Autenticação de dispositivos de Internet das Coisas baseada nas características do sinal eletromagnético

Marcos Felipe B. de Abreu[1], **Pabllo F. A. Sousa**[1],
Vinicius da C. M. Borges[1], **Antonio C. de O. Júnior**[1], **Kleber V. Cardoso**[1]

[1]Instituto de Informática – Universidade Federal de Goiás (UFG)
Alameda Palmeiras, Quadra D, Câmpus Samambaia CEP 74690-900 - Goiânia - GO – Brazil

{marcos,pabllosousa,vinicius,antonio,kleber}@inf.ufg.br

Abstract. *Accessing unauthorized devices on a network is an security issue on Internet of Things. The unique identifiers of the devices used to authenticate them can be easily cloned, thus requiring another form of authentication. By monitoring the electromagnetic spectrum by means of a software defined radio it is possible to capture data transmitted by various wireless communication devices. These data allow us to extract unique characteristics of a device, since an electric circuit that generates the electromagnetic signal does not behave perfectly like another. These characteristics can then be used to create a unique signature, thus enabling device differentiation. There are several IoT technologies on the market and it is expected that the implementation of an authentication technique will be technology independent. For the validation of the technique are collected signals of nRF24L01+ technology devices, extracting characteristics of the magnitude of the signal. These characteristics are used in a classifier, which gives an accuracy of 94.7% in device differentiation.*

Resumo. *O acesso de dispositivos não autorizados em uma rede é um problema de segurança em Internet das Coisas. Os identificadores únicos dos dispositivos usados para autenticação dos mesmos podem ser facilmente clonados, sendo assim necessário outra forma de autenticação. Monitorando o espectro eletromagnético através de um rádio definido por software é possível capturar dados transmitidos por diversos dispositivos de comunicação sem fio. Esses dados nos permite extrair características únicas de um dispositivo, visto que, um circuito elétrico que gera o sinal eletromagnético não se comporta perfeitamente igual a outro. Essas características podem então ser usadas na criação de uma assinatura única, possibilitando assim a diferenciação de dispositivos. Há várias tecnologias IoT no mercado e espera-se que a implementação de uma técnica de autenticação seja independente de tecnologia. Para validação da técnica são coletados sinais de dispositivos da tecnologia nRF24L01+, extraindo características da magnitude do sinal. Essas características são usadas em um classificador, ao qual é obtida uma acurácia de 94,7% na diferenciação de dispositivos.*

1. Introdução

Internet das Coisas, do inglês *Internet of Things* (IoT), é um paradigma que está ganhando espaço na área de comunicações sem fio modernas devido ao seu grande impacto na vida da população. A quantidade de dispositivos conectados é enorme, com cerca de 9 bilhões de coisas conectadas à internet em 2013 e previsão de mais de 24 bilhões de coisas estejam conectadas até 2020 [J. Gubbi 2013]. E-saúde, assistentes pessoais, vida assistida são exemplos de aplicações presentes em um ambiente doméstico, enquanto no contexto corporativo temos, como exemplos, automação, logística, gerenciamento de negócios/pessoas e transporte inteligente [Gomez and Paradells 2010]

Padrões e especificações de segurança começam a ser pensados, a exemplo do Brasil com o Plano Nacional de Internet das Coisas [BNDES 2017] e nos Estados Unidos, onde foi elaborado um documento listando riscos e oferecendo sugestões para aplicação de segurança na Internet das Coisas [of Homeland Security 2016]. Observa-se, entretanto, um cenário diferente, dispositivos tem apresentado falhas graves que comprometem a segurança dos mesmos [Zhao and Ge 2013]. Um ataque bastante conhecido em redes de computadores, que se repete em IoT, é o roubo de identidade [Nawir et al. 2016]. Como a maior parte não provém mecanismos de segurança a implementação desses não ultrapassam o nível de enlace, a autenticação de dispositivos sem fio por padrão são baseados em identificadores únicos, como o endereço MAC (*Media Access Control*) no Bluetooth e no Wi-Fi. Entretanto, esses dispositivos podem ser forjados por alguém mal intencionado para se passar pelo dispositivo original, abrindo assim portas para execução de outros ataques.

