Instituto Nacional de Telecomunicações
Mestrado em Telecomunicações
TP546 - Internet das Coisas e Redes Veiculares
Prof. Dr. Samuel Baraldi Mafra

PROBLEMAS DE SEGURANÇA EM REDES IOT COM FOCO EM ATAQUE SYBIL

Flávio Romeiro Simões

5 de outubro de 2024

Resumo

A Internet das Coisas (IoT) conecta dispositivos físicos à rede, trazendo conveniência, mas também vulnerabilidades, como o ataque Sybil. Esse ataque envolve a falsificação de identidades de nós, afetando a integridade e o desempenho da rede. Para mitigar ataques Sybil, são utilizados métodos como criptografia, análise de força de sinal (RSSI) e inteligência artificial. A criptografia garante a segurança das comunicações, enquanto o RSSI ajuda a identificar nós maliciosos com baixo consumo de energia. Técnicas de inteligência artificial, como algoritmos de enxame, melhoram o roteamento e detectam intrusões de forma eficiente.

1 Introdução

O conceito Internet das Coisas (IoT) vem da capacidade de dispositivos físicos se conectarem a uma rede e trocar dados, onde cada dispositivo pode ser identificado de forma única [1], desde dispositivos domésticos inteligentes até sensores industriais. Estes dispositivos uma vez conectados trazem conveniência e eficiência. No entanto, esta conectividade podem apresentar vulnerabilidades e serem uma porta de acesso de ataques às empresas, lares e outras instituições a que estejam conectados. Neste sentido este trabalho explora os principais problemas de segurança que os dispositivos IoT podem apresentar e dentre eles destacar o ataque Sybil e quais as soluções para mitigar este tipo de ataque.

2 As camadas que compõe uma arquitetura IoT

Essencialmente a arquitetura IoT é formada pela camada de percepção que contém os dispositivos físicos é a camada de sensoriamento devido aos sensores incorporados nos objetos físicos, nesta camada os sensores fazem as coletas dos dados dos dispositivos e encaminham para a camada de rede. A camada rede faz a conexão da camada de percepção por meio de conexões com fio ou sem fio com a camada de aplicação. A camada de aplicação recebem os dados fazendo o tratamento com o fornecimento de serviços e tomada de decisões e enviando os resultados para a camada de percepção por meio da camada de rede [4], conforme ilustrado na figura 1.

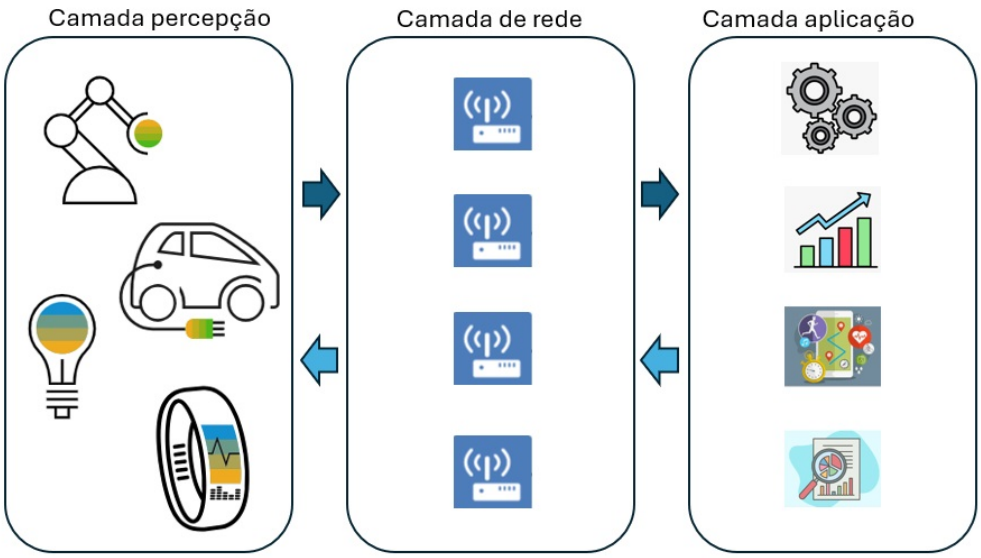

Figura 1: Arquitetura IoT em três camadas

Cada camada necessita de mecanismos para garantir a integridade das informações que são trocadas entre os dispositivos contidos na camada de percepção e a camada de aplicação, e conhecendo as características de cada camada que formam a arquitetura IoT permite entender melhor seus pontos fortes e fracos em termos de vulnerabilidade e qual tipo de ataque seria mais prejudicial.

