O USO DA TECNOLOGIA ESPACIAL EM OPERAÇÕES MILITARES

Categoria: Matemática Aplicada e/ou Inter-relação com outras Disciplinas

Modalidade: Ensino Médio

POLLETO, Cássia Regina Fracaro; GODOY, Leriane Dias; BARRIQUELLO, Marilei Rosanelli;

Instituição participante: Escola Técnica Estadual 25 de Julho - Ijuí/RS.

INTRODUÇÃO

O projeto em questão, realizado por um grupo da Turma 302, composto por 4 alunos, durante o período de 5 meses, integra as disciplinas de Matemática e Atividades Orientadas em Tecnologia. A pesquisa aborda o papel das comunicações via satélite em operações militares, destacando a importância de compreender suas vulnerabilidades e benefícios.

Diante da crescente ameaça de ataques cibernéticos, surge a curiosidade de como algoritmos de criptografia, fundamentados em teorias matemáticas complexas, podem garantir a segurança dessas comunicações. A questão central a ser investigada é: como a matemática é utilizada dentro da tecnologia espacial e qual seu papel dentro da prevenção de riscos ?

Os objetivos incluem não apenas compreender a tecnologia espacial aplicada nas operações militares, mas também propor medidas embasadas em análises estatísticas para prevenir problemas. A animação em vídeo e a maquete visam ilustrar o funcionamento dos satélites.

CAMINHO METODOLÓGICO, RESULTADOS E DISCUSSÃO

A pesquisa adotou uma abordagem qualitativa e bibliográfica, com coleta de dados a partir de artigos acadêmicos e fontes confiáveis. Para Mello (2001), o qualitativo está na interpretação da realidade e não em sua quantificação. Foram investigadas as vulnerabilidades das comunicações via satélite em operações militares e a aplicação de algoritmos de

criptografia para mitigar esses riscos. Foi realizada uma simulação, acompanhada de uma maquete, que representou a evolução dos satélites e demonstrou as técnicas de proteção e criptografia aplicadas. A análise dos dados utilizou uma revisão sistemática da literatura e métodos quantitativos para avaliar a eficácia das estratégias de segurança.

História e evolução dos satélites

Segundo Nobrega (2021), a exploração espacial teve início na Guerra Fria com o desenvolvimento do míssil balístico V2 pela Alemanha em 1942, que posteriormente se tornou o precursor dos primeiros veículos espaciais. Em 1957, a União Soviética gerou um marco histórico ao lançar o Sputnik, o primeiro satélite artificial, seguido pelo Sputnik 2, que levou o primeiro ser vivo ao espaço. Nesse período viu também os Estados Unidos responderem com seu próprio programa espacial e a fundação da NASA, acelerando a corrida espacial entre as superpotências.

Ao longo das décadas seguintes, avanços significativos foram alcançados com o desenvolvimento de satélites de comunicação. Segundo o site *National Air and Space Museum*, o Telstar, lançado em 1962, foi pioneiro na transmissão de sinais de televisão e telefone em escala global, embora fosse relativamente grande e pesado. Nas décadas de 1970 e 1980, os satélites geoestacionários, posicionados a cerca de 36.000 quilômetros acima da Terra, tornaram-se essenciais para comunicações, previsões meteorológicas e estudos astronômicos avançados.

Em um desenvolvimento paralelo, o Brasil ingressou na exploração espacial em 1993 com o lançamento do satélite brasileiro através do foguete Pegasus, de origem norte-americana. Mais tarde, em 2006, o país celebrou a primeira viagem espacial de um brasileiro, Marcos Pontes, a bordo da nave russa Soyuz TMA-8, partindo do Cazaquistão (Francisco, s/a).

Na era contemporânea, empresas privadas como a SpaceX têm desempenhado um papel crucial na exploração espacial, lançando constelações de satélites como o Starlink para fornecer internet de alta velocidade em escala global. Esses avanços destacam a evolução contínua das tecnologias espaciais e sua importância crescente na vida cotidiana e nos avanços científicos.

Por outro lado, na área militar, os satélites desempenham papéis cruciais em reconhecimento e comunicação. Satélites de reconhecimento são projetados para coletar

informações sobre alvos estratégicos, como bases militares inimigas, enquanto satélites de comunicação garantem conectividade segura e transmissão de dados em tempo real para as forças armadas. Essas capacidades têm redefinido as dinâmicas da segurança global e a estratégia militar moderna.

Estratégias de proteção e prevenção contra ataques cibernéticos

A era dos satélites militares começou com o lançamento do Sputnik 1 em 1957, marcando o início da utilização de satélites em operações estratégicas e militares. Desde então, esses dispositivos tornaram-se essenciais para comunicações, vigilância e reconhecimento, mas também expuseram vulnerabilidades significativas, especialmente em segurança cibernética. No decorrer do avanço tecnológico, surgiram ataques cibernéticos projetados para explorar falhas em sistemas de comunicação, o que levou à necessidade urgente de reforçar as defesas.

