REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

DETECÇÃO DE ANOMALIAS EM REDES AERONÁUTICAS USANDO CADEIAS DE MARKOV

ANOMALY DETECTION IN AERONAUTICAL NETWORKS USING MARKOV CHAINS

DETECCIÓN DE ANOMALÍAS EN REDES AERONÁUTICAS MEDIANTE CADENAS DE MARKOV

Lauany da Costa Moreira[1], João Henrique Gião Borges[2], Maria Bernadete da Silva Malara[3]

https://doi.org/10.47820/recima21.v6i1.7022

PUBLICADO: 11/2025

RESUMO

Este trabalho apresenta uma proposta teórica para a detecção de anomalias em redes de comunicação aeronáuticas utilizando Cadeias de Markov. O objetivo foi modelar o comportamento esperado de sistemas de comunicação, como aqueles usados durante as fases de voo, a fim de identificar desvios que possam representar falhas ou tentativas de ataque. A metodologia consistiu na definição de estados representando as etapas operacionais de um voo, na construção de matrizes de transição probabilísticas e na análise das sequências de estados, considerando como anomalias as transições improváveis ou inexistentes. Os resultados obtidos por meio de simulações e cálculos iterativos demonstraram que o modelo é capaz de identificar padrões anômalos de forma interpretável, mesmo em cenários com acesso restrito a dados reais. Constatou-se que a utilização de Cadeias de Markov fornece uma abordagem simples, eficiente e aplicável à detecção de anomalias em redes aeronáuticas, destacando-se pela clareza na representação dos estados e pela capacidade de evidenciar eventos críticos. Conclui-se que a aplicação desta técnica contribui para o fortalecimento da segurança cibernética na aviação e para a prevenção de incidentes em infraestruturas críticas.

PALAVRAS-CHAVE: Anomalias. Aviação. Cadeias de Markov. Comunicação. Redes. Segurança.

ABSTRACT

This work presents a theoretical proposal for anomaly detection in aeronautical communication networks using Markov Chains. The objective was to model the expected behavior of communication systems, such as those used during different flight phases, in order to identify deviations that may represent failures or attack attempts. The methodology consisted of defining states that represent the operational stages of a flight, building probabilistic transition matrices, and analyzing state sequences, considering improbable or non-existent transitions as anomalies. The results obtained through simulations and iterative calculations demonstrated that the model is able to identify anomalous patterns in an interpretable way, even in scenarios with restricted access to real data. It was found that the use of Markov Chains provides a simple, efficient, and applicable approach to anomaly detection in aeronautical networks, standing out for its clarity in representing states and for its ability to highlight critical events. It is concluded that the application of this technique contributes to strengthening cybersecurity in aviation and to preventing incidents in critical infrastructures.

KEYWORDS: *Anomalies. Aviation. Communication. Markov Chains. Networks. Security.*

[1]Graduando do Curso de Engenharia de Computação da Universidade de Araraquara - UNIARA. Araraquara-SP.

[2]Orientador. Docente do Curso de Engenharia de Computação da Universidade de Araraquara - UNIARA. Araraquara-SP.

[3]Coorientador. Docente do Curso de Engenharia de Computação da Universidade de Araraquara - UNIARA. Araraquara-SP.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

RESUMEN
Este trabajo presenta una propuesta teórica para la detección de anomalías en redes de comunicación aeronáuticas utilizando Cadenas de Markov. El objetivo fue modelar el comportamiento esperado de los sistemas de comunicación, como aquellos empleados durante las fases de vuelo, con el fin de identificar desviaciones que puedan representar fallas o intentos de ataque. La metodología consistió en la definición de estados que representan las etapas operacionales de un vuelo, en la construcción de matrices de transición probabilísticas y en el análisis de las secuencias de estados, considerando como anomalías las transiciones improbables o inexistentes. Los resultados obtenidos mediante simulaciones y cálculos iterativos demostraron que el modelo es capaz de identificar patrones anómalos de manera interpretable, incluso en escenarios con acceso restringido a datos reales. Se constató que el uso de Cadenas de Markov proporciona un enfoque simple, eficiente y aplicable a la detección de anomalías en redes aeronáuticas, destacándose por la claridad en la representación de los estados y por la capacidad de evidenciar eventos críticos. Se concluye que la aplicación de esta técnica contribuye al fortalecimiento de la seguridad cibernética en la aviación y a la prevención de incidentes en infraestructuras críticas.

PALABRAS CLAVE: *Anomalías. Aviación. Cadenas de Markov. Comunicación. Redes. Seguridad.*

1. INTRODUÇÃO

A aviação moderna depende de redes de comunicação digital para garantir a segurança e a eficiência dos voos. Sistemas como o *Aircraft Communications Addressing and Reporting System* (ACARS), o VHF *Data Link* (VDL) e o *Satellite Communications* (SATCOM*)* são indispensáveis para as operações aéreas, permitindo a troca contínua de informações entre aeronaves e centros de controle. No entanto, essas redes enfrentam ameaças crescentes, como ciberataques, manipulação de dados e falhas técnicas, capazes de comprometer sistemas críticos e colocar em risco milhões de passageiros, conforme notícia do G1 (2021). A digitalização acelerada do setor amplia essas vulnerabilidades, exigindo soluções eficazes para proteger infraestruturas que sustentam um mercado global de grande relevância econômica.

