Journal of Technology & Information

Detecção de *Man-In-The-Middle* em Redes Locais por Meio de Análise do *Address Resolution Protocol*

Local Area Network Man-In-The-Middle Detection Through Address Resolution Protocol Analysis

Recebido: 24/04/2023 | Revisado: 18/05/2023 | Aceito: 20/06/2023 | Publicado: 21/06/2023

https://www.doi.org/10.5281/zenodo.8064015

Felipe Gonçalves Kobayashi
Fatec de Santana de Parnaíba
https://orcid.org/0000-0002-4496-9951
felipe.kobayashi@fatec.sp.gov.br

Irapuan Glória Júnior
Fatec Santana de Parnaíba
http://orcid.org/0000-0003-2973-3470
ijunior@ndsgn.com.br

Resumo

Este artigo destina-se à identificação de pesquisas existentes a respeito de métodos de detecção de *Man-In-The-Middle* em redes locais por meio de análises do protocolo ARP realizadas por inteligências artificias. A pesquisa possui natureza qualitativa e a revisão sistemática foi utilizada como procedimento metodológico. Os principais resultados mostraram que 31% dos artigos focam em vulnerabilidades de redes locais, 31% visam métodos de envenenamento do ARP, 19% estudam métodos detectivos por meio de uma análise do *Round Trip Time* e 19% dos artigos pesquisaram métodos de automatização de análises por meio de *machine learning*. A contribuição para a teoria é estabelecer um caminho para que estudos mais aprofundados possam ser realizados com base neste artigo. Em relação a contribuição para a prática é de demonstrar que existe formas efetivas de detecção de MITM.

Palavras-chave: *Man-In-The-Middle*, redes locais, *ARP*, detecção.

Abstract

This article is intended to identify existing research on Man-In-The-Middle detection methods in Local Area Networks through ARP protocol analyses performed by artificial intelligences. The research has a qualitative nature and the systematic review was used as a methodological procedure. The main results showed that 31% of the articles focus on vulnerabilities of local networks, 31% aim at ARP poisoning methods, 19% study detectable methods through a Round Trip Time analysis and 19% of the articles researched methods of automating analyses through machine learning. The contribution to theory is to establish a path for further studies to be conducted based on this article. Regarding the contribution to the practice, it is to be demonstrated that there are effective forms MITM detection.

Keywords: Man-In-The-Middle, Local Area Network, ARP, detection.

1. Introdução

Com o passar do tempo, as informações se tornaram um dos bens mais valiosos que o homem pode obter, devido a informação ser sinônimo de poder para muitos. Com isso, muitos passaram a desenvolver métodos de invasão com a intenção de roubarem as informações, seja para vender, benefício próprio ou qualquer outra finalidade. Um dos métodos que se tornaram conhecidos na área de segurança da informação é o ataque denominado de *Man in the Middle* (MITM), que faz com que o atacante intercepte os dados que estão sendo trocados em uma comunicação entre dois ou mais dispositivos (Liu, Cobert & Cheng, 2019).

A facilidade de execução e a dificuldade de detecção são características de um ataque MITM, o que o torna viável para o roubo de informações confidenciais. Um dos métodos de detecção estudados neste artigo se baseia em análises do *Address Resolution Protocol* (ARP) feitas por inteligência artificial, no qual o tempo de resposta das requisições são analisadas para descobrirem se há alguma anomalia na rede (Folarin, 2019).

Este artigo possui como questão de pesquisa: "Quais as pesquisas a respeito da detecção de *Man-In-The-Middle* em redes locais por meio de uma análise do ARP realizada por inteligência artificial?". Os objetivos são: (1) Identificar os artigos existentes a respeito de detecção de MITM por meio do ARP; e (2) Apresentar as linhas de pesquisa a respeito do tema.

2. Referencial Teórico

2.1. Local Area Network

A rede local, também conhecida como LAN, é uma forma de estabelecer a conexão entre diversos dispositivos para que consigam trocar informações, e para isso é necessário um dispositivo de rede, como um *switch*; um meio de comunicação, como

cabos coaxiais, par trançado e até fibra ótica; e os dispositivos finais, que são qualquer dispositivo que se conecte à rede (Goni, 2021).

Manter a rede local segura contra os ataques conhecidos como MITM, *Denial of Service* ou até de malwares é essencial quando se trata da segurança dos dados que trafegam pela rede, portanto, a implementação de um sistema de *Intrusion Prevention System* (IPS) junto com um *Intrusion Detection System* (IDS) são práticas comuns na área de segurança da informação para garantir a integridade dos dados que estão na rede (Hussain, Induruwa & Qi, 2021).

