadores e sistemas de segurança são duas áreas em que a lógica *Fuzzy*, se enquadra de forma positiva por ser uma ferramenta poderosa para lidar com informações imprecisas. No contexto da segurança de redes de computadores, a proteção de dados confidenciais e a prevenção de acesso não autorizado dependem significativamente da detecção precoce de possíveis invasões na rede. As complexidades e ambivalências ligadas a este processo não podem ser adequadamente abordadas por sistemas convencionais baseados em raciocínio claro. Para solucionar esses desafios, a aplicação da lógica *Fuzzy* em sistemas de detecção tem se mostrado uma estratégia promissora.

Na lógica *Fuzzy*, o princípio central reside no uso de conjuntos *Fuzzy*, que possibilitam a representação de graus de pertinência em relação a um conjunto específico. Através desses conjuntos, é possível lidar com a imprecisão e a incerteza presentes em muitos problemas do mundo real. As regras de inferência são definidas utilizando operadores Fuzzy, que combinam os graus de pertinência para obter resultados mais flexíveis e adaptáveis. Essa abordagem permite uma análise mais refinada e realista, levando em conta a natureza ambígua e imprecisa dos dados.

Nesse contexto, será demonstrado de forma prática a implementação de um sistema de lógica *fuzzy* na área de redes de computadores. O presente artigo está subdividido em: segurança da rede (seção 2); estudo de caso (seção 3); modelagem e testes (seção 4) contendo informações sobre a implementação do sistema; na seção 5 são apresentados os resultados, seguidos do parecer do especialista na área (seção 6); e na seção 7 as considerações finais.

2. Segurança na Rede

A segurança de rede é uma condição primordial que visa preservar sistemas contra riscos de ataques cibernéticos que possam afetar seus dados, envolvendo desenvolvimentos de ações e leis que se propõem a certificar a confidenciabilidade e integridade de informações que se deslocam pela rede. Isso compromete o uso de firewalls, sistemas de detecção e prevenção de intrusões, autenticação robusta, criptografia e um gerenciamento adequado de acesso e permissões. Além disso, o conhecimento por parte

dos usuários é essencial para prevenir ataques e viabilizar uma cultura de segurança (Palo Alto Networks, 2023).

Quando ocorre uma violação de segurança, há o risco de acesso não autorizado a dados, aplicativos, redes ou dispositivos de computador. Isso pode resultar em perdas financeiras, danos à reputação e até consequências legais para uma organização. Mesmo em redes pequenas, é essencial considerar ameaças e vulnerabilidades de segurança ao planejar sua implantação. Uma abordagem eficaz de segurança de rede leva em consideração as vulnerabilidades conhecidas, bem como a atividade criminosa e as tendências de ataque atuais. Ao estar ciente desses fatores, é possível implementar medidas adequadas para proteger a rede e minimizar os riscos de violação de segurança.

Uma maneira de resolver essa questão da vulnerabilidade, são os SDIs ou sistemas de detecção de intrusos, atuam na captação de atividades dissimuladas e com potencial de ameaça. Tais sistemas foram planejados a fim de monitorar a atividade de tráfego com conduta maliciosa ou invasões. (Scrafone, 2007). Existem dois principais tipos de sistemas de detecção de intrusos, o primeiro é os sistemas baseados em assinatura: Esses sistemas comparam o tráfego de rede com uma biblioteca de assinaturas conhecidas de ataques e malware. Se uma correspondência for encontrada, o SDI emite um alerta. Esses sistemas são eficazes para detectar ataques conhecidos, mas podem não ser capazes de identificar ataques novos ou variantes de ataques existentes. O segundo são os sistemas baseados em comportamento: Esses sistemas monitoram o tráfego de rede e analisam o comportamento dos dispositivos e usuários em busca de desvios do padrão normal. Eles estabelecem um perfil de comportamento esperado e alertam quando ocorrem atividades anormais ou suspeitas. Esses sistemas são mais eficazes na detecção de ameaças desconhecidas e ataques sofisticados.

3. Estudo de Caso

O presente artigo apresenta o estudo de caso da segurança na rede de computadores utilizando a lógica *fuzzy*, uma abordagem que lida com a complexidade e incerteza associadas à proteção dos sistemas de informação. A lógica *fuzzy* permite uma modelagem mais flexível e adaptável dos sistemas de segurança, levando em consideração não apenas os valores binários de "verdadeiro" ou "falso", mas também a possibilidade de graduações intermediárias. Neste artigo, será explorada a aplicação prática da lógica *fuzzy* na detecção e prevenção de ataques cibernéticos, analisando como essa abordagem pode contribuir para aprimorar as estratégias de defesa e fortalecer a proteção das redes de computadores. Além disso, serão discutidos o processo da implementação da lógica *fuzzy* nesse contexto, bem como possíveis direções futuras de pesquisa nessa área promissora da segurança cibernética.