3 Os problemas de segurança relacionados a IoT

Ao contrário dos sistemas de informações tradicionais que possuem um cenário de segurança robusto, com regras e procedimentos definidos, a segurança relacionada ao IoT ainda não se mostra madura o suficiente, onde os fabricantes priorizam o funcionamento dos dispositivos e não se preocupam com os aspectos de segurança necessários para estes dispositivos[2]. Um resumo de problemas de segurança relacionados a IoT é destacado na tabela 1 [1].

Os problemas de segurança de IoT conforme destacados, podem ser a porta de acesso para os ataques se não mitigados. Na figura 2, é demonstrado os tipos ataques que podem ocorrer nas camadas de percepção, rede e aplicação [5].

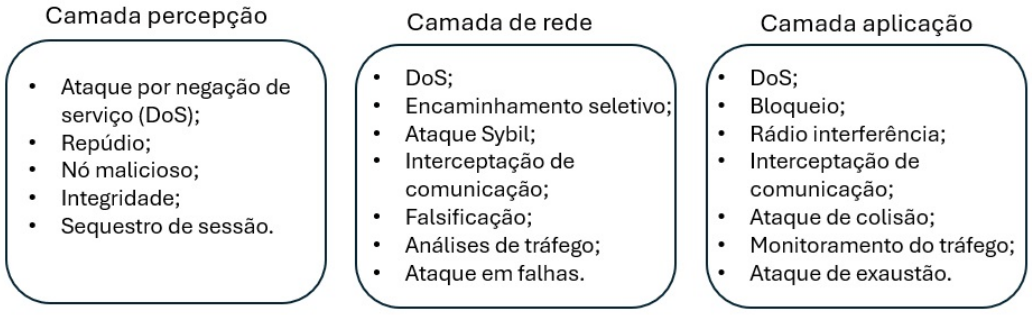

Figura 2: Camadas e possíveis ataques

4 O Ataque Sybil na camada de rede IoT

Neste tipo de ataque, um nó malicioso assume a identidade de um verdadeiro nó IoT, manipulando a identidade de nós que foram comprometidos. Isso resulta em um impacto negativo no desempenho da rede. O dispositivo falsificado pode sobrecarregar os canais com pacotes enganosos, tornando os serviços do sistema IoT indisponíveis para usuários autorizados. Além disso, ele pode realizar escuta clandestina nas comunicações, criar mensagens fraudulentas[5], influenciar decisões, como o consenso em redes distribuídas, ou controlar o tráfego de informações. A detecção desse tipo de ataque é complexa, pois identificar e distinguir entre identidades legítimas e falsas representa um desafio, especialmente em redes que carecem de métodos eficientes para verificar a identidade. As consequências do ataque Sybil são significativas e abrangem várias áreas. Primeiramente, há o comprometimento da integridade dos dados, uma vez que o atacante pode inserir informações erradas ou enganosas na rede. Isso resulta em uma redução da confiabilidade do sistema, pois a confiança nas interações entre os nós da rede pode ser prejudicada, impactando o desempenho e a eficácia da rede como um todo. Com este tipo de ataque surgem dificuldades em mecanismos de segurança, uma vez que os protocolos que dependem da identidade dos nós podem ser facilmente burlados, tornando a rede mais vulnerável a ataques e manipulações. Sendo o ataque Sybil uma ameaça iminente às redes IoT algumas medidas contra este tipo de ataque consiste em prever antecipadamente que o ataque poderá ocorrer, detectar quando há uma violação de segurança na rede e mitigar por meio de soluções que reduzam os impactos causados por este tipo de ataque [7].

4.1 Algumas soluções de mitigação do ataque Sybil

Em pesquisas recentes, pesquisadores se concentram em mecanismos de criptografia, indicador do sinal mais forte recebido (RSSI) e Inteligência artificial como alternativas contra ataques Sybil.

4.1.1 Criptografia

Embora demande considerável poder de processamento, a criptografia continua a ser uma área ativa de pesquisa com enfoques principais em distribuição de chaves determinística e a probabilística. Nos métodos determinísticos, para garantir máxima segurança, cada entidade pode estabelecer um vínculo seguro com outras. Contudo, o protocolo de gerenciamento de chaves se torna suscetível a ataques de segurança. Técnicas criptográficas como criação e gerenciamento, distribuição e validação de chaves para identidades são opções. A distribuição de chaves simétricas utiliza uma chave idêntica para criptografar e descriptografar mensagens, como o Padrão de Criptografia Avançada (AES), o Rivest Cipher 4 (RC4) e o Triple Data Encryption Standard (3DES). No entanto, desafios no gerenciamento de chaves e questões de escalabilidade são as principais desvantagens da chave simétrica. Os nós da rede são alimentados por baterias, o que não é apropriado para a implementação de criptografia de chave pública devido ao elevado consumo de processamento e à carga alta na rede ao gerar, distribuir e manter chaves. Dispositivos criptográficos estão mais vulneráveis a ataques de força bruta. A distribuição de chaves assimétricas emprega a chave pública para criptografar, enquanto a chave privada é utilizada para descriptografar.