2.2. Man-In-The-Middle

O MITM é um método de invasão na área da segurança da informação que consiste em se infiltrar em uma conexão entre dois dispositivos finais, podendo utilizar-se de diversos métodos de infiltração, com isso será possível interceptar os pacotes que são enviados entre eles, podendo apenas visualizar, deletar ou até editar as informações que são trafegadas na comunicação, por isso foi traduzido como "Homem no meio" (Ganapathy, 2020).

Por mais que o MITM seja um método de ataque considerado antigo, ainda é um dos desafios da segurança da informação por ser um ataque simples de se executar, dependendo do método utilizado para se infiltrar, e muito complicado de ser detectado pela complexidade de se identificar um intruso na rede, entretanto, com o passar do tempo diversas técnicas foram sendo desenvolvidas pelos pesquisadores para a detecção de MITM em redes locais, uma delas é a implementação de um *Intrusion Detection System*, outra foi a proposta de alteração do protocolo ARP, que é um dos principais alvos dos atacantes de MITM, envolvendo novas criptografias e até o modo como as requisições são feitas e entre outras formas que não solucionaram o problema de MITM por completo, seja pelo custo ou pela complexidade de implementação. (Kponyo, Agyemang & Klogo, 2020).

2.3. Address Resolution Protocol

O protocolo de resolução de endereços é responsável pelo mapeamento dos dispositivos que estão na rede, de forma a salvar o endereço físico de um dispositivo associado com o seu endereço lógico em seu cache, podendo ser IPV4 ou IPV6, portanto, para que um dispositivo se comunique com outro pela LAN é necessário que se tenha o endereço MAC. No caso de um dispositivo que ainda não tenha sido mapeado, o *host* que solicitar a comunicação enviará uma requisição ao ARP que enviará um *broadcast* na rede para localizar o endereço físico não mapeado e o encontrado responderá com um pacote em formato *unicast* contendo seu endereço físico para que seja mapeado e assim estabelecendo a comunicação entre os dispositivos (Nasser & Hussain, 2022).

Uma das formas de se conseguir informação de forma indevida é por meio do envenenamento do ARP, que geralmente acontece com o envio de requisições alteradas para comprometer a integridade do seu cache, e com seu comprometimento será possível que o atacante se passe pelo endereço físico de qualquer dispositivo na rede, assim interceptando os pacotes que são trafegados pela rede. Esse caso seria uma forma de ataque MITM usando o ARP como método de infiltração, entretanto, há outras formas de prejudicar a rede com o envenenamento do protocolo. Um exemplo seria ao invés de interceptar os pacotes, o atacante poderia excluir todos os pacotes da rede gerando um ataque de negação de serviço (Ganapathy, 2020).

Ainda há outras formas que são utilizadas para comprometer a integridade das informações da rede, nesse caso são por meio do envenenamento da requisição ou da resposta do protocolo ARP, para uma melhor compreensão desses ataques há um exemplo que é muito usado, no qual há um computador e o atacante se passa pelo gateway da rede, dessa forma, o atacante envia uma requisição do ARP ao dispositivo com informações falsas para se passar pelo *gateway*, o que faz com que esse protocolo atualize suas informações de *cache* com as informações passadas pelo suposto *gateway* (Nasser &

Hussain, 2022). Há versões com o uso de inteligência artificial (Kponyo, Agyemang & Klogo, 2020).

Diferente da requisição, o envenenamento da resposta acontece de forma que o dispositivo recebe uma mensagem de resposta sem que uma requisição tenha sido feita anteriormente, sendo assim, essa técnica não é utilizada pelos atacantes por ser fácil de se identificar, afinal, não existe uma resposta sem uma requisição (Nasser & Hussain, 2022).

Uma solução que foi proposta por pesquisadores se baseia em análises do protocolo ARP realizadas por inteligências artificias, no qual diversas requisições do ARP seriam enviadas pela rede em busca de anomalias no tempo de resposta dos dispositivos, em que esse método se provou eficaz pelos testes feitos, pois o atacante não consegue se ocultar para que não receba esses pacotes por ser um protocolo que está presente em todos os dispositivos (Kponyo, Agyemang & Klogo, 2020).

3. Metodologia

Este artigo é de natureza qualitativa (Martins & Theophilo, 2016), no qual a metodologia de revisão sistemática (Kitchenham, 2004) foi utilizada para encontrar outros artigos que tratassem a respeito de MITM em redes locais por meio de envenenamento do ARP.