4. Modelagem e Testes

Para a modelagem e testes do sistema, foi utilizado o software interativo para o cálculo numérico: *MatLab* versão R2023a, junto com a sua *ToolBox Fuzzy,* que permite projetar e testar o sistema de inferência *fuzzy.*

4.1 Aquisição de Conhecimento

A aquisição do conhecimento para a construção do sistema se deu por meio de entrevistas com um especialista na área e consultas de artigos didáticos. O especialista entrevistado foi o Professor Doutor Luiz Antônio Rodrigues do curso de Ciência da Computação da Universidade Estadual do Oeste do Paraná Campus de Cascavel, possui conhecimento nas áreas de redes de computadores e sistemas distribuídos, e programação de sistemas. Já os artigos didáticos estudados estão disponíveis na seção apêndice desse documento.

4.2 Variáveis de Entrada e Saída

O sistema de inferência da rede é constituído por três variáveis de entrada do tipo trapezoidal, sendo elas: número de conexões, tamanho dos pacotes e a frequência de transmissão. O número de conexões é definido por vezes de acessos, pode ser utilizado para detectar tentativas de varredura de portas ou outros tipos de atividades suspeitas que envolvam muitas conexões em um curto período. O tamanho dos pacotes é representado pela quantidade de *bytes*, identifica tráfego de rede incomum, como o envio de grandes quantidades de dados que podem ser indicativos de uma transferência de arquivos ou de uma infiltração de dados. A frequência de transmissão é calculada em milissegundos (ms), detecta comportamentos incomuns, como um tráfego de rede muito intenso em momentos em que normalmente o tráfego é baixo.

Para a saída do sistema há apenas a variável de tipo trapezoidal: risco na rede. Através dela podemos obter três possíveis resultados: risco baixo, médio ou alto. Esses resultados representam a probabilidade que haver um risco na rede com base na situação adquirida pelo valor das entradas.

Cada uma das variáveis recebem um valor em *crisp*, ou seja, um valor numérico preciso e definido. A partir daí o módulo de *fuzzificação* modela esses valores para conjunto *fuzzy* com seus respectivos domínios, através dessa etapa que utilizamos o conhecimento fornecido pelo especialista para moldar os dados. Como a entrada do sistema é um valor *crisp* a saída também deverá ser um valor *crisp*, a *defuzzyficação* desse processo será mais detalhada na seção 4.5 desse módulo.

Abaixo temos a Tabela 1 com os valores de cada uma das variáveis.

Variáveis			
Entrada			**Faixa**
Número de Conexões	**poucas**	[50 150]	[0 1000]
	algumas	[200 400]	
	muitas	[500 1000]	
Tamanho dos Pacotes	**pequenos**	[20 30]	[0 100]
	médios	[50 60]	
	grandes	[80 100]	
Frequência de Transmissão	**baixa**	[1 2]	[0 10]
	média	[3 6]	
	alta	[7 10]	
Saída			
Risco	**baixo**	[10 30]	[0 100]

	médio	[50 60]	
	alto	[80 100]	

Tabela 1 – Valores das variáveis.

Para representar variáveis nebulosas utilizamos as funções de pertinência, elas facilitam expressar e lidar com observações e medidas incertas ou imprecisas. A partir dos intervalos das entradas calculamos o grau de pertinência, as funções trapezoidais utilizam um vetor X de valores reais e 4 parâmetros (a, b, m, n, onde):

- A e B são a parte inferior do trapézio.
- M e N são a parte superior do trapézio, nesses pontos os valores de pertinência é 1.

Abaixo na Figura 1 está a representação das funções de pertinência utilizada para as variáveis de entrada, veremos os resultados delas nos testes realizados na seção 5.

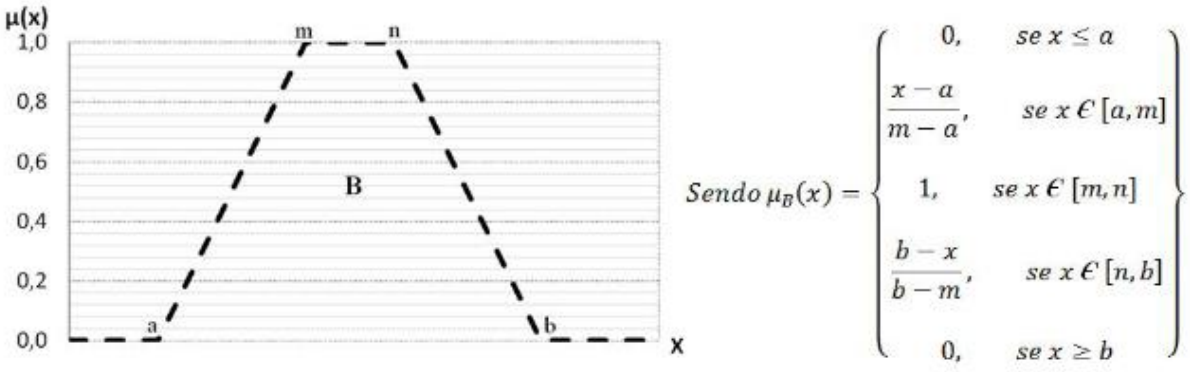

Figura 1 – Função de pertinência trapezoidal. Fonte: Zimmermann (1991).