Tradicionalmente o problema de autenticação é resolvido usando criptografia, mas isso se torna inviável quando falamos de IoT devido as características dos dispositivos, que contam com um baixo poder computacional. Os autores em [Xu et al. 2014] mostram que tratar ao nível de hardware é uma solução, mas demoraria para entrar no mercado incluir esse tipo de tecnologia em dispositivos que possuem como ideal serem baratos. Uma das soluções é trazer a responsabilidade de autenticação desses dispositivos para um terceiro que possui mais poder computacional.

Dispositivos sem fio podem ser diferenciados com base em sua assinatura eletromagnética [Danev et al. 2012]. A diferenciação de placas é possível, pois, são geradas imperfeições, não propositais, no processo de fabricação dos módulos geradores de sinais dos dispositivos. Essas imperfeições influenciam na geração do sinal a ser transmitido. Com base nisso é possível analisar o sinal transmitido por um dispositivo e criar uma assinatura para o mesmo.

A ideia de um *gateway* que conecte vários dispositivos IoT e ofereça, através de uma solução centralizada, segurança e processamento vem ganhando espaço em IoT [Zhu et al. 2010]. A proposta é analisar e identificar dispositivos IoT, sendo que para isso é necessário utilizar um SDR (*Software Defined Radio*). O SDR é um dispositivo capaz de capturar e analisar sinais independente da tecnologia usada pelas coisas, além de permitir implementar a solução no *gateway*, evitando aumento de latência na rede. Isso se torna viável, pois, a proposta é que a solução execute em um *gateway* que se comunique com múltiplas tecnologias de redes sem fio, e.g., SOFTWAY4IoT [LABORA 2017].

O objetivo do trabalho é investigar a viabilidade de autenticar dispositivos de IoT

com base no sinal eletromagnético das suas interfaces sem fio. É importante que a solução possa ser integrada a um *gateway* de comunicação IoT. O trabalho é dividido em duas etapas. Na primeira etapa, é apresentada uma prova de conceito da técnica de análise dos sinais eletromagnéticos que permite diferenciar dispositivos com base em um conjunto de características peculiares (*features*). Na segunda etapa, é feita uma análise sobre a aplicação da técnica avaliada a um *gateway* de comunicação IoT.

Esse trabalho está organizado conforme segue: Na Seção 2, são apresentados os trabalhos relacionados. Na seção 3, é detalhada a metodologia aplicada no trabalho. Na seção 4, são apresentados os experimentos e os resultados obtidos e, na seção 5, é discutida a implementação da técnica em um *gateway* IoT. A seção 6 apresenta a conclusão e os trabalhos futuros.

2. Trabalhos Relacionados

Identificar dispositivos com base nas suas características eletromagnéticas não é um tema novo. Na Segunda Guerra Mundial controladores de voo analisavam visualmente ondas emitidas por radares para identificar possíveis transmissões que não vinham de seus dispositivos. Os primeiros trabalhos na área de computação, que automatizaram esse processo se deu em 1995 com os trabalhos de [Toonstra and Kinsner 1995] e [Choe et al. 1995].