3.1 Procedimentos metodológicos

Os procedimentos metodológicos adotados para essa pesquisa foram:

Passo 1: Identificação da pesquisa. As *strings* de busca foram elaboradas e testadas nesta etapa, no qual diversos termos relacionados ao comprometimento da integridade dos dados em uma rede local foram utilizados, alguns deles foram: *Man-In-The-Middle*, *ARP spoofing*, *machine learning e local area networks*.

Passo 2: Seleção dos artigos. Todos os artigos encontrados a partir de 2018 que tinham alguma relação com o tema principal foram selecionados para estudo.

Passo 3: Extração dos dados e monitoramento. Uma análise mais profunda foi realizada nos artigos selecionados para extrair o máximo de informações úteis possíveis dentro de cada artigo para que fossem utilizadas neste documento.

Passo 4: Síntese dos dados. Assim que todas as informações necessárias foram obtidas, deu-se início a escrita do artigo em questão, expondo todos os principais pontos dos artigos que foram selecionados nas etapas anteriores.

3.2 Critérios de seleção

A revisão sistemática considera os seguintes itens para a escrita de um artigo:

(1) Somente os artigos com até 5 anos de existência serão considerados, portanto, no ano de 2022, todos os artigos de 2017 e de anos anteriores não são considerados.

(2) Somente artigos científicos publicados devem ser considerados, dessa forma descarta-se monografias, teses, livros, dissertações e qualquer outro documento.

(3) Documentos no formato PDF.

(4) Os artigos devem apresentar conteúdos relacionados ao tema do artigo a ser escrito.

3.3 Termos de pesquisa

Os termos de pesquisa utilizados para a busca de material válido para este artigo foram "*Man-in-the-middle*", "*Local area network*", "*Address resolution protocol*", "*analysis*", "*Machine Learning*" e "*Detection*" conforme apresentado na Tabela 1.

Tabela 1 – *String* de busca

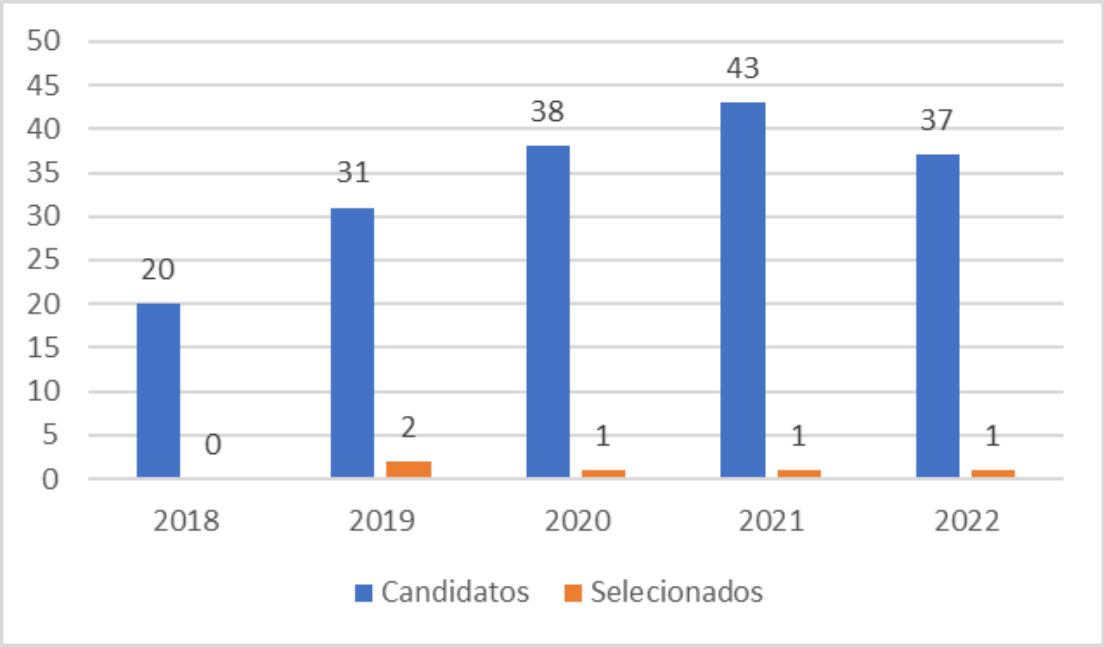
Base	String
Google Scholar www.scholar.google.com.br	*("Man-in-the-middle" AND "local area network") AND ("Address resolution protocol" AND "analysis") AND ("Machine Learning") AND ("Detection")*

4. Análise e Interpretação dos Resultados

4.1. Artigos disponíveis a respeito de MITM por meio do protocolo ARP

De acordo com a pesquisa realizada pode-se perceber que houve uma crescente publicação de artigos científicos a respeito de MITM a partir de 2018 até o final de outubro de 2022, como mostra na Figura 1.