Os valores utilizados nas extremidades do trapézio foram definidos a partir do conhecimento do especialista, nas Figuras 2, 3 e 4 são apresentados os parâmetros das variáveis.

Name	Type	Parameters
poucas	Trapezoidal	[0 50 150 200]
algumas	Trapezoidal	[150 200 400 450]
muitas	Trapezoidal	[400 500 1000 1200]

Figura 2 – Parâmetros do Número de Conexões.

Name	Type	Parameters
pequenos	Trapezoidal	[0 20 30 40]
médios	Trapezoidal	[25 50 60 70]
grandes	Trapezoidal	[55 80 100 150]

Figura 3 – Parâmetros do Tamanho dos Pacotes.

Name	Type	Parameters
baixa	Trapezoidal	[0 1 2 3]
média	Trapezoidal	[2 3 6 7]
alta	Trapezoidal	[5 7 10 15]

Figura 4 – Parâmetros da Frequência de transmissão.

Logo abaixo nas Figuras 5, 6, 7 e 8 temos a Modelagem do Sistema de Inferência das entradas e da saída.

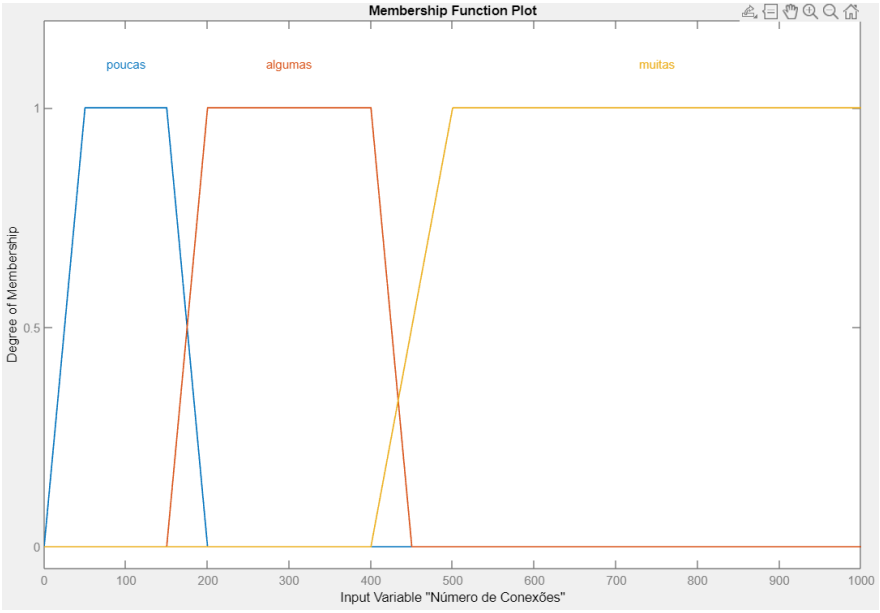

Figura 5 – Modelagem do Sistema de Inferência: número de conexões.

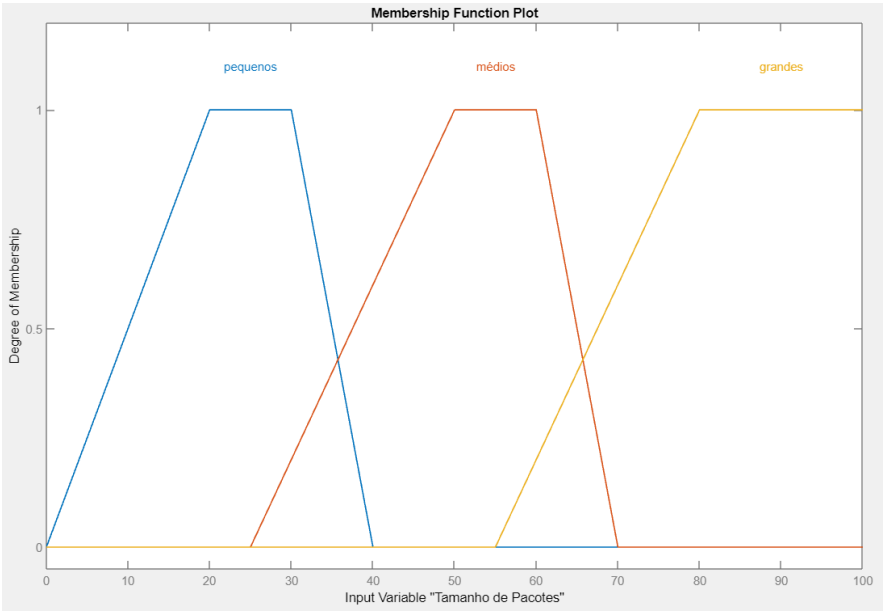

Figura 6 – Modelagem do Sistema de Inferência: tamanho de pacotes.