[Danev et al. 2012] faz um resumo da área de identificação de dispositivos sem fio e traz algumas métricas usadas para medir a viabilidade e a eficácia de novos métodos. A performance de um método é medida de acordo com a velocidade, acurácia, custo e segurança. A métrica velocidade é utilizada para medir o tempo gasto para o sistema tomar alguma decisão, por exemplo bloquear um dispositivo na rede. Essa métrica é de extrema importância, se o trabalho é executado de uma forma reativa, ou seja, autoriza-se qualquer dispositivo na rede enquanto a análise do sinal é feita, um dispositivo mal intencionado pode nesse meio tempo já ter obtido algum sucesso em seu ataque e ou exploração. Por outro lado, se o trabalho é executado de uma forma ativa, ou seja, o dispositivo é autorizado somente após a análise do seu sinal, é introduzido um atraso de transmissão na rede e torna-se necessária a implementação de politicas de cache. A segunda métrica, acurácia, trata da porcentagem de erros em uma técnica. Quer se minimizar duas taxas de erro, a FAR (*False Accept Rate*), que é quando há a autorização de um dispositivo impostor, e a FRR (*False Reject Rate*), que é a probabilidade de não autorizar um dispositivo genuíno. A métrica custo está relacionada ao hardware necessário para fazer a análise e o processamento desse sinal. Para se obter o sinal eletromagnético em um dispositivo é necessário que o hardware ofereça essa função.

A escolha das características é uma parte extremamente importante no trabalho, visto que essa terá total impacto na diferenciação dos dispositivos. A escolha está relacionada às imperfeições geradas na fabricação de cada placa. [Danev and Capkun 2009] trabalha com características coletadas do início da transmissão do sinal pelo dispositivo, essas chamadas na literatura de *transient features*. Baseia-se em parâmetros como distância, polarização da antena e voltagem, posteriormente verificam como esses parâmetros influenciam na acurácia da coleta e por fim verificam a viabilidade de certos ataques de personificação de dispositivo.

Várias tecnologias de redes sem fio já foram exploradas. Os trabalhos [Hall et al. 2005] e [Barbeau et al. 2006] diferenciam dispositivos Bluetooth usando

como características Amplitude, Frequência e Fase, coletadas do inicio da transmissão do sinal. [Bihl et al. 2016] aplica algoritmos de seleção de características para identificação de dispositivos Zigbee. Nenhum desses trabalhos considera múltiplas tecnologias, ou ainda, extração de características independentes de tecnologia, capazes de diferenciar dispositivos diversos, sejam eles pertencentes a qualquer padrão.

Há na literatura outras formas de abordar o problema de identificação de dispositivos com base no comportamento da transmissão. [Meidan et al. 2017] classifica dispositivos analisando pacotes TCP recebidos. [Bezawada et al. 2018] trabalha no problema de identificação de dispositivos IoT usando cabeçalho e carga útil dos pacotes TCP/IP. A desvantagem dessa abordagem é o tempo que leva para coletar, analisar e tomar uma decisão.

Outra abordagem, [Verma et al. 2015] propõe autenticar dispositivos com base em uma `tag`, sinal de baixa potência que o transmissor adiciona em sua transmissão. Uma prova de conceito é feita usando um par de SDRs, sendo demonstrada a viabilidade e a segurança oferecidas pela técnica. Entretanto para a aplicação do método é necessário que ambos dispositivos, transmissor e receptor ofereçam suporte, o que torna os dispositivos de Internet das Coisas atuais incompatíveis.

3. Metodologia

Nessa seção, é detalhada a metodologia usada neste artigo. A Figura 1 mostra o fluxo do experimentos, o qual é apresentado em detalhes a seguir.

Figura 1. Fluxo dos experimentos.

Transmissão

A Figura 2 apresenta o ambiente experimental utilizado para transmissão e captura do sinal.

Coleta do sinal

O equipamento utilizado para a captura do sinal é o SDR. Composto de todos os componentes de um rádio comum, o SDR possuiu o que é chamado de *RF Front End* programável. O *RF Front end* de um rádio é composto por filtros, amplificadores, oscilador local e mixer. Esses componentes podem ser acessados via softwares de configuração fornecidos pelas fabricantes, ou até de ferramentas de processamento de sinal como GNU-Radio [Blossom 2004]. Os componentes podem ser programados utilizando a linguagem C/C++, ou em alguns casos em Python. O SDR possui duas antenas, podendo ser configuradas para trabalharem ambas em modo de recepção ou, uma em modo de recepção e outra em modo de transmissão.