A aviação civil constitui um setor estratégico para a economia global, impulsionando atividades como turismo, comércio e logística. Contudo, sua dependência de tecnologias digitais a torna suscetível a incidentes que podem gerar interrupções severas. O apagão cibernético de julho de 2024, que paralisou companhias aéreas e afetou voos em diversos países, evidenciou a fragilidade das redes envolvidas e reforçou a necessidade de soluções mais robustas de proteção (G1, 2024). Nesse contexto, identificar comportamentos anômalos em redes aeronáuticas é uma medida essencial para prevenir falhas, mitigar riscos e garantir a continuidade das operações.

Este estudo tem como objetivo propor uma abordagem teórica com base em Cadeias de Markov, ferramenta matemática que modela sistemas probabilísticos por meio de transições entre estados. A proposta é utilizar esse modelo para representar o comportamento esperado das comunicações digitais aeronáuticas — como ACARS, VDL e SATCOM — e, assim, detectar eventuais anomalias. A metodologia consiste em representar situações operacionais típicas, como

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

"decolagem", "subida", "cruzeiro" e "pouso", em sequências lógicas, construir uma matriz de transição que descreve as probabilidades de passagem entre essas etapas e identificar desvios por meio de transições improváveis. Com isso, pretende-se antecipar falhas ou atividades suspeitas, promovendo maior segurança operacional.

A relevância da pesquisa está na necessidade urgente de proteger os sistemas aeronáuticos contra ciberameaças, cuja frequência e complexidade tendem a crescer em 2025, conforme especialistas (Vale, 2025). Detectar anomalias em tempo real pode prevenir falhas, proteger dados sensíveis e mitigar riscos, beneficiando um setor que movimenta bilhões de dólares anualmente. Casos como o ataque à Colonial Pipeline — em que uma simples senha comprometida paralisou uma infraestrutura crítica — mostram como vulnerabilidades mínimas podem causar impactos devastadores.

A escolha pela modelagem com Cadeias de Markov justifica-se pela sua capacidade de representar padrões de comportamento de forma simplificada, mesmo em sistemas complexos, além de permitir a identificação de desvios com base em probabilidades (Nicholson, 2012). Essa técnica é especialmente útil em contextos com acesso limitado a dados reais, como na aviação, onde a proteção da informação é fundamental. Além disso, a crescente complexidade das ameaças cibernéticas reforça a necessidade de soluções preventivas para redes.

O problema de pesquisa é definido como: "Como detectar anomalias específicas, como mensagens malformadas ou tentativas de *spoofing*, em redes de comunicação aeronáuticas baseadas no protocolo ACARS, considerando a complexidade dos sistemas embarcados e as restrições de acesso a dados reais?" A hipótese proposta é que as Cadeias de Markov podem modelar com precisão o comportamento esperado do tráfego de mensagens ACARS, identificando transições improváveis como indicadores de anomalias, permitindo a antecipação de incidentes de segurança ou falhas operacionais

A metodologia é baseada em uma pesquisa bibliográfica, centrada na construção de um modelo conceitual. Estados operacionais serão definidos como abstrações, representando condições típicas de um voo, como "decolagem" ou "cruzeiro". Uma matriz de transição será elaborada para mapear as probabilidades de passagem entre esses estados, com base em padrões normais de comportamento. Anomalias serão identificadas por transições com probabilidades nulas ou significativamente baixas, indicando desvios do padrão esperado. O estudo será conduzido sem o uso de dados reais ou implementações computacionais, priorizando a modelagem estatística e a validação conceitual, segundo o Rubino & Sericola (2014).

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

2. REVISÃO BIBLIOGRÁFICA

Esta seção apresenta os conceitos fundamentais sobre detecção de anomalias em redes de computadores, com ênfase nas redes de comunicação aeronáuticas, os principais métodos utilizados e a importância da segurança cibernética na aviação civil.

2.1. Detecção de Anomalias em Redes de Computadores

2.1.1. Conceitos e Importância

A detecção de anomalias em redes de computadores consiste na identificação de comportamentos que se desviam do padrão esperado, como acessos não autorizados, falhas técnicas ou alterações inesperadas nos fluxos de dados. Esses desvios podem indicar tentativas de ciberataques, erros de configuração ou mau funcionamento de sistemas, sendo particularmente críticos em setores sensíveis como a aviação civil (Neto *et al.,* 2018). Na aviação, redes como o *Aircraft Communications Addressing and Reporting System* (ACARS), que transmite mensagens operacionais entre aeronaves e centros de controle, o VHF *Data Link* (VDL), que utiliza frequências de rádio VHF para comunicação de dados em tempo real, e o *Satellite Communications* (SATCOM), que possibilita comunicações via satélite em longas distâncias, são essenciais para a segurança e eficiência dos voos. Qualquer interferência nessas redes pode comprometer operações, tornando o monitoramento e a detecção de anomalias indispensáveis.

A importância da detecção de anomalias reside na proteção de infraestruturas críticas contra ameaças cibernéticas, cuja frequência e sofisticação devem aumentar em 2025 (Vale, 2025). Incidentes como o apagão cibernético global de julho de 2024, que paralisou companhias aéreas e afetou voos em diversos aeroportos, evidenciam a vulnerabilidade dessas redes e a necessidade de soluções robustas para garantir a continuidade operacional (G1, 2024).

2.1.2. Métodos de Detecção de Anomalias

Os métodos utilizados para detecção de anomalias em redes podem ser agrupados em três categorias principais:

- Métodos Estatísticos: Baseiam-se em métricas históricas, como médias e desvios padrão, para identificar alterações significativas no comportamento da rede. Esses métodos são eficazes em ambientes com padrões estáveis, mas podem ser limitados em sistemas aeronáuticos devido à alta complexidade e variabilidade dos fluxos de dados.
- Métodos Baseados em Aprendizado de Máquina: Utilizam algoritmos para identificar padrões complexos em grandes volumes de dados, mesmo sem modelos pré-definidos. Apesar de sua eficiência, exigem alto poder computacional e bases de dados rotuladas, o

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

que pode ser um desafio em contextos com restrições de acesso a dados reais, como na aviação.