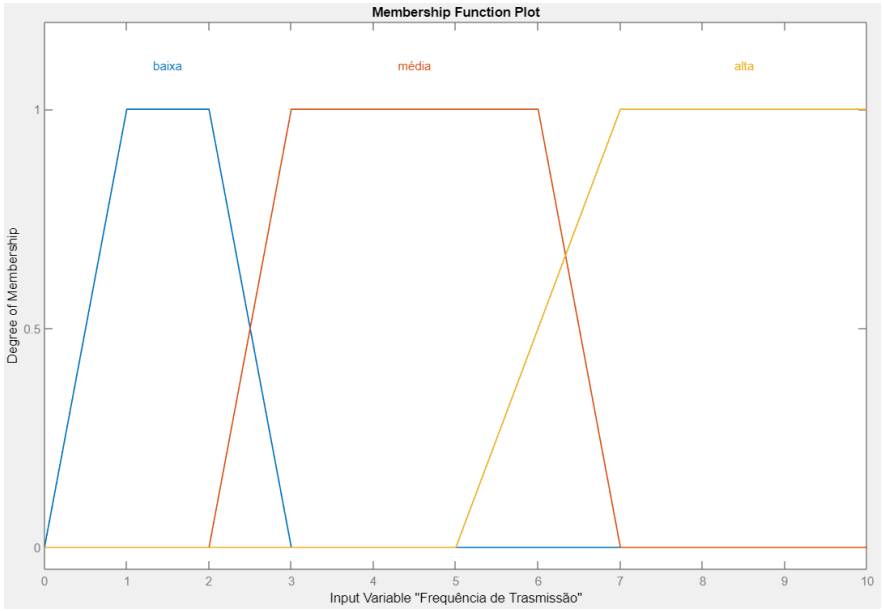

Figura 7 – Modelagem do Sistema de Inferência: frequência de transmissão.

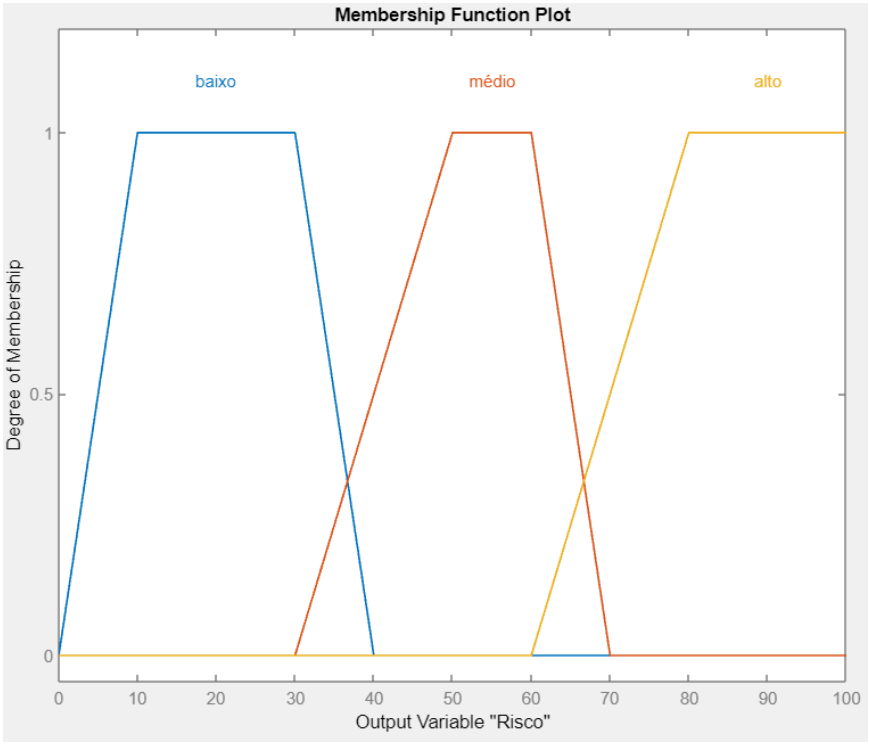

Figura 8 – Modelagem do Sistema de Inferência: risco.

A Figura 9 ilustra o sistema de inferência completo, com as três variáveis de entrada, mais o método de inferência e a saída.