Um método de autenticação de nós para sensores sem fio, com o objetivo de prevenir ataques de segurança e garantir canais de comunicação seguros. A estação base é responsável por gerar um valor aleatório e um valor secreto para distribuir entre os nós sensores, que devem armazenar seus respectivos valores. Outro método como o uso da árvore de hash de Merkel, valores de confiança e códigos de autenticação de mensagens para um algoritmo de verificação de localização, funcionando bem em redes organizadas em uma estrutura hierárquica. Esse método se insere na taxonomia de criptografia híbrida. Um modelo baseado em políticas de segurança foi sugerido para unir um modelo de distribuição em grupo com criptografia baseada em identidade. Além disso, outra proposta combinou as vantagens dos métodos criptográficos públicos e simétricos para gerenciamento de chaves em redes sem fio, onde cada nó é equipado com um sistema de chave pública para estabelecer chaves simétricas ponto a ponto com outros nós. Uma abordagem adicional implantou nós auxiliares para realizar o estabelecimento de chaves entre os nós sensores, utilizando um Algoritmo de Agrupamento Fuzzy seguro para determinar quais nós podem se unir ao cluster de forma segura. O cabeçote do cluster supervisiona o roteamento com base em critérios de confiança e energia. Foi sugerido também um esquema escalável e robusto de estabelecimento de chaves hierárquico que melhora a resiliência contra captura de nós, análise de tráfego e spoofing de reconhecimento. Além disso, esse esquema proporciona atualizações críticas periódicas sem custos de comunicação para transporte de chaves. Existe ainda uma abordagem para mitigar o ataque Sybil, composta por dois algoritmos inovadores: o primeiro fragmenta os dados para evitar a detecção por um nó malicioso, enquanto o segundo visa fornecer autenticação para nós que se juntam à rede por meio

da criptografia [7].

4.1.2 RSSI

O RSSI tem sido utilizado para identificar ataques Sybil e não exige hardware especializado para estimar a localização de vizinhos, onde diferentes abordagens têm sido exploradas, utilizando apenas dois receptores e outras incorporando múltiplos vizinhos para aumentar a precisão e a verificação de localização com quatro ou mais nós detectores, facilitando a rápida identificação de nós maliciosos com baixo consumo de energia. A estrutura hierárquica das redes em cluster traz benefícios em eficiência energética, escalabilidade e roteamento. Novas abordagens combinam RSSI e Informação de Estado do Canal (CSI) para proteger essas redes contra ataques Sybil, enquanto métodos leves propõem algoritmos para detectar nós Sybil disfarçados. Um mecanismo de comunicação segura foi desenvolvido para redes sem fio agrupadas, baseado em criptografia de curva elíptica (ECC). No entanto, essa abordagem depende de registros históricos, o que pode afetar sua estabilidade. Recentemente, um método para detectar ataques Sybil em redes hierárquicas centralizadas foi proposto, que identifica nós Sybil antes do cluster para otimizar recursos. Essa detecção analisa a força do sinal recebido de dois nós de alta energia. Outra proposta combina CSI com um algoritmo de classificação adaptativa para identificar ataques em nós dinâmicos e estáticos. Diversas metodologias foram sugeridas para detectar e isolar ataques Sybil, integrando um modelo de confiança distribuído a protocolos de roteamento. Um protocolo oportunista utiliza mensagens de beacon e RSSI para identificar localizações falsas de nós maliciosos e se defender de ataques como buracos cinzas. No entanto, essa abordagem é limitada se o atacante tiver maior capacidade de energia e potência de transmissão. Um framework que utiliza autenticação e RSSI foi criado para detectar ataques Sybil, onde os valores de RSSI são calculados a partir do ângulo de chegada e armazenados em cada nó. A otimização por colônia de formigas é aplicada para definir a rota mais eficiente para os pacotes. Propostas de criptografia, como o algoritmo Fujisaki Okamoto, também visam proteger contra ataques Sybil por meio de verificação baseada em ID. Por fim, um algoritmo chamado Teste Aproximado de Ponto em Triangulação (SF-APIT) foi desenvolvido para detectar ataques Sybil em redes sem fio de forma distribuída, utilizando métodos de refinamento iterativo onde a localização de um nó desconhecido é estimada através da triangulação, considerando o centróide da área sobreposta como sua posição aproximada [7].