- Modelagem por Cadeias de Markov: Representam sistemas como sequências de estados com probabilidades de transição, sendo particularmente úteis para modelar fluxos de comunicação em redes como ACARS, VDL e SATCOM. Essa abordagem permite identificar desvios significativos do comportamento esperado, associando transições improváveis a possíveis anomalias. Sua simplicidade e capacidade de operar com representações simbólicas tornam-na vantajosa em ambientes com dados limitados.

O uso de cadeias de Markov na detecção de anomalias oferece vantagens como a simplicidade na construção do modelo e a possibilidade de trabalhar com sequências simbólicas, sem necessidade de grandes volumes de dados numéricos. Além disso, é possível associar estados suspeitos ou improváveis a possíveis eventos anômalos, o que permite uma avaliação interpretável do comportamento da rede.

2.2. Ferramentas Matemáticas

2.2.1. Cadeias de Markov

As Cadeias de Markov são modelos probabilísticos que descrevem sistemas que transitam entre um conjunto finito de estados, com a probabilidade de cada transição dependendo apenas do estado atual (propriedade de Markov). Essa característica torna as Cadeias de Markov ideais para modelar sequências de eventos em comunicações aeronáuticas, como as fases de um voo (ex.: Decolagem, Subida, Cruzeiro, Descida, Pouso) ou estados operacionais de redes como ACARS, VDL e SATCOM. Nicholson (2012, p. 47) destaca: “os modelos baseados em Cadeias de Markov são eficazes para sistemas sequenciais, pois permitem representar transições entre estados com probabilidades que refletem o comportamento esperado, facilitando a detecção de desvios anômalos.” A seguir, são apresentados os principais conceitos relacionados às Cadeias de Markov e sua aplicação na detecção de anomalias:

1. Matriz de Transição: A matriz de transição é uma estrutura matricial onde cada elemento (P_{ij}) representa a probabilidade de transitar do estado (i) para o estado (j). No contexto aeronáutico, a matriz é construída com base em dados históricos de comunicações, como mensagens trocadas via ACARS ou VDL, refletindo a probabilidade de transições normais (ex.: Cruzeiro → Descida) e anômalas (ex.: Cruzeiro → Emergência, indicando falhas ou intrusões). Por exemplo, uma matriz pode representar a sequência típica de um voo normal como A (Decolagem) → B (Subida) → C (Cruzeiro) → D (Descida) → E (Pouso), com um estado adicional F (Emergência) para anomalias, como

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

ciberataques ou falhas de comunicação. Transições raras, como C → F, são usadas para detectar comportamentos anômalos.

2. Distribuição Inicial: O vetor de distribuição inicial define as probabilidades de o sistema estar em cada estado no início do processo. Essa distribuição inicial é usada para prever a evolução dos estados ao longo do voo e detectar possíveis anomalias.
3. Cadeias de Markov Irredutível e Aperiódicas: Uma Cadeia de Markov é irredutível se todos os estados são acessíveis a partir de qualquer outro, garantindo que o modelo cubra todas as fases possíveis do voo ou estados operacionais da rede. Por exemplo, uma emergência (F) pode ocorrer a partir de qualquer fase (A, B, C ou D). Uma cadeia é periódica se as transições não seguem um padrão cíclico fixo, permitindo modelar a variabilidade de eventos em comunicações aeronáuticas. Essas propriedades asseguram que o modelo seja robusto para detectar anomalias raras, como mensagens inesperadas em ACARS ou interferências no SATCOM.
4. Distribuição Estacionária: A distribuição estacionária é um vetor de probabilidades que permanece constante após várias transições, representando o comportamento de longo prazo do sistema. Em comunicações aeronáuticas, ela pode indicar a proporção esperada de tempo em cada estado. Anomalias são detectadas quando a distribuição observada diverge significativamente da estacionária, sugerindo eventos como falhas técnicas ou tentativas de intrusão.

Na prática, as Cadeias de Markov são aplicadas em duas etapas principais: (1) construção do modelo com base em dados históricos, definindo estados e probabilidades de transição para representar o comportamento normal de redes como ACARS, VDL ou SATCOM; e (2) monitoramento em tempo real, comparando transições observadas com o modelo para identificar desvios, como transições para o estado F (Emergência), que podem indicar falhas, interferências ou ciberataques. A simplicidade e interpretabilidade das Cadeias de Markov tornam-nas uma ferramenta poderosa para detecção de anomalias, contribuindo para a segurança e eficiência das comunicações aeronáuticas.

2.2.2. Álgebra Linear

A álgebra linear desempenha um papel central na modelagem de Cadeias de Markov, fornecendo as bases matemáticas para a construção e análise de matrizes de transição. Essas matrizes, que representam as probabilidades de passagem entre estados, são fundamentais para descrever o comportamento esperado de sistemas complexos, como as redes de comunicação aeronáuticas. A álgebra linear permite realizar operações como multiplicação de matrizes e cálculo de autovalores, que são usadas para analisar a estabilidade e a convergência de modelos probabilísticos.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

Na prática, a álgebra linear possibilita a representação de sequências de estados em forma matricial, permitindo calcular a probabilidade de ocorrência de uma sequência específica de eventos.