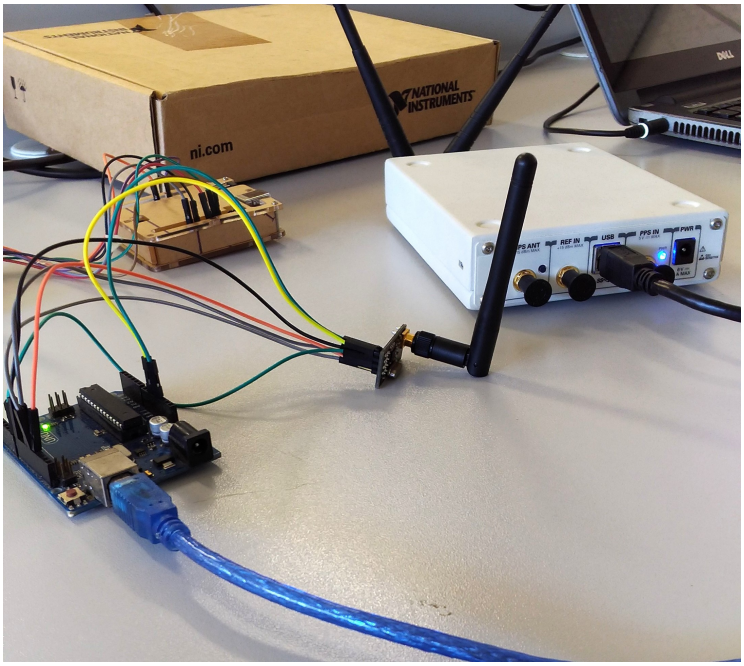


Figura 2. SDR e dispositivo de IoT.

Processamento do sinal

A ferramenta utilizada para realizar a análise e extração das características do sinal recebido é chamada GNURadio. GNURadio é um *toolkit* para implementação em SDR, que traz blocos como ferramentas de processamento de sinal. Esses blocos podem exercer as mais variadas funções, como filtros, moduladores, conversores de domínio do sinal, etc. Os blocos podem conter *buffers* de entrada, *buffers* de saída ou ambos, e são denominados *source blocks*, *sink blocks* e *general blocks* respectivamente.

Na Figura 3, é apresentado o conjunto de blocos usados no GNURadio para realizar o processamento do sinal eletromagnético e a extração das características peculiares. Para identificar um determinado dispositivo, é preciso primeiramente armazenar os dados capturados em um *buffer*, enviar essas amostras para um demodulador específico da tecnologia, identificar o preâmbulo do pacote transmitido pelo dispositivo, se há a existência de um preâmbulo, as amostras anteriormente guardadas no *buffer* são armazenadas em um arquivo.

Ao iniciar a captura, armazena-se os valores no *buffer* de entrada do bloco *Stream to vector*, que faz a decimação do sinal. Então esse bloco envia o sinal decimado para um outro bloco chamado FFT (*Fast Fourier Transform*) que converte os dados do domínio do tempo para o domínio da frequência. O *buffer* de saída do bloco FFT entrega um vetor de números complexos, a partir do qual é possível obter a magnitude do sinal (distância entre o símbolo e a origem) em cada frequência, onde cada valor do vetor é aplicado à seguinte expressão:

$$|X[k]| = \sqrt{{X_{re}}^2 + {X_{im}}^2}, \tag{1}$$

onde X_{re} representa a parte real do sinal e X_{im} representa a parte imaginária. A fase de

cada componente do sinal é obtida através da aplicação de cada valor do vetor na seguinte expressão:

$$\angle X[k] = tan^{-1}\left(\frac{X_{im}}{X_{re}}\right). \quad (2)$$

Outra característica extraída é o EVM (*Error Vector Magnitude*), baseada nos erros relacionados à modulação. O EVM é a diferença entre o valor da magnitude em cada amostra do sinal capturado e o valor da magnitude ideal para aquela modulação. Colhidas as características necessárias, essas agora são armazenadas.