4.1.3 Confiança

Há uma carência de estudos focados na detecção de ataques de segurança com base em critérios alternativos, como a perda e alteração de pacotes. Foi observado que a confiança em redes de IoT pode ser construída automaticamente, sem a necessidade de interação direta entre nós desconhecidos. Para garantir a segurança da rede, um centro de confiança utiliza uma chave compartilhada entre dois nós, o que permite a verificação e autenticação. Utilização de métodos de criptografia e gerenciamento de confiança que permitem detectar e prever o comportamento de um atacante Sybil. Essa confiança é essencial, especialmente na escolha do próximo salto durante o roteamento. A decisão sobre o próximo salto pode se basear tanto em critérios de confiança quanto de energia.

Um módulo de monitoramento calcula o consumo energético dos nós vizinhos e registra essas informações em uma tabela, além de estimar o gasto médio de energia necessário para o roteamento. Um método proposto para detectar ataques Sybil leva em consideração nome, localização e energia dos nós durante o roteamento de novas mensagens. Este método usa um sistema em vários níveis, onde agentes específicos aplicam regras para identificar atacantes Sybil. Esses atacantes podem manipular dados em diferentes estágios, comprometendo a integridade da rede, e também modificar timestamps com múltiplas identidades, causando problemas de sincronização nos relógios dos dispositivos IoT. Um outro método inovador para detectar nós Sybil com identidades falsas antes da formação de clusters em redes hierárquicas centralizadas, com o objetivo de otimizar os recursos onde essa detecção é feita através da análise da força do sinal dos nós vizinhos. Além disso, existem técnicas que ajudam a prever o consumo energético de maneira eficaz e aumentam a detecção de nós maliciosos. A confiabilidade dos marcos de roteamento é essencial, pois todos os protocolos dependem de mecanismos de localização. Métodos leves que combinam técnicas de localização e detecção de intrusões, usando um modelo de confiança, têm sido utilizados para combater uma variedade de ataques de segurança. Um método seguro de roteamento geográfico (GSR), derivado de abordagens anteriores, destaca-se por seu baixo consumo de recursos computacionais ao lidar com ataques como spoofing e Sybil, incorporando elementos de autenticação. Também foram desenvolvidas técnicas de monitoramento que otimizam o uso de energia, garantindo segurança, e que se mostraram eficazes na defesa contra ataques Sybil [7].

4.1.4 Inteligência Artificial

Inteligência artificial é exemplificada por sistemas de detecção de intrusões no campo da cibersegurança, que distinguem entre nós legítimos e maliciosos através de uma análise detalhada do tráfego. Os ciberataques foram inicialmente identificados com sistemas baseados em regras, capazes de reconhecer ataques por suas assinaturas desde os primórdios da Internet. A Inteligência de Enxame uma ramificação da inteligência artificial, se inspira no comportamento inteligente de enxames biológicos para resolver e simular problemas reais. Estes algoritmos buscam explorar conceitos de indivíduos simples que, por meio de colaboração, organização, troca de conhecimento e aprendizado, podem exibir comportamentos complexos de otimização em enxame. Há ainda o método denominado Autômatos Finitos Dinâmicos Determinísticos em Aprendizado para detecção de intrusões, garantindo a transmissão de dados de forma segura por caminhos otimizados. Por fim, em outro método de algoritmos de inteligência de enxame baseados em abelhas para criar um esquema de roteamento seguro. O mecanismo de roteamento proposto utiliza abelhas scout primárias e secundárias para realizar um roteamento otimizado e seguro. Isso melhora a eficiência dos dados em vários cenários, ao mesmo tempo em que proporciona segurança contra ataques de inundação, spoofing e Sybil. Contudo, suas desvantagens incluem a possibilidade de estagnar em um ótimo local quando a solução está próxima do ótimo global.

5 Conclusão

Conclui-se que, embora a Internet das Coisas (IoT) ofereça benefícios notáveis em termos de conectividade e automação, ela também introduz novas e significativas vulnerabilidades de segurança que precisam ser abordadas com urgência. O ataque Sybil é uma dessas ameaças, capaz de comprometer gravemente a integridade e o desempenho das redes IoT ao falsificar identidades de nós e realizar manipulações prejudiciais, como escuta clandestina, falsificação de dados e controle indevido do tráfego de informações.