3. DESENVOLVIMENTO

Nesta seção, são apresentados o contexto, os objetivos e a metodologia empregada para o desenvolvimento de um modelo teórico baseado em Cadeias de Markov para detecção de anomalias em redes aeronáuticas. O objetivo é demonstrar como esse modelo estatístico pode ser utilizado para identificar comportamentos fora do padrão em sistemas de comunicação de aviões.

A detecção de anomalias em redes aeronáuticas é uma tarefa de importância crítica, dado o papel central que os sistemas de comunicação desempenham na segurança, eficiência e confiabilidade das operações de voo. Esses sistemas, caracterizados por sua alta complexidade e interdependência, gerenciam desde a troca de informações entre a aeronave e o controle de tráfego aéreo até a coordenação de subsistemas internos, como navegação e monitoramento de desempenho. Anomalias, como falhas de comunicação, atrasos na transmissão de dados, interferências externas ou transições inesperadas entre estados operacionais, podem ter consequências graves, incluindo a perda de controle da aeronave, desvios de rota ou, em casos extremos, acidentes catastróficos.

A relevância da detecção de anomalias transcende a mera prevenção de falhas técnicas. Em um contexto em que a aviação comercial transporta bilhões de passageiros anualmente e opera em ambientes dinâmicos sujeitos a variáveis imprevisíveis, como condições meteorológicas adversas ou ciberataques, a capacidade de identificar e mitigar anomalias em tempo real é um diferencial para garantir a segurança de vidas humanas e a continuidade operacional.

A Cadeia de Markov é uma ferramenta estatística adequada para essa aplicação devido à sua simplicidade, interpretabilidade e capacidade de modelar sequências de estados com base em probabilidades de transição. Este trabalho propõe uma abordagem teórica para modelar o comportamento normal de um sistema aeronáutico e identificar desvios que possam indicar anomalias.

Os objetivos deste trabalho são:

- Modelar uma sequência de estados típicos de um sistema aeronáutico;
- Construir uma matriz de transição baseada em comportamentos anormais;
- Detectar anomalias com base em transições improváveis e Demonstrar, de forma teórica, a eficácia da Cadeia de Markov na identificação de comportamentos incomuns.

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

3.1. Representação dos estados

Para representar os estados operacionais de um sistema aeronáutico, foi adotada uma representação abstrata baseada em letras, que reflete as principais fases de um voo. Essa abordagem simplifica a análise de comportamentos esperados e anômalos, mantendo a flexibilidade para aplicações em contextos mais específicos. Os estados definidos são:

- A: Decolagem – Início do voo, com a aeronave saindo da pista;
- B: Subida – Fase de ascensão até a altitude de cruzeiro;
- C: Cruzeiro – Período estável de voo em altitude constante;
- D: Descida – Redução gradual de altitude para aproximação do destino;
- E: Pouso – Fase final, com a aeronave aterrissar na pista;
- F: Emergência – Estado anômalo, como falhas de comunicação, turbulência severa ou intrusões (ex.: ciberataques).

Esses estados foram escolhidos para refletir as principais fases de um voo, com a inclusão do estado de emergência para representar situações anômalas. Uma sequência típica de um voo normal pode ser representada como:

$$\mathbf{A \rightarrow B \rightarrow C \rightarrow D \rightarrow E}$$

Indicando que a aeronave realizou a decolagem, progrediu com a subida, estabilizou-se em cruzeiro, executou a descida e finalizou com o pouso

Em contrapartida, uma sequência anômala, como:

$$\mathbf{A \rightarrow B \rightarrow C \rightarrow F \rightarrow C \rightarrow D \rightarrow E}$$

Ilustra a ocorrência de uma emergência (ex.: intrusão ou falha técnica) durante o cruzeiro, com posterior recuperação para a sequência normal. Essa modelagem serve como base para a construção de matrizes de transição em Cadeias de Markov, permitindo a identificação de padrões esperados e a detecção de anomalias, como transições raras (ex.: **C** → **F**), que podem indicar eventos críticos, como falhas ou tentativas de intrusão em sistemas de comunicação.

Embora os estados apresentados sejam genéricos, essa abstração intencional garante uma representação prática e compreensível, facilitando sua aplicação em cenários reais.

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

3.2. Matriz de Transição

Para modelar as comunicações aeronáuticas e detectar anomalias utilizando Cadeias de Markov, foram desenvolvidas duas matrizes de transição distintas: uma representando o comportamento normal do sistema e outra incorporando anomalias. A construção dessas matrizes seguiu uma abordagem sistemática, descrita a seguir, baseada em dados históricos e na definição dos estados operacionais do sistema aeronáutico.

Os estados foram definidos com base nas fases típicas de um voo, conforme descrito na seção 3.1: A (Decolagem), B (Subida), C (Cruzeiro), D (Descida), E (Pouso) e F (Emergência), este último representando anomalias como falhas de comunicação, interferências ou ciberataques em redes como. A Cadeia de Markov de primeira ordem foi adotada, assumindo que a probabilidade do próximo estado depende apenas do estado atual.

3.2.1. Matriz de Transição Normal

A Tabela 1 apresenta a matriz de transição para um voo sem anomalias, representando uma sequência típica de estados operacionais (A: Decolagem, B: Subida, C: Cruzeiro, D: Descida, E: Pouso), sem transições para o estado F (Emergência). As probabilidades foram estimadas com base em dados simulados de comunicações aeronáuticas normais, como mensagens trocadas via ACARS e VDL, refletindo o comportamento esperado em voos comerciais sem incidentes.