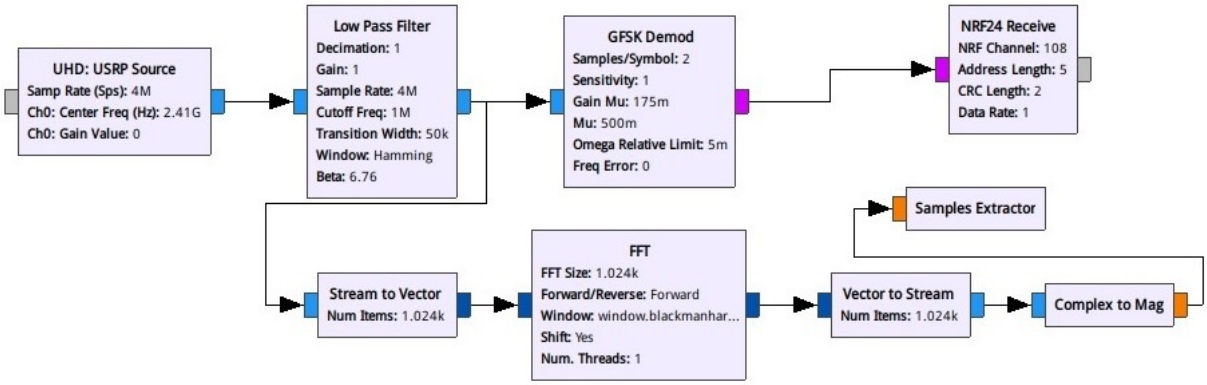


Figura 3. Blocos do GNURadio usados no processamento do sinal e extração das características.

Treinamento

Obtidas as características do transmissor é iniciada a classificação. Nessa fase é aplicado um classificador nas amostras. O problema se encaixa na categoria de aprendizado não supervisionado pois conhecemos as características dos dispositivos cadastrados mas não as dos intrusos. Dentre os algoritmos da categoria o que mais obteve desempenho em outros trabalhos [Brik et al. 2008], ou seja, menor taxa de erros, é o SVM (*Support Vector Machine*). O SVM é usado para detecção de anomalias, ou seja, dado um conjunto de amostras, ele detectará o limite flexível desse conjunto de modo a classificar novos pontos como pertencentes a esse conjunto ou não. Como resultado obtivemos um grau de similaridade entre o sinal que estamos analisando e o conjunto de sinais já cadastrados.

Avaliação

A avaliação consiste em comparar as amostras coletadas de um dispositivo com ele mesmo e com amostras de outros dispositivos, esses que seriam os possíveis intrusos. Quer se minimizar duas taxas de erro, a FAR (*False Accept Rate*), que é quando há a autorização de um dispositivo impostor, e a FRR (*False Reject Rate*), que é a probabilidade de não autorizar um dispositivo genuíno.

4. Experimentos

A captura do sinal é feita usando um SDR ettus b200, que possui cobertura de sinal entre as frequências de 70 MHz a 6 GHz, operação full-duplex com largura de banda em