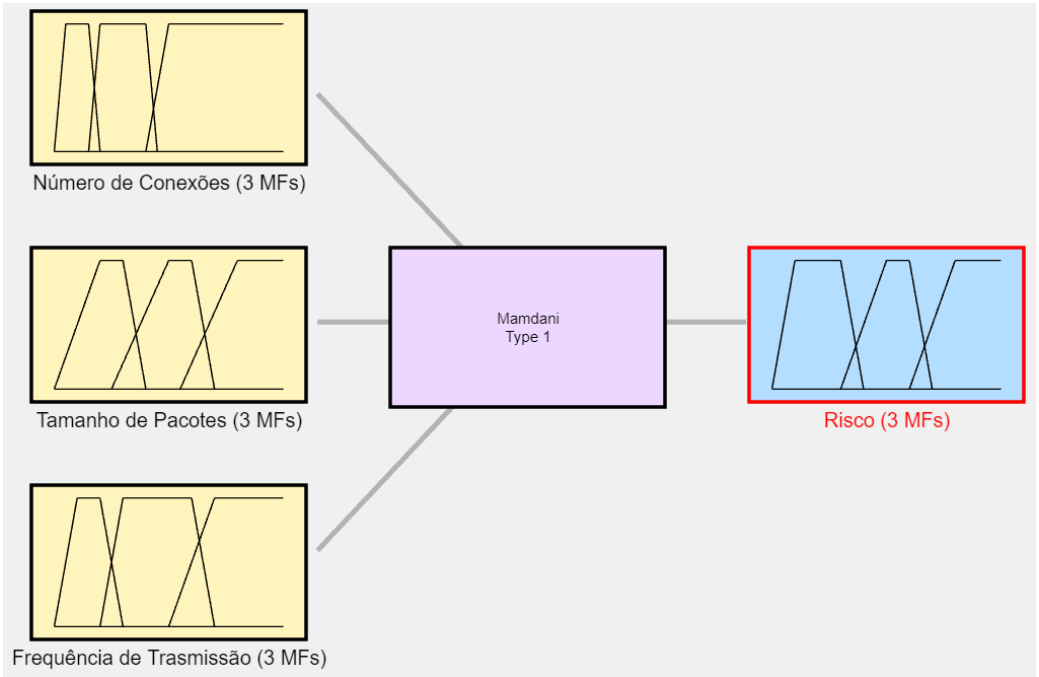

Figura 9 – Sistema de Inferência da Rede.

4.3 Regras Utilizadas

Para fazermos as deduções lógicas a partir dos fatos conhecidos utilizamos as regras de inferência, elas auxiliam na automação do raciocínio e a tomada de decisões. As regras de inferência foram definidas através de todas as combinações possíveis entre as variáveis de entrada, totalizando cerca de vinte e sete regras. Na Tabela 2 é demonstrada cada uma das regras de inferência utilizadas para a implementação do sistema nebuloso.

Regras de Inferência			
Nº conexões	**Tamanho dos pacotes**	**Frequência de Transmissão**	**Risco na Rede**
Poucas	Pequenos	Baixa	Baixo
Poucas	Pequenos	Média	Médio
Poucas	Pequenos	Alta	Médio
Poucas	Médios	Baixa	Baixo
Poucas	Médios	Média	Médio
Poucas	Médios	Alta	Alto
Poucas	Grandes	Baixa	Baixo
Poucas	Grandes	Média	Médio
Poucas	Grandes	Alta	Alto
Algumas	Pequenos	Baixa	Baixo
Algumas	Pequenos	Média	Médio
Algumas	Pequenos	Alta	Médio
Algumas	Médios	Baixa	Baixo
Algumas	Médios	Média	Médio
Algumas	Médios	Alta	Alto
Algumas	Grandes	Baixa	Baixo
Algumas	Grandes	Média	Alto
Algumas	Grandes	Alta	Alto
Muitas	Pequenos	Baixa	Baixo
Muitas	Pequenos	Média	Médio
Muitas	Pequenos	Alta	Alto
Muitas	Médios	Baixa	Médio
Muitas	Médios	Média	Médio
Muitas	Médios	Alta	Alto
Muitas	Grandes	Baixa	Baixo
Muitas	Grandes	Média	Médio
Muitas	Grandes	Alta	Alto

Tabela 2 – Regras de Inferência.

4.4 Método de Inferência

O método de inferência utilizado foi o Mamdani para criar um sistema de controle sintetizando um conjunto de regras de controle linguístico obtidas de operadores humanos experientes, “os sistemas Mamdani têm bases de regras mais intuitivas e fáceis de entender, eles são adequados para aplicativos de sistemas especializados em que as regras são criadas a partir do conhecimento especializado humano, como diagnósticos médicos” (The MathWorks, 2023).

4.5 Método de *Defuzzificação*

Para realizar a *defuzzificação*, ou seja, converter as variáveis fuzzy em valores crispis (números precisos), foi utilizada a técnica de *defuzzificação* centroide. Esse método utiliza o conceito centroide geométrico ponderado para determinar o valor crisp. O centroide é calculado multiplicando cada valor do universo do discurso pelo grau de pertinência correspondente e, em seguida, dividindo a soma desses produtos pelo somatório dos graus de pertinência.