Entre as principais vulnerabilidades dos satélites estão a injeção de código malicioso, falhas de autenticação e a interceptação de dados durante a transmissão. Esses problemas podem expor informações estratégicas e comprometer operações militares. As comunicações via satélite, por exemplo, enfrentam riscos de ataques como *ransomware* e ataques de *Distributed Denial of Service* (DDoS), que bloqueiam o acesso a sistemas críticos ou sobrecarregam a rede, tornando-a inacessível. Priorizar a segurança cibernética é crucial para mitigar essas ameaças, protegendo dados sensíveis contra ataques e invasões.

Para combater essas vulnerabilidades, diversas estratégias de proteção têm sido adotadas. A criptografia desempenha um papel vital na proteção das comunicações via satélite. Algoritmos como RSA e AES, que utilizam operações matemáticas complexas, garantem que dados sejam transmitidos de forma segura, criptografando as informações para evitar interceptações. No caso do RSA, a segurança se fundamenta na seguinte fórmula:

$$(m^{e})^{d} = m\ (mod\ N)$$

m – mensagem a ser transmitida
e – exponencial da chave pública (e,N)
d - exponencial da chave privada
N – número grande produto de dois primos

Além disso, o uso de técnicas como Pentest (testes de penetração) permite analisar seu nível de proteção testando todo o ambiente, simulando um ataque real de um criminoso e medindo o risco e as consequências desses ataques (VIEIRA, 2018).

A latência do sinal, outro problema técnico significativo em satélites geoestacionários, também pode comprometer a eficiência das comunicações, especialmente em tempo real. Para mitigar esse problema, estratégias de compressão de dados e protocolos de transmissão eficientes são empregados, baseados em princípios matemáticos de otimização e teoria da informação. Além disso, algoritmos de correção de erros, como os códigos de Hamming e CRC, são aplicados para garantir que os dados transmitidos sejam íntegros, mesmo em condições de interferência.

Em suma, enquanto os satélites militares oferecem vantagens estratégicas, eles permanecem alvos vulneráveis a uma série de ameaças. A combinação de criptografia avançada, simulações de ataques e algoritmos matemáticos de correção de erros é fundamental para reforçar a segurança dessas comunicações críticas, garantindo que as operações militares não sejam comprometidas por falhas de segurança ou ataques cibernéticos.

Entre os tipos de estratégias de prevenção, o pentest se mostra eficaz para prevenir e manter a rede constantemente segura. Consiste em um método de testes com diversas etapas com o objetivo de verificar e analisar as possíveis vulnerabilidades dentro de uma rede(Vieira, 2018). Esses métodos envolvem o uso de simulações desses ataques para analisar qual o nível atual da segurança e diagnosticar se há alguma falha existente tanto em hardware quanto em software para correção.

Ainda sobre proteção e prevenção, existem meios que são utilizados por todo o mundo, como os programas antivírus que oferecem proteção e capacidade de eliminar quaisquer ameaças no computador, e também os VPNs, que criptografam o tráfego do usuário dentro da rede dificultando ataques no computador ou na rede.

Vulnerabilidades das comunicações via satélite

No dia 4 de outubro de 1957, às 19h12, a União Soviética lançava com sucesso o primeiro satélite artificial do mundo, o Sputnik I . Com o tamanho de uma bola de basquete e peso de 83,6 kg, o Sputnik I levava aproximadamente 98 minutos para orbitar a Terra em trajetória elíptica. Seu lançamento inaugurou uma política militar com novos

desenvolvimentos tecnológico-científicos e marcou o começo da era espacial de russos e norte-americanos (GARBER, 2007). Desde então, os satélites evoluíram, tornando-se fundamentais para comunicações, vigilância e reconhecimento, mas também expondo novas vulnerabilidades tecnológicas.

Satélites militares modernos enfrentam desafios de segurança significativos. Entre as principais vulnerabilidades estão a injeção de código malicioso, falhas de autenticação e a interceptação de dados durante a transmissão. Esses problemas podem expor informações sensíveis e comprometer a segurança das operações militares, exigindo atenção constante às falhas nos sistemas de comunicação.

Outro grande problema nas comunicações via satélite é a latência do sinal, principalmente em satélites geoestacionários, que orbitam a 36.000 km da Terra. Essa latência afeta a performance de aplicações em tempo real, como videoconferências e transmissões de dados, e expõe as operações a riscos de atrasos críticos.

A capacidade de reprogramar satélites em órbita, embora útil para atualizações, também introduz novas vulnerabilidades. Hackers podem tentar assumir o controle ou alterar a função desses dispositivos, aumentando o risco de manipulação maliciosa. Além disso, os altos custos de manutenção tornam a segurança uma preocupação constante, já que qualquer falha pode ter consequências financeiras e operacionais severas.