A detecção e mitigação de ataques Sybil, apesar de desafiadoras, têm recebido atenção crescente da comunidade científica. Soluções baseadas em criptografia, como a utilização de chaves simétricas e assimétricas, desempenham um papel vital na autenticação de nós e na garantia da segurança das comunicações, embora enfrentem desafios de escalabilidade e consumo energético. O uso do indicador de sinal mais forte (RSSI) tem se mostrado eficaz na detecção de identidades falsas sem a necessidade de hardware especializado, enquanto técnicas de inteligência artificial, como algoritmos inspirados em enxames, oferecem potencial para melhorar a segurança e a otimização dos sistemas IoT de forma adaptativa.

No entanto, mesmo com essas soluções, há uma necessidade contínua de aprimorar os mecanismos de detecção e defesa, especialmente em redes IoT com estrutura distribuída e recursos limitados. Métodos leves de roteamento seguro, como o Geographical Secure Routing (GSR), que combinam baixa demanda computacional com autenticação robusta, são promissores, mas demandam mais investigações para garantir resiliência contra ataques complexos como o Sybil.

Portanto, a segurança das redes IoT exige uma abordagem multifacetada, que integre técnicas de criptografia, monitoramento contínuo, modelos de confiança distribuídos e avanços em inteligência artificial. Apenas com a aplicação coordenada dessas estratégias será possível mitigar adequadamente os riscos de ataques Sybil e garantir que a IoT possa continuar a crescer de forma segura, atendendo às demandas de eficiência e confiabilidade em diversos cenários, desde ambientes domésticos até industriais.

Referências

[1] Atanasova, Tatiana & Dineva, Kristina. (2019). SECURITY IN IOT SYSTEMS.0.5593/sgem2019/2.1/S07.075.

[2] Rytel, Marcin, Anna Felkner, and Marek Janiszewski. "Towards a safer internet of things—a survey of iot vulnerability data sources."Sensors 20.21 (2020): 5969.

[3] Hameed, Ali, and Alauddin Alomary. "Security issues in IoT: A survey."2019 International conference on innovation and intelligence for informatics, computing, and technologies (3ICT). IEEE, 2019.

[4] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim and S. R. Chaudhry, "IoT architecture challenges and issues: Lack of standardization,"2016 Future Technologies Conference (FTC), San Francisco, CA, USA, 2016, pp. 731-738, doi: 10.1109/FTC.2016.7821686.

[5] Anand, Pooja, et al. "IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges."IEEE Access 8 (2020): 168825-168853.

[6] Levine, Brian Neil, Clay Shields, and N. Boris Margolin. "A survey of solutions to the sybil attack."University of Massachusetts Amherst, Amherst, MA 7 (2006): 224.

[7] 7. Arshad, Akashah, et al. "A survey of Sybil attack countermeasures in IoT-based wireless sensor networks."PeerJ Computer Science 7 (2021): e673.

Item	Problemas	Detalhe
1	Padrões Interoperabilidade	Há uma grande variedade de dispositivos, o que torna a adesão a padrões desafiadora. Além disso, alguns fabricantes não demonstram preocupação com a segurança.
2	Informações e portas abertas	Não há encriptação na transmissão de dados
3	Ausência de medidas básicas de segurança ou privacidade.	Não há suporte para a autenticação ou autorização de dispositivos.
4	Apoio a Atualizações de Firmware e SO	Atualizar o firmware de dispositivos já incorporados continua sendo um desafio, e é crucial que essas atualizações venham exclusivamente de fontes confiáveis.
5	Desafios de Armazenamento	Devido ao tamanho reduzido dos dispositivos, o espaço disponível é limitado; isso gera problemas na gestão e na continuidade dos dados.
6	Credenciais pré-definidas e vulneráveis	Codificadas de maneiras frágeis e fácil de serem quebradas
7	Furto e adulteração	Proteger o acesso físico a dispositivos remotos é um desafio.
8	Interfaces web vulneráveis	A maioria dos dispositivos vêm com uma interface web embutida.
9	Questões de estouro de buffer	Existem riscos de estouro de buffer ou de ataques de injeção de outros tipos.
10	Desafios no desenvolvimento	Encontrar especialistas com competências adequadas para a Internet das Coisas é uma tarefa complicada.
11	Apoio do fabricante	A qualidade de um dispositivo depende do reconhecimento do fornecedor e do suporte que ele proporciona.
12	Questões Regulatórias e de Direitos	Trata-se de um problema relacionado ao que pode ocorrer devido à conexão entre dispositivos IoT. Caso um incidente aconteça, pode não existir uma legislação específica para abordá-lo corretamente.

Tabela 1: Problemas de segurança relacionados a IoT.