4.6 Apresentação para o usuário

Para apresentarmos os resultados foi implementado um pseudocódigo chamado **TesteRedes.m**, onde utilizamos a função ***evalfis*** do próprio MatLab para avaliar o sistema de inferência *fuzzy* (FIS) e calcular as saídas com base nas entradas fornecidas. Abaixo está uma representação do pseudocódigo implementado.

```
function TesteRedes()
    % Exemplifica a utilizacao dos modelos fuzzy criados pelo FIS
    % dentro de codigo Matlab

    % Le o modelo fuzzy criado com o FIS
    Modelo = readfis('redes.fis');

    % entrando com os valores de entrada para nº conexões,
    % tamanho dos pacotes e a frequência de transmissão
    continua = 's';

    while (continua == 's')
        conexoes = input('Informe o numero de conexoes: >> ');
        pacotes = input('Qual o tamanho do pacote? >> ');
        transmissao = input('Qual a taxa de transmissao? >> ');

        % avaliação
        risco = evalfis(Modelo, [conexoes, pacotes, transmissao]);

        fprintf('\nRisco na Rede (probabilidade):');
        disp(risco);

        categoria = "";

        if(risco < 37)
            categoria = "baixo";
        elseif(risco < 67)
            categoria = "medio";
        else
```

```
            categoria = "alto";
        end

        fprintf("Categoria do risco: %s\n", categoria);

        continua = input('continua ? (s/n): ','s');
    end
end
```

Além disso, foi utilizado como base para a classificação dos dados, um gráfico gerado pelo próprio Matlab com a função **Membership**, que resultou a modelagem do Sistema de Inferência: Risco, onde demonstra os pontos de intersecção entre a transição de categorias, ou seja, demonstra o momento em que muda de uma classificação para outra. A Figura 10 exemplifica esse processo.

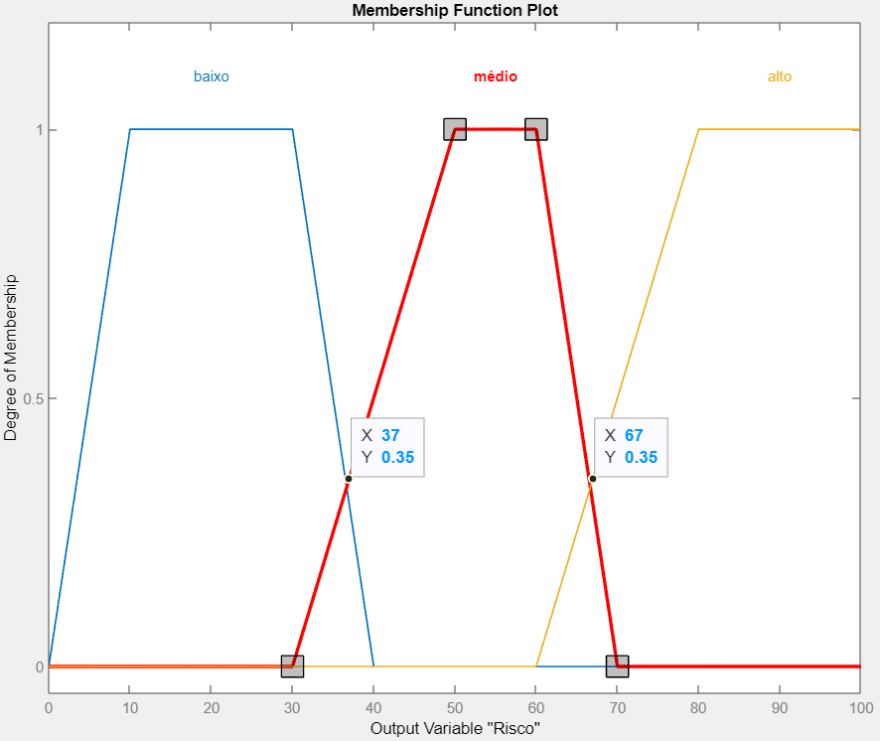

Figura 10 – Classificação de dados com a Modelagem do Sistema de Inferência do Risco.

5. Análise de Resultados

Após finalizarmos a implementação, foi realizado então alguns testes com a finalidade de visualizar a probabilidade de risco na rede e as classificações conforme as entradas fornecidas pelo usuário. Estas classificações podem ser visualizadas através da Tabela 2. Após os resultados aplicamos a função de inferência vista na Figura 1 para cada um dos valores de entrada para cada situação.

Para iniciar será realizado o teste para a classificação “baixo”, conforme demonstrado abaixo na Figura 11.

```
Informe o numero de conexoes: >> 30
Qual o tamanho do pacote? >> 43
Qual a taxa de transmissao? >> 2

Risco na Rede (probabilidade):   20.0000

Categoria do risco: baixo
```

Figura 11 – Teste risco baixo.

Aplicação do cálculo do grau de pertinência com os parâmetros definidos na modelagem das variáveis para o valor x = 30 pode ser vista na Tabela 3.

Número de conexões		**Valor de pertinência**
poucas	[0 50 120 200]	0,6
algumas	[150 200 400 450]	0
muitas	[400 500 1000 1200]	0

Tabela 3 – Grau de pertinência para X = 30.