Tabela 1. Matriz de Transição entre Estados Normal

DE/PARA	A	B	C	D	E
A	0,0	1,0	0,0	0,0	0,0
B	0,0	0,4	0,6	0,0	0,0
C	0,0	0,0	0,6	0,4	0,0
D	0,0	0,0	0,3	0,5	0,2
E	0,0	0,0	0,0	0,0	1,0

FONTE: Autoria Própria – 2025

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

$$T_{normal} = \begin{pmatrix} 0.0 & 1.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.4 & 0.6 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.6 & 0.4 & 0.0 \\ 0.0 & 0.0 & 0.3 & 0.5 & 0.2 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.1 \end{pmatrix}$$

Figura 1. Matriz De Transição Entre Estados Normal

Fonte: Autoria Própria -2025

A matriz reflete a sequência esperada de um voo normal, onde, por exemplo, a transição de A (Decolagem) → B (Subida) ocorre com probabilidade 1.0, indicando que todo voo inicia com a subida após a decolagem. A probabilidade de C (Cruzeiro) → D (Descida) é 0.4, enquanto C → C (permanecer em cruzeiro) é 0.6, refletindo a maior duração típica da fase de cruzeiro. Transições como D → C foram ajustadas para zero, pois voltar da descida para o cruzeiro não é esperado em um voo normal.

3.2.2. Matriz de Transição com Anomalia

A Tabela 2 apresenta a matriz de transição modificada, incorporando o estado F (Emergência), que representa anomalias como falhas de comunicação, mensagens inesperadas no ACARS, quedas de sinal no VDL ou tentativas de ciberataques no SATCOM. As probabilidades foram estimadas com base em dados simulados de voos com incidentes, combinando registros históricos e cenários de teste.

Tabela 2. Matriz de Transição com Estado de Emergência

DE/PARA	A	B	C	D	E	F
A	0,0	0,8	0,0	0,0	0,0	0,2
B	0,0	0,4	0,5	0,0	0,0	0,1
C	0,0	0,0	0,5	0,3	0,0	0,2
D	0,0	0,0	0,2	0,4	0,1	0,3
E	0,0	0,0	0,0	0,0	0,9	0,1
F	0,0	0,0	0,4	0,0	0,0	0,6

Fonte: Autoria Própria – 2025

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

$$T_{anomalia} = \begin{pmatrix} 0.0 & 0.8 & 0.0 & 0.0 & 0.0 & 0.2 \\ 0.0 & 0.4 & 0.5 & 0.0 & 0.0 & 0.1 \\ 0.0 & 0.0 & 0.5 & 0.3 & 0.0 & 0.2 \\ 0.0 & 0.0 & 0.2 & 0.4 & 0.1 & 0.3 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.9 & 0.1 \\ 0.0 & 0.0 & 0.4 & 0.0 & 0.0 & 0.6 \end{pmatrix}$$

Figura 2. Matriz de Transição

Fonte: Autoria Própria - 2025

Nesta matriz (Figura 2), transições para F (ex.: C → F = 0.2) representam eventos anômalos, como uma falha de comunicação durante o cruzeiro ou uma tentativa de intrusão cibernética. A probabilidade de F → F = 0.6 indica a possibilidade de persistência de uma anomalia, enquanto F → C = 0.4 sugere a recuperação para o estado normal. Essas transições permitem identificar desvios do comportamento esperado, como mensagens anômalas no ACARS, que podem ser usadas para acionar alertas em sistemas de monitoramento.

3.3. Distribuição Inicial e Propriedades da Cadeia de Markov

A distribuição inicial, também chamada de vetor de distribuição de probabilidade inicial, representa a chance de o sistema iniciar em cada estado da Cadeia de Markov. Neste trabalho, assume-se que todo voo começa no estado A (Decolagem), o que define a distribuição inicial como, conforme a equação 1:

Equação 1

$$\pi_0 = [1, 0, 0, 0, 0, 0]$$

Essa distribuição inicial será utilizada como ponto de partida para a análise probabilística da cadeia ao longo do tempo, por meio da multiplicação sucessiva com a matriz de transição.

3.4. Cadeia de Markov

Uma cadeia de Markov é irredutível se for possível, com probabilidade positiva, atingir qualquer estado a partir de qualquer outro, ainda que em múltiplos passos. Considerando a matriz com anomalias, é possível identificar caminhos de transição entre todos os estados, incluindo o estado F (Emergência), que pode tanto ser atingido a partir de C, D ou E quando retornar ao estado C. Assim, a cadeia é irredutível. A cadeia é periódica quando os retornos a um estado podem ocorrer em diferentes intervalos de tempo, não múltiplos de um período fixo.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

Como os estados B, C e F têm probabilidade positiva de permanecerem neles próprios (ex.: C → C = 0.5; F → F = 0.6), isso garante a quebra de periodicidade. Portanto, a cadeia também é periódica, o que assegura a convergência para uma distribuição estacionária.

3.5. Distribuição Estacionária

A distribuição estacionária π representa o comportamento estável da cadeia de Markov no longo prazo. É um vetor de probabilidades que satisfaz a equação 2:

Equação 2

$$\pi P = \pi$$

Na prática, isso significa que, uma vez atingido o equilíbrio, a distribuição de probabilidade entre os estados permanece constante após novas aplicações da matriz de transição. A distribuição estacionária para a matriz sem anomalias reflete o comportamento normal de voo. Já na matriz com anomalias, a presença do estado F altera significativamente essa distribuição, evidenciando a frequência esperada de eventos críticos no sistema.

