A Fuzzy-based approach to Enhance Cyber Defence

Security for Next-generation IoT: O que é preciso falar

*Abstract*—Na era moderna, a Internet das Coisas Cognitiva (CIoT) aprimora a IoT adicionando inteligência para redes de próxima geração, mas os dispositivos IoT são vulneráveis a ataques de spam na web. Para resolver isso, o artigo propõe uma Estrutura de Spammer Cognitiva (CSF) usando classificadores fuzzy e de aprendizado de máquina, alcançando 97,3% de precisão na detecção de spam na web.

# **Introdução**

**A Internet das Coisas (IoT) oferece serviços essenciais em diversas aplicações, como transporte e medicina, no contexto das redes de próxima geração** (Nx-IoT), utilizando objetos que sensoreiam o ambiente e realizam tarefas de computação e transferência de dados. **No entanto, as arquiteturas atuais de IoT não atendem aos padrões internacionais, destacando a necessidade de avanços como a Internet das Coisas Cognitiva (CIoT) para decisões inteligentes**.

Uma das técnicas de otimização, usada principalmente para tomada de decisões com previsão, foi adotada para decisões futuras nas três camadas dos anéis cognitivos em CIoT. O aprendizado de máquina (ML), com técnicas como máquinas de vetores de suporte e redes neurais, é utilizado para raciocínio inicial em CIoT, sendo crucial para a inferência ontológica e permitindo inovações como serviços médicos inteligentes e a tecnologia de rádio cognitivo.

# **Background**

**A discussão acima ilustra o uso do aprendizado de máquina (ML) em aplicações cognitivas, destacando a necessidade atual de detectar spam na web**. **Web spam é o envio indesejado de conteúdo para websites ou resultados de busca, geralmente com fins promocionais ou maliciosos.** Motivados por essa exigência, nosso objetivo é detectar páginas maliciosas usando ML com poder cognitivo, combatendo práticas injustas que manipulam os rankings dos motores de busca para obter melhores posições nos resultados.

**As técnicas existentes para detectar páginas maliciosas geralmente focam na análise após serem indexadas pelos motores de busca.** Os métodos incluem:

1. **Algoritmo de classificação: O algoritmo PageRank** do Google é manipulado por spammers, mas atualizações podem detectar páginas maliciosas antes de aparecerem nos resultados.
2. **Comportamento do usuário: Analisar o comportamento do usuário, como tempo de permanência e número de cliques, ajuda na detecção de spam**.
3. **Qualidade da página: A qualidade da página é avaliada para determinar sua importância**, como no modelo de confiança de conteúdo.
4. **Aprendizado de máquina**: ML é crucial para validar algoritmos de detecção de spam, **treinando modelos com características combinadas de páginas para detectar spam com sucesso**.

**Motivação**

**Técnicas diferentes trabalham de forma diferente. Ao combinar diferentes técnicas de inteligência computacional, o chamado Ensemble, os resultados na detecção de spam melhoram.**

**Como até o Google usa lógica fuzzy pra detecção de spam de e-mails, nesse trabalho é proposto um novo framework para melhorar os resultados das páginas de resultados de mecanismos de busca utilizando um classificador por regras Fuzzy e um esemble Fuzzy**.

# **Modelo do Sistema**

A CIoT capacita sistemas para operarem de maneira mais inteligente através da sensação do ambiente, com o machine learning sendo uma ferramenta poderosa para previsão e extração de dados. Ao combinar modelos de machine learning com fuzzificação, pode-se melhorar a detecção de spam na web, contribuindo para resultados de busca mais precisos. Este projeto visa aprimorar a precisão dos modelos de machine learning com a ajuda de novos classificadores e técnicas de conjunto fuzzy, visando maximizar a detecção de spam e, consequentemente, aprimorar os resultados de busca.