Aplicação do cálculo do grau de pertinência com os parâmetros definidos na modelagem das variáveis para o valor x = 43 pode ser vista na Tabela 4.

Tamanho dos pacotes		**Valor de pertinência**
pequenos	[0 20 30 40]	0
médios	[25 50 60 70]	0,72
grandes	[55 80 100 150]	0

Tabela 4 – Grau de pertinência para X = 43.

Aplicação do cálculo do grau de pertinência com os parâmetros definidos na modelagem das variáveis para o valor x = 2 pode ser vista na Tabela 5.

Tempo de transmissão		**Valor de pertinência**
baixa	[0 1 2 3]	1
média	[2 3 6 7]	0
alta	[5 7 10 15]	0

Tabela 5 – Grau de pertinência para X = 2.

Posteriormente, realizamos então os testes para a classificação posterior, sendo ela “médio” (Figuras 12 e 13). Para isto foi concedido valores diferentes do teste anterior, sendo maiores, para que mudasse de classificação final.

```
Informe o numero de conexoes: >> 200
Qual o tamanho do pacote? >> 65
Qual a taxa de transmissao? >> 5

Risco na Rede (probabilidade):   65.8527

Categoria do risco: medio
```

Figura 12 – Teste risco médio.

Aplicação do cálculo do grau de pertinência com os parâmetros definidos na modelagem das variáveis para o valor x = 200 pode ser vista na Tabela 6.

Número de conexões		**Valor de pertinência**
poucas	[0 50 120 200]	0
algumas	[150 200 400 450]	1
muitas	[400 500 1000 1200]	0

Tabela 6 – Grau de pertinência para X = 200.

Aplicação do cálculo do grau de pertinência com os parâmetros definidos na modelagem das variáveis para o valor x = 65 pode ser vista na Tabela 7.

Tamanho dos pacotes		**Valor de pertinência**
pequenos	[0 20 30 40]	0
médios	[25 50 60 70]	1.6
grandes	[55 80 100 150]	1.75

Tabela 7 – Grau de pertinência para X = 65.

Aplicação do cálculo do grau de pertinência com os parâmetros definidos na modelagem das variáveis para o valor x = 5 pode ser vista na Tabela 8.

Tempo de transmissão		**Valor de pertinência**
baixa	[0 1 2 3]	0

média	[2 3 6 7]	3
alta	[5 7 10 15]	1.6

Tabela 8 – Grau de pertinência para X = 5.

Note que no teste da Figura 12 as entradas para adquirir o risco médio foram maiores do que na Figura 13. Isso significa que não necessariamente as entradas têm que ser maiores para obtermos um risco mais elevado, mas sim as regras de inferência que atuam sobre esses valores definem qual vai ser a saída final.

```
Informe o numero de conexoes: >> 47
Qual o tamanho do pacote? >> 36
Qual a taxa de transmissao? >> 3

Risco na Rede (probabilidade):   51.0191

Categoria do risco: medio
```

Figura 13 – Teste risco médio.

Aplicação do cálculo do grau de pertinência com os parâmetros definidos na modelagem das variáveis para o valor x = 47 pode ser vista na Tabela 9.

Número de conexões		**Valor de pertinência**
poucas	[0 50 120 200]	0,94
algumas	[150 200 400 450]	0
muitas	[400 500 1000 1200]	0

Tabela 9 – Grau de pertinência para X = 47.

Aplicação do cálculo do grau de pertinência com os parâmetros definidos na modelagem das variáveis para o valor x = 36 pode ser vista na Tabela 10.

Tamanho dos pacotes		**Valor de pertinência**
pequenos	[0 20 30 40]	0,6
médios	[25 50 60 70]	0
grandes	[55 80 100 150]	0

Tabela 10 – Grau de pertinência para X = 36.

Aplicação do cálculo do grau de pertinência com os parâmetros definidos na modelagem das variáveis para o valor x = 3 pode ser vista na Tabela 11.

Tempo de transmissão		Valor de pertinência
baixa	[0 1 2 3]	1
média	[2 3 6 7]	1
alta	[5 7 10 15]	0

Tabela 11 – Grau de pertinência para X = 3.

Por fim, foi realizado o teste para a última classificação, sendo ela “alto”. Novamente modificamos os valores, e aumentamos eles conforme a Tabela 2. Sendo assim, finalizamos os testes, demonstrando todas as classificações, abaixo na Figura 14 com a classificação “alto”.

```
Informe o numero de conexoes: >> 300
Qual o tamanho do pacote? >> 65
Qual a taxa de transmissao? >> 7

Risco na Rede (probabilidade):   82.6338

Categoria do risco: alto
```

Figura 14 – Teste risco baixo.

Aplicação do cálculo do grau de pertinência com os parâmetros definidos na modelagem das variáveis para o valor x = 300 pode ser vista na Tabela 12.