Figura 1 – Artigos candidatos e selecionados



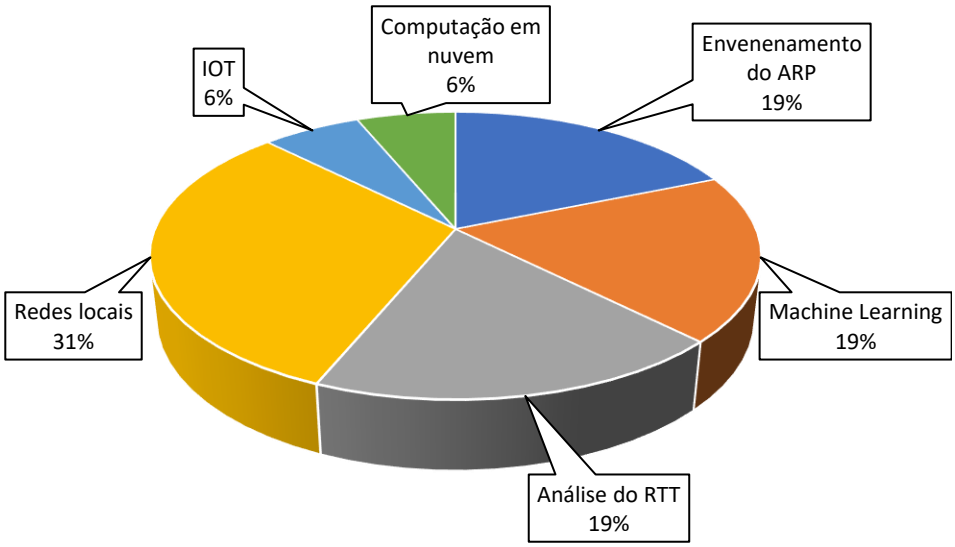
4.2. Orientações de estudo dos artigos selecionados

Os resultados das pesquisas a respeito de detecção de MITM, conforme é mostrado na Figura 2, revelaram que há diversas áreas de estudos entre os artigos selecionados, no qual uma delas está focada no envenenamento do ARP (19%), que é um dos métodos de invasão MITM que consiste em manipular os valores da tabela ARP (Nasser & Hussain, 2022; Hussain, Induruwa & Qi, 2021; Liu, Cobert & Cheng, 2019). Com isso, um dos métodos de detecção mais eficazes é baseado na análise do tempo de resposta (19%), denominado *Round Trip Time* (RTT), de um determinado protocolo, que nos artigos selecionados foram analisados os protocolos ARP (Kponyo, Agyemang & Klogo, 2020), *Internet Control Message Protocol* (ICMP) (Liu, Cobert & Cheng, 2019) e *Secure Socket Layer* (SSL) (Folarin, 2019).

A partir das análises do RTT dos protocolos, a área de *machine learning* (19%) foi abordada com o intuito de automatizar estas análises e assim tornar o processo mais efetivo para a detecção de MITM, de forma que observasse a rede em busca de anomalias no tempo de resposta de um determinado protocolo para detectar uma possível invasão (Folarin, 2019; Liu, Cobert & Cheng, 2019; Kponyo, Agyemang & Klogo, 2020).

Outra área de estudos abordada em todos os artigos são as redes locais (31%), que é essencial para evitar possíveis vulnerabilidades que possibilitem o fácil acesso à rede, o que poderia levar a um ataque MITM ou diversos outros tipos de ataques. Além disso, ainda existe uma área de estudos voltada a *Internet Of Things* (IOT) (6%), que busca compreender os riscos de um ataque MITM neste ambiente (Hussain, Induruwa & Qi, 2021), e a área que aborda a questão da computação em nuvem (6%) (Liu, Cobert & Cheng, 2019).

Figura 2 – Índice porcentual de estudos dos artigos selecionados



4.3. Discussão

Os ataques MITM são uma das preocupações na área da segurança da informação e com o passar do tempo diversas pesquisas surgiram com propostas diferentes tanto para detecção quanto para mitigação dos danos causados por uma invasão.