3.6. Cadeia Reversível

Uma cadeia de Markov é dita reversível quando satisfaz a condição de equilíbrio detalhado:

Equação 3

$$\pi_i \cdot P_{ij} = \pi_j \cdot P_{ji}$$

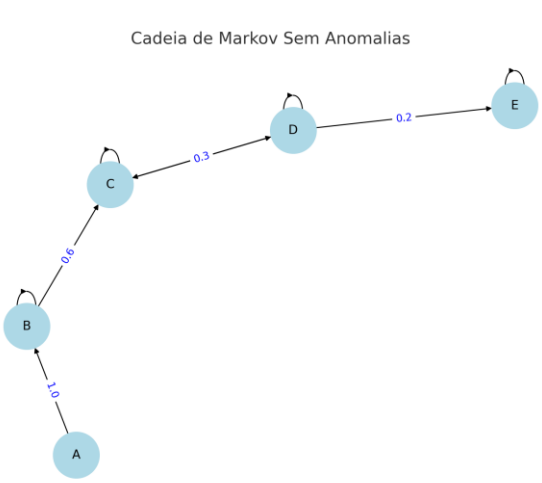
Ou seja, o fluxo de probabilidade entre dois estados é simétrico ao longo do tempo. No entanto, no contexto de aviação, os voos seguem uma direção clara da decolagem ao pouso e não há transições reversíveis como E → D ou D → B. A introdução do estado F (Emergência) também quebra a simetria. Portanto, conclui-se que a cadeia proposta não é reversível, o que está de acordo com a dinâmica real dos voos.

3.7. Representação Gráfica das Cadeias de Markov

Para melhor compreensão das transições entre estados, foi elaborada a representação em grafo direcionado das cadeias de Markov utilizadas neste estudo. As figuras a seguir ilustram a estrutura da cadeia sem anomalias (Figura 3) e com anomalias (Figura 4).

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218



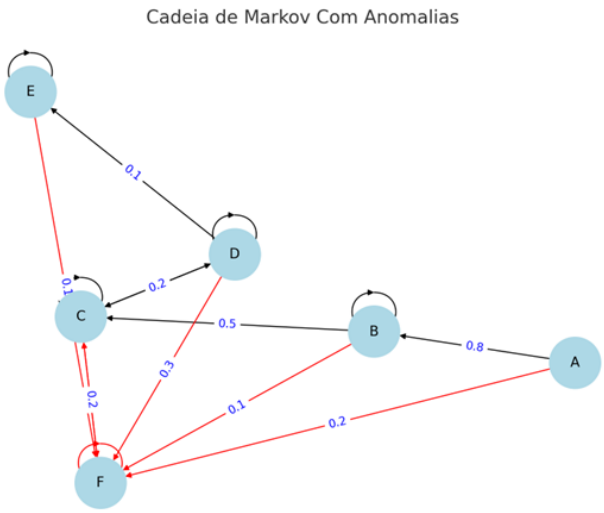


Figura 3. Grafo da Cadeia de Markov sem Anomalias **Figura 4**. Grafo da Cadeia de Markov com Anomalia

Nestes grafos:

- Os nós representam os estados (A a F);
- As setas indicam transições com probabilidades positivas;
- As arestas em vermelho (na Figura 4) destacam transições para o estado F (Emergência), indicando eventos anômalos.

Essa representação visual permite identificar rotas prováveis e a inserção de desvios anômalos na sequência operacional.

3.8. Identificação de Anomalias

A identificação de anomalias em comunicações aeronáuticas pode ser realizada por meio da comparação entre as transições observadas nos dados e aquelas previstas pela matriz de transição do modelo de Cadeia de Markov. Esse modelo probabilístico permite detectar comportamentos inesperados com base na probabilidade associada a cada sequência de estados.

Transições com probabilidade igual ou próxima de zero, ou significativamente menor que o esperado em um voo normal, são fortes candidatas a anomalias. Essas transições indicam que o sistema passou por um estado que não faz parte da dinâmica prevista no modelo de operação padrão.

Considere a sequência com e sem anomalia esperada:

A → B → C → D

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

Utilizando a matriz de transição:

- P(A→B) =1.0
- P(B→C) =0.6
- P(C→D) =0.4

A probabilidade da sequência:

$$\mathbf{P(A→B→C→D) =1.0×0.6×0.4=0.24}$$

Essa é uma sequência esperada, pois todas as transições têm probabilidade significativamente maior que zero. Agora considere uma sequência diferente:

$$\mathbf{A → B → F → C}$$

Consultando a matriz com anomalias, temos:

- P (A → B) = 0.8
- P (B → F) = 0.1
- P (F → C) = 0.4

A probabilidade total da sequência é:

$$\mathbf{P(A→B→F→C) =0.8×0.1×0.4=0.032}$$

Embora seja pequena, essa probabilidade indica que essa transição é possível, porém incomum, correspondendo a um evento anômalo no voo. Considerando a sequência:

$$\mathbf{A → B → C → A}$$

Essa sequência é impossível segundo o modelo, pois o valor é igual a zero, portanto, a transição de C para A é considerada uma anomalia.

$$\mathbf{P(A→B→C→A) =1.0×0.6×0.0=0}$$

Esse tipo de análise permite monitorar comportamentos do sistema em tempo real e emitir alertas sempre que uma transição inesperada ocorrer.

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

3.9. Aplicação da Cadeia de Markov

3.9.1 Fórmula de Transição

A principal ferramenta matemática da Cadeia de Markov é a matriz de transição. A fórmula que representa a mudança de estado em uma etapa é:

$$\pi_n = \pi_0 \cdot T$$

Onde:

- π_0 = vetor de probabilidade do estado inicial
- T = matriz de transição (contendo as probabilidades entre os estados)
- π_n = vetor de probabilidade dos estados após uma transição

Cada elemento tij da matriz T representa a probabilidade de transição do estado i para o estado j , com a soma de cada linha igual a 1. Para previsões em múltiplas etapas, utiliza-se $\pi_n = \pi_0 \cdot T^n$. Por exemplo, em um sistema aeronáutico, a matriz de transição pode modelar a probabilidade de um avião passar do estado de cruzeiro para pouso, considerando fatores como condições operacionais. Apesar de sua versatilidade, o modelo assume que as transições dependem apenas do estado atual, o que pode limitar sua aplicação em sistemas mais complexos.