Número de conexões		Valor de pertinência
poucas	[0 50 120 200]	0
algumas	[150 200 400 450]	3
muitas	[400 500 1000 1200]	0

Tabela 12 – Grau de pertinência para X = 300.

Aplicação do cálculo do grau de pertinência com os parâmetros definidos na modelagem das variáveis para o valor x = 65 pode ser vista na Tabela 13.

Tamanho dos pacotes		Valor de pertinência
pequenos	[0 20 30 40]	0

médios	[25 50 60 70]	1.6
grandes	[55 80 100 150]	1.75

Tabela 13 – Grau de pertinência para X = 65.

Aplicação do cálculo do grau de pertinência com os parâmetros definidos na modelagem das variáveis para o valor x = 7 pode ser vista na Tabela 14.

Tempo de transmissão		**Valor de pertinência**
baixa	[0 1 2 3]	0
média	[2 3 6 7]	5
alta	[5 7 10 15]	1

Tabela 14 – Grau de pertinência para X = 7.

6. Parecer do Especialista

O embasamento teórico da área de redes está coerente. O estudo de caso apresenta consistência conforme a metodologia e o objetivo propostos.

7. Considerações Finais

Em conclusão, este artigo apresentou a aplicação da lógica *Fuzzy* na segurança de redes de computadores como uma estratégia promissora para lidar com a imprecisão e ambiguidade dos dados. A lógica Fuzzy permitiu a representação de graus de pertinência, possibilitando uma análise mais refinada e realista dos sistemas de segurança. O estudo de caso apresentado demonstrou a implementação prática de um sistema de detecção de intrusos utilizando e mostrando como essa abordagem pode contribuir para melhorar as estratégias de defesa e fortalecer a proteção das redes.

Os resultados obtidos com o desenvolvimento do sistema de inferência *Fuzzy* foram explorados e discutidos, expondo a efetividade dessa abordagem na detecção e prevenção de ataques cibernéticos. No entanto, é importante ressaltar que a lógica *Fuzzy* na segurança de redes de computadores é uma área em constante evolução, e pesquisas futuras podem explorar novas técnicas e aprimoramentos para apurar ainda mais a eficácia dos sistemas de defesa.

Apêndice

A. Midzic, Z. Avdagic and S. Omanovic. **Intrusion detection system modeling based on neural networks and fuzzy logic**. *2016 IEEE 20th Jubilee International Conference on Intelligent Engineering Systems (INES)*, Budapest, Hungary, 2016, pp. 189-194, doi: 10.1109/INES.2016.7555118. Disponível em: https://ieeexplore.ieee.org/abstract/document/7555118. Acesso em 28 de abril de 2023.

Al senawi, Hiba & Najjar, Firas. **A Study to investigate the possibility of using a decision making model with IPS**. 2012. ResearchGate. Disponível em: https://www.researchgate.net/publication/243458113_A_Study_to_investigate_the_possibility_of_using_a_decision_making_model_with_IPS. Acesso em 29 de abril de 2023.

JI, Carolina Yoshico; et al. **Lógica nebulosa aplicada a um sistema de detecção de intrusos em computação em nuvem**. 2013. 224 f. Dissertação (Mestrado em Redes de Telecomunicações; Sistemas Inteligentes e Automação) - Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2013. Disponível em: https://dimap.ufrn.br/~cbsf/pub/anais/2012/10001203.pdf. Acesso em 28 de abril de 2023.

JUNIOR, Francisco Rodrigues Lima; et al. **Uma metodologia baseada no modelo SCOR e em inferência *fuzzy* para apoiar a avaliação de desempenho de fornecedores**. Encontro Internacional sobre Gestão Empresarial e Meio Ambiente. 2016. Disponível em: http://engemausp.submissao.com.br/17/anais/arquivos/142.pdf. Acesso em 30 de abril de 2023.

VIRTI, Émerson; TAROUCO, Liane. Um IDS utilizando SNMP e Logica Difusa. Universidade Federal do Rio Grande do Sul, Rio Grande do Sul. GTS. 2007. Slide. 34 slides. color. Disponível em: https://pop-rs.rnp.br/images/publicacoes/2007/07-IDS-SNMP-Fuzzy.pdf. Acesso em 29 de abril de 2023.

Referências

MAMDANI and Sugeno Fuzzy Inference Systems. [*S. l.*]: The MathWorks, 2023. Disponível em: https://www.mathworks.com/help/fuzzy/types-of-fuzzy-inference-systems.html. Acesso em 14 de junho de 2023.

PALOALTO. **What is Network Security?**, 2023 Disponível em: https://www.paloaltonetworks.com/cyberpedia/what-is-network-security. Acesso em 10 de junho de 2023.

SCARFONE, K., Mell, P., & Paulsen, J. (2007). **Guide to Intrusion Detection and Prevention Systems (IDPS)**.

ZIMMERMANN, H.J. **Fuzzy set theory and its applications**. 1 ed. Massachussets: Kluwer Academic, 1991.