Dentre os artigos, havia os que falavam sobre MITM em redes elétricas, em sistemas de Identificação por Radiofrequência (RFID) e poucos voltavam seu foco para as redes locais no começo de 2018, entretanto, essa realidade mudou por volta de 2021, no qual a maioria dos artigos publicados tinham seu foco para MITM em LAN e em 2022 havia mais de 10 artigos a respeito, o que indica que os pesquisadores começaram a se preocupar mais com o tema.

5. Conclusões

Com o passar do tempo, a informação se tornou um dos bens mais valiosos que o ser humano pode obter, afinal, informação é poder e mantê-las seguras é essencial. Com isso, diversos ataques surgiram para a obtenção de informações ilegais e dentre eles há o MITM, que é um ataque relativamente simples de se executar e muito complicado de ser identificado, se executado corretamente.

O resultado da pesquisa apresentou que os artigos tinham como foco métodos para detecção de MITM e o mais recorrente nos artigos utilizava uma análise do RTT do protocolo ARP por meio de *machine learning*, que possibilitou uma análise mais precisa no tempo de resposta dos dispositivos que estejam conectados na rede em busca de anomalias que podem levar a uma suspeita de MITM.

Como contribuição teórica deste artigo está o estabelecimento de um caminho de estudos, que ainda não há tanto foco por parte dos pesquisadores, para que outros possam aprofundar ainda mais em busca de outros métodos detectivos de MITM que envolvam o protocolo ARP. Enquanto na prática, este artigo demonstra que de fato existem métodos detectivos efetivos de MITM que podem ser usados por profissionais de segurança da informação para estudo.

As futuras pesquisas estão relacionadas a um estudo mais aprofundado sobre a implementação de métodos detectivos, assim como uma abordagem mais detalhada a respeito das técnicas utilizadas para detectar MITM.

Referencial Bibliográfico

CHENG, C.; COLBERT, E.; LIU, H.; (2019) *Experimental Study on the Detectability of Man-in-the-Middle Attacks for Cloud Applications. Washington: The Catholic University of America*

FOLARIN, S.; (2019) *Improved ssl/tls man-inthe-middle attack detection technique using timing analysis and other behavioral anomalies. Ireland: National College of Ireland*.

GANAPATHY, A.; (2020) *Virtual Dispersive Network in the Prevention of Third Party Interception: A Way of Dealing with Cyber Threat. California*: ABCJAR.

GONI, O.; (2019) *Implementation of local area network (lan) and build a secure lan system for atomic energy research establishment. International Associations of Professionals and Technical Teachers*.

HUSSAIN, F.; INDURUWA, A.; QI, M.; (2021) *Security Vulnerabilities of Popular Smart Home Appliances. United Kingdom: School of Engineering, Technology and Design Canterbury Christ Church University Canterbury*.

KITCHENHAM, B. (2004). *Procedures for Performing Systematic Reviews*.Vol. Keele, v. 33. 1-26.

KPONYO, J.; AGYEGMAN, J.; KLOGO, G.; (2020) *Detecting End-Point (EP) Man-In-The-Middle (MITM) Attack based on ARP Analysis: A Machine Learning Approach*. Ghana: IJCNIS.

NASSER, H.; HUSSAIN, A.; (2022) *Provably curb man-in-the-middle attack-based ARP spoofing in a local network.* Iraq: *Bulletin of Electrical Engineering and Informatics*.

THEOPHILO, C. R.; MARTINS, G. de A. (2016). Metodologia Da Investigação Científica(3a). Atlas.

ANEXO A – Artigos selecionados

Ano	Título/Autores	Foco
2019	*Experimental Study on the Detectability of Man-in-the-Middle Attacks for Cloud Applications* Cheng-yu Cheng Edward Colbert Hang Liu	Detecção de MITM com envenenamento do ARP em aplicações em nuvem por meio de análise do RTT do ICMP
2019	*Improved ssl/tls man-in-the-middle attack detection technique using timing analysis and other behavioral anomalies* Samuel Folarin	Detecção de MITM em redes por meio de análise do RTT do SSL handshake
2020	*Detecting End-Point (EP) Man-In-The-Middle (MITM) Attack based on ARP Analysis: A Machine Learning Approach* Jerry John Kponyo Justice Owusu Agyemang Griffith Selorm Klogo	Detecção de MITM em redes por meio de análise do RTT do ARP
2021	*Security Vulnerabilities of Popular Smart Home Appliances* Fida Hussain Abhaya Induruwa Man Qi	Vulnerabilidades em redes locais envolvendo aplicações IOT
2022	*Provably curb man-in-the-middle attack-based ARP spoofing in a local network* Hiba Imad Nasser Mohammed Abdulridha Hussain	Deteção de envenenamento do ARP para ataque MITM em redes locais