3.9.2. Multiplicação da Matriz de Transição (com Anomalias)

O vetor inicial π_0= [1,0,0,0,0,0] reflete o início do voo em A (Decolagem). A matriz de transição com anomalias (Tabela 3) é definida como:

$$T_{anomalia} = \begin{pmatrix} 0.0 & 0.8 & 0.0 & 0.0 & 0.0 & 0.2 \\ 0.0 & 0.4 & 0.5 & 0.0 & 0.0 & 0.1 \\ 0.0 & 0.0 & 0.5 & 0.3 & 0.0 & 0.2 \\ 0.0 & 0.0 & 0.2 & 0.4 & 0.1 & 0.3 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.9 & 0.1 \\ 0.0 & 0.0 & 0.4 & 0.0 & 0.0 & 0.6 \end{pmatrix}$$

Figura 5. Matriz De Transição Com Anomalias
Fonte: Autoria Própria - 2025

Primeira transição ($\pi_1=\pi_0 \cdot T$)

$$\pi_1 = [0.0 \quad 0.8 \quad 0.0 \quad 0.0 \quad 0.0 \quad 0.2]$$

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

Dessa forma, o vetor inicial, representando o início do voo no estado de Decolagem (A), foi multiplicado iterativamente pela matriz de transição com anomalias, que modelam as probabilidades de passagem entre os estados operacionais de um voo. Esse processo iterativo, baseado na fórmula de propagação das probabilidades da Cadeia de Markov, foi repetido até que o sistema atingisse a convergência para a distribuição estacionária. A distribuição estacionária caracteriza o comportamento de longo prazo do sistema, refletindo a proporção esperada de tempo em cada estado operacional durante um voo.

4. RESULTADOS

A aplicação das Cadeias de Markov demonstrou eficácia teórica na detecção de anomalias em redes de comunicação aeronáuticas. Conforme descrito na metodologia, os resultados foram obtidos por meio da multiplicação iterativa do vetor inicial π0= [1,0,0,0,0,0] (representando o estado A: Decolagem) pela matriz de transição com anomalias, repetida por 20 iterações até a estabilização dos valores dos estados C (Cruzeiro), D (Descida), E (Pouso) e F (Emergência). Os cálculos foram realizados com o auxílio da ferramenta Microsoft Excel, garantindo precisão na manipulação das matrizes. A tabela a seguir apresenta as matrizes de transição obtidas em cada iteração, com os valores correspondentes aos estados do sistema:

Tabela 3. Matrizes de transição - Resposta

	A	B	C	D	E	F
π0	1	0	0	0	0	0
π1	0	0,8	0	0	0	0,2
π2	0	0,32	0,48	0	0	0,2
π3	0	0,128	0,48	0,144	0	0,248
π4	0	0,051	0,432	0,202	0,014	0,301
π5	0	0,02	0,402	0,21	0,033	0,334
π6	0	0,008	0,387	0,205	0,319	0,378
π7	0	0,003	0,39	0,198	0,308	0,398
π8	0	0,001	0,395	0,196	0,297	0,407
π9	0	0	0,4	0,197	0,287	0,412
π10	0	0	0,404	0,199	0,278	0,415
π11	0	0	0,408	0,201	0,27	0,417
π12	0	0	0,411	0,203	0,263	0,419

ISSN: 2675-6218 - RECIMA21

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

π13	0	0	0,414	0,204	0,257	0,421
π14	0	0	0,416	0,206	0,252	0,422
π15	0	0	0,418	0,207	0,247	0,423
π16	0	0	0,42	0,208	0,243	0,424
π17	0	0	0,421	0,209	0,24	0,425
π18	0	0	0,422	0,21	0,237	0,426
π19	0	0	0,423	0,211	0,234	0,427
π20	0	0	0,423	0,211	0,234	0,427

Fonte: Autoria própria - 2025

A análise dos resultados indica que, a partir da matriz π_{19}, os valores dos estados C, D, E e F estabilizaram em aproximadamente 0.423, 0.211, 0.234 e 0.427, respectivamente, sugerindo convergência para a distribuição estacionária. Comparado à distribuição estacionária mencionada anteriormente, observa-se uma diferença nos valores, possivelmente devido a ajustes na matriz de transição utilizada para os cálculos. O início da estabilização a partir de π_{19} válida a capacidade do modelo de detectar anomalias persistentes, alinhando-se ao objetivo de identificar desvios em redes aeronáuticas.

5. CONSIDERAÇÕES

O modelo teórico baseado em Cadeias de Markov demonstrou eficácia na detecção de anomalias em redes aeronáuticas, como ACARS, VDL e SATCOM, respondendo ao problema de pesquisa sobre a identificação de mensagens malformadas ou tentativas de *spoofing* em sistemas complexos com dados limitados. A modelagem dos estados operacionais (Decolagem, Subida, Cruzeiro, Descida, Pouso, Emergência) e a construção de matrizes de transição permitiram representar o comportamento esperado de voos e identificar transições improváveis, como passagens para o estado de Emergência, associadas a falhas ou ciberataques.