Em resumo, apesar da sua importância estratégica, os satélites militares continuam suscetíveis a uma série de vulnerabilidades tecnológicas, tornando essencial que novas abordagens e medidas sejam desenvolvidas para mitigar esses riscos.

Fortalecendo a segurança global: cooperação internacional na comunicação militar via satélite

A preservação e proteção das comunicações militares por satélite é crucial para a segurança nacional de muitos países. Esse tipo de comunicação é vital para operações militares, vigilância e controle estratégico, tornando-se alvos de ataques cibernéticos e físicos. Países devem cooperar internacionalmente, pois nenhum país pode proteger seus satélites sozinho devido a áreas que atravessam fronteiras. Isto requer regras de cibersegurança, como normas de defesa e protocolos de proteção.

Regras e acordos de segurança em que todos os países concordem são necessários para garantir a integridade das comunicações via satélite. Esses acordos podem incluir padrões de

segurança cibernética, protocolos de resposta a incidentes e restrições sobre armas espaciais contra satélites.

Medidas estão sendo adotadas para fortalecer a segurança dos satélites militares através da cooperação internacional, como o compartilhamento de informações sobre ameaças e vulnerabilidades e a realização de exercícios conjuntos de segurança cibernética e física. Isso fortalece as defesas individuais e promove a confiança mútua e a transparência entre as nações, reduzindo equívocos e assegurando a coordenação eficaz das respostas a incidentes.

A cooperação internacional é essencial para proteger as comunicações de defesa por satélite, especialmente com os desafios de segurança crescendo rapidamente. Com regras claras, acordos fortes e ações coordenadas, os países podem garantir que suas redes de satélites militares permaneçam seguras e operacionais, mesmo diante de ameaças emergentes e em constante evolução.

CONCLUSÃO

A pesquisa evidenciou que, embora a evolução da tecnologia espacial tenha proporcionado avanços significativos nas operações militares, também trouxe novos desafios relacionados à segurança cibernética das comunicações via satélite. As vulnerabilidades identificadas, como injeção de código e falhas de autenticação, destacam a necessidade de inovações constantes e colaboração internacional para desenvolver normas de segurança e compartilhar informações sobre ameaças. Assim, a proteção dessas comunicações é fundamental para garantir a eficácia operacional e a segurança de informações sensíveis em um cenário global cada vez mais interconectado e suscetível a ataques cibernéticos.

REFERÊNCIAS

FRANCISCO, Wagner de Cerqueira e. **Conquista do Espaço**, Brasil Escola. Disponível em: https://brasilescola.uol.com.br/geografia/conquista-do-espaco2.htm. Acesso em: 16 de abr. 2024.

GARBER, Steve. **Sputnik and The Dawn of the Space Age,** 2007. Disponível em: https://www.nasa.gov/history/sputnik/index.html. Acesso em: 11 de jul. 2024.

MELLO, Luiz Gonzaga de. **Antropologia cultural:** iniciação teorias e temas. 8. ed. São Paulo: Vozes, 2001.

NATIONAL AIR AND SPACE MUSEUM. **Telstar.** Disponível em: https://airandspace.si.edu/collection-objects/communications-satellite-telstar/nasm_A20070113000. Acesso em: 11 jul. 2024.

NOBREGA, Leila Berg da. **Capítulo 10:** Histórico da Exploração Espacial. Acervo museológico dos laboratórios de ensino de física, 2021. Disponível em: https://www.ufrgs.br/amlef/2021/11/30/capitulo-10-historico-da-exploracao-espacial/#:~:text=A%20primeira%20publica%C3%A7%C3%A3o%20s%C3%A9ria%20que,o%20Sputnik%202%2C%20em%20sequ%C3%AAncia. Acesso em: 03 de abr. 2024.

VIEIRA, Yago Dyogennes Bezerra. **Utilização de pentest na prevenção de ataques cibernéticos às organizações**. 2018. Disponível em: https://repository.ufrpe.br/handle/123456789/1542. Acesso em: 5 de abr. 2024.

Trabalho desenvolvido com a turma 302, da Escola Técnica Estadual 25 de Julho, pelos alunos: Cássia Regina Fracaro Polleto; Gabriel da Silva Corrêa Frantz; Leriane Dias Godoy; Natália da Silva da Costa.

Dados para contato:

Expositor: Cássia Regina Fracaro Polleto; **e-mail:** cassia-rfpolleto@educar.rs.gov.br;

Expositor: Leriane Dias Godoy; **e-mail:** leriane-godoy@educar.rs.gov.br;

Professor Orientador: Marilei Rosanelli Barriquello;

e-mail: marilei-rbarriquello@educar.rs.gov.br;