# **O esquema proposto**

1. **A extração de características reduz a dimensão do conjunto de dados, transformando variáveis correlacionadas em variáveis não correlacionadas**, geralmente usando o método dos componentes principais (PCA).
2. **As principais features são selecionadas com base na importância calculado por modelos de árvore de decisão**. Esse resultado é conhecido como índice Gini. **Então as features com menor importância são descartadas. No estudo, 13 características com o maior índice foram escolhidas**, como hostid, Label, entre outros.
3. **A limpeza de dados é crucial para a precisão do esquema**. Um método de sobre-amostragem, SOTU, é usado devido à escassez relativa de rótulos de spam. **Os dados são distribuídos em 11 conjuntos balanceados de amostras e cada classificador é treinado com cada conjunto**.
4. **Após a extração e seleção de características, os dados são alimentados em três diferentes modelos de aprendizado de máquina, juntamente com um classificador baseado em regras fuzzy, para experimentos de classificação**. Foram utilizados 8 modelos de classificação, onde os 3 melhores em acurácia foram escolhidos para a próxima etapa.
5. **A abordagem de conjunto (Ensemble)** onde três modelos de Machine Learning (**Bagged Mars, Modelo Linear Generalizado Bayesiano, Modelo Linear Impulsionado**) e um **classificador baseado em regras fuzzy (FRBC) são combinados**. Os resultados de cada classificador são normalizados (0 = spam, 1 = não spam) e combinados usando uma equação específica, resultando em uma avaliação de desempenho.

**Resultados**

1. Dados

**O framework proposto foi validado através de experimentos realizados no conjunto de dados publicamente disponível, WEBSPAM-UK2007, composto por 114529 hosts e 41 features**. Este conjunto de dados, lançado pela Universita degli Studi di Milano, **contém informações como ID do host, pontuação do pagerank, links de entrada e saída, entre outros**. Os rótulos foram divididos em dois conjuntos, **SET1 para treinamento e SET2 para teste**, com as categorias 'spam', 'não spam', 'fronteira' e 'não classificável'.

1. Impacto dos modelos de machine learning

Os dados são pré-processados utilizando técnicas de extração e seleção de características, resultando em dados limpos e livres de ruídos. Quatro diferentes classificadores são treinados: Bagged MARS, Modelo Linear Generalizado Bayesiano, e Modelo Linear Impulsionado. **O Bagged MARS captura a não linearidade da regressão polinomial, o Modelo Linear Generalizado Bayesiano manipula a aleatoriedade de variáveis incompletas e o Modelo Linear Impulsionado utiliza a técnica 'BstLm'. Os resultados são avaliados por meio de curvas ROC**.

**O classificador baseado em regras fuzzy é implementado utilizando regras IF-THEN com rótulos de classe fixados em dois.** **Um modelo 'MAMDANI' FRBS é construído com a função de camada única**. **A técnica de desfusificação usada para avaliação das regras é o método de média ponderada**. **O modelo**, chamado 'sim-0', **trata 13 características como uma combinação de três variáveis, sendo var.1 e var.2 as variáveis de entrada e var.3 a variável de saída**. Os intervalos para as variáveis de treinamento são fixados em -2.716 a 2.834 para Var1, e 45.6 a 60.5 para Var2. **As regras tem a seguinte forma:**

1. Comparação com modelos de aprendizado de máquina

**Uma síntese comparativa dos modelos de aprendizado de máquina é apresentada** na Tabela V, com base em diversos parâmetros. **Cada modelo é treinado com 11 conjuntos de dados resultantes da abordagem de limpeza de dados**. Assim, a Tabela VI compara o tempo de execução e a precisão dos diferentes classificadores com diferentes conjuntos de amostras.

1. **Limitações**

**O esquema proposto enfrenta dificuldades na detecção e prevenção de imagens spam**. **O framework propost não funciona bem em ambientes no qual o armazenamento o é local.** A complexidade da manipulação de imagens no esquema proposto torna-se um obstáculo nesse ambiente, com **aumento do tempo computacional e de busca conforme o número de dispositivos aumenta**, conforme ilustrado na Figura 9.

1. **Comparação com modelos anteriores**

**O esquema proposto foi comparado com várias técnicas de referência existentes para detecção de spam na web, usando a acurácia como parâmetro de avaliação. Conclui-se que o esquema proposto superou as técnicas existentes**. A análise dos diferentes algoritmos é apresentada na Figura 10. Os experimentos foram conduzidos em três conjuntos de dados separados: WEBSPAM-UK 2006, WEBSPAM-UK 2007 e Microsoft Learning to Rank (MLR). **Observou-se que a eficiência do esquema proposto depende do tamanho do experimento, mas também aumenta o custo ao equilibrar as classes com o aumento do tamanho dos dados**. Podemos inferir que, para utilizar o método proposto, é necessário considerar a escala da análise de dados.