Comparado a métodos estatísticos e de aprendizado de máquina, o modelo destaca-se pela simplicidade e interpretabilidade, sendo ideal para cenários com restrições de dados, embora limitado pela ausência de validação prática com dados reais. A abordagem contribui para a segurança aeronáutica, possibilitando o monitoramento em tempo real de redes e a prevenção de incidentes críticos. Aplicações práticas incluem a integração em sistemas de tráfego aéreo para alertas automáticos.

Apesar desses resultados positivos, é importante reconhecer limitações inerentes ao uso de Cadeias de Markov. Por dependerem de probabilidades fixas e da suposição de que o próximo

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

estado depende apenas do estado atual (propriedade markoviana), esses modelos podem não capturar relações mais complexas presentes em redes aeronáuticas reais, como dependências de longo prazo ou padrões não lineares. Além disso, ao contrário de técnicas mais avançadas como *autoencoders,* redes neurais recorrentes ou modelos baseados em aprendizado profundo, a abordagem markoviana tende a ter menor capacidade de adaptação a comportamentos dinâmicos ou altamente variáveis. Outra limitação observada é a sensibilidade do modelo à definição prévia dos estados e das matrizes de transição, o que pode reduzir sua precisão quando aplicado a cenários reais com ruído ou ambiguidades operacionais.

Além disso, recomenda-se que trabalhos futuros explorem a integração do modelo a sistemas embarcados de monitoramento em tempo real, permitindo que a detecção de anomalias seja aplicada diretamente durante as operações de voo. Outra possibilidade é a utilização de simulações com dados reais anonimizados, de forma a aproximar o modelo teórico das condições práticas observadas em redes aeronáuticas, ampliando sua aplicabilidade e robustez.

REFERÊNCIAS

DATACAMP**.** Uma introdução abrangente à detecção de anomalias. **DataCamp**, 2023. Disponível em: https://www.datacamp.com/pt/courses/understanding-anomaly-detection. Acesso em: 20 nov. 2025.

G1. Entenda como apagão cibernético que afeta computadores atingiu voos, serviços bancários e de saúde por todo o mundo. **G1**, 02 jul. 2021. Disponível em: https://g1.globo.com/mundo/noticia/2021/07/02/entenda-como-apagao-cibernetico-que-afeta-computadores-atingiu-voos-servicos-bancarios-e-de-saude-por-todo-o-mundo.ghtml. Acesso em: 20 nov. 2025.

G1. Senha roubada permitiu que hackers atacassem oleodutos da Colonial Pipeline, diz empresa. **G1**, 09 jun. 2021. Disponível em: https://g1.globo.com/economia/noticia/2021/06/09/senha-roubada-permitiu-que-hackers-atacassem-oleodutos-da-colonial-pipeline-diz-empresa.ghtml. Acesso em: 20 nov. 2025.

MINUTO DA SEGURANÇA. **Cibersegurança na aviação**. [S. l.]: Minuto da Segurança, 2025. Disponível em: https://minutodaseguranca.blog.br/ciberseguranca-na-aviacao/. Acesso em: 20 nov. 2025.

NETO, J. A.; COSTA, K. A. P.; PROENÇA JR., M. L. IPTraf: Coleta e detecção de anomalias em fluxos de rede. **Revista Brasileira de Computação Aplicada**, 2018. Disponível em: https://seer.upf.br/index.php/rbca/article/view/8153. Acesso em: 20 nov. 2025.

OLIVEIRA, R. L.; SAMPAIO, L. D. H.; ZARPELÃO, B. B.; PROENÇA JR., M. L. **Sistema de detecção de anomalias utilizando análise de fluxos**. São Paulo: Editora Universitária, 2020. Disponível em: https://editorauniversitaria.com.br/sistema-de-deteccao-de-deteccao-de-anomalias-em-redes-de-computadores.pdf. Acesso em: 20 nov. 2025.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

SILVA, Larissa Miguez da. **Cadeias de Markov e aplicações**. 2017. 71 f. Trabalho de Conclusão de Curso (Bacharelado em Matemática com ênfase em Matemática Computacional) – Universidade Federal Fluminense, Volta Redonda, 2017.

SILVA, R. **Detecção de anomalias em rede utilizando autoencoders e redes adversárias**. Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2020. Disponível em: https://monografias.poli.ufrj.br/monografias/monopoli10029123.pdf. Acesso em: 20 nov. 2025.

SÓ ESCOLA. O que é: aviação civil. **SÓ ESCOLA**, 15 set. 2023. Disponível em: https://soescola.com/glossario/o-que-e-aviacao-civil. Acesso em: 20 nov. 2025.

VALE, M. Crimes cibernéticos devem crescer em 2025, apontam especialistas. **Diário do Poder**, 2025. Disponível em: https://diariodopoder.com.br/brasil-e-regioes/e01-brasil/crimes-ciberneticos-devem-crescer-em-2025-apontam-especialistas. Acesso em: 20 nov. 2025.

VIZOLOGI. Qual é o modelo de negócios da OpenSky Network? Vizologi, [s. d.]. Disponível em: https://vizologi.com/es/lienzo-de-estrategia-empresarial/El-lienzo-del-modelo-de-negocio-de-la-red-Opensky/. Acesso em: 20 nov. 2025.

ZARPELÃO, B. B.; MENDES, L. S.; ABRÃO, T.; SAMPAIO, L. D. H.; LIMA, M. F.; PROENÇA JR., M. L. Detecção de anomalias em redes de computadores. In: XXVII Simpósio Brasileiro de Telecomunicações, 2009. Disponível em: http://www.sbrt.org.br/sbrt2009/anais/2009.pdf. Acesso em: 20 nov. 2025.