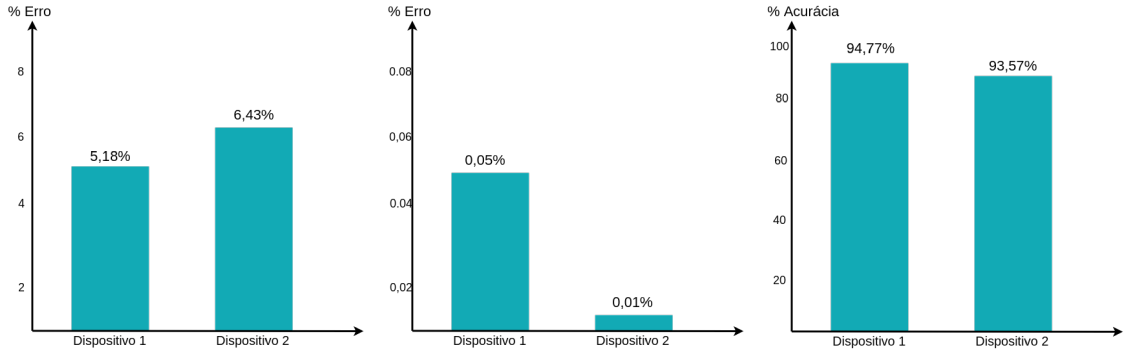
tempo real de 56 MHz, conectividade rápida e conveniente alimentada por barramento SuperSpeed USB 3.0. São usados 2 dispositivos da tecnologia nrf24L01+ transmitindo em intervalos pré-definidos em um mesmo canal de comunicação. Antes de realizar a captura do sinal é necessário definir a frequência e a taxa de amostragem em que o SDR vai trabalhar. Isso é feito na interface gráfica da ferramenta GNURadio. Para determinar que uma amostra é válida, primeiro ela é bufferizada, demodulada e decodificada. Assim que um quadro da tecnologia é identificado nessa amostra, os dados que estão no *buffer* são passados para o extrator de características. Foram coletadas 2000 amostras da transmissão de cada um dos dispositivos em diferentes posições no cenário. A mudança de local é realizada para ver a variação que há entre as magnitudes de um mesmo dispositivo, visto que essa característica é fortemente influenciada pela amplitude do sinal. Cada amostra é um conjunto de 1024 características que representam a magnitude do sinal.

4.1. Seleção de melhores características e análise dos dados

A seleção de características relevantes é uma fase importante para obtenção de melhores resultados na classificação. Para isso usa-se algoritmos que analisam os dados e apontam quais as características mais relevantes para a classificação. O algoritmo utilizado no conjunto de dados foi o *Principal Component Analysis* (PCA) [Jolliffe 2011].

4.2. Avaliação da solução

Nos experimentos, são realizados dois testes. Dos dois dipositivos, um é usado como referência e o outro faz o papel de um intruso que tenta se comunicar com o *gateway*. Um pequeno número de amostras é necessário para a fase de treinamento e de acordo com [Brik et al. 2008] a quantidade ideal é de 20 amostras. O conjunto de dados, com 2000 amostras de cada dispositivo, é dividido em 20 partes cada um contendo 100 amostras. São usadas 20 amostras para treinamento e as 80 restantes para teste. Cada parte é comparada com as 2000 amostras do dispositivo intruso.



(a) FAR (*False Accept Rate*) (b) FRR (*False Reject Rate*) (c) Acurácia

Figura 4. Erros e acurácia obtidas dos experimentos

Como visto na figura 4(c) foi obtida uma acurácia máxima de 94,77%. Usando o dipositivo 1 como referência é obtida uma taxa de erro FAR e FRR de 5,18% e 0,05%, respectivamente. Treinando o classificador com o dispositivo de referência 2 o erro FAR foi de 6,43% e o erro FRR foi de 0,01%.f As taxas de erro são inversamente proporcionais devido à característica do classificador. O SVM ajusta um limiar de variação das

características. Se esse limiar é alto, a taxa de falsos positivos (erro FRR) pode aumentar e consequentemente a taxa de verdadeiros negativos (erro FAR) diminuir. Tendo em vista essa característica, devemos então escolher um limiar para o classificador de acordo com o erro que se deseja minimizar.

5. Aplicação da técnica em um *gateway* IoT

O processo de autenticação em um *gateway* IoT é dividido em duas etapas. A primeira etapa é a de cadastro de uma novo dispositivo que precisa se comunicar com o *gateway*. Para isso, é necessário criar uma assinatura desse dispositivo que consiste basicamente em: 1) capturar o sinal eletromagnético emitido pelo dispositivo por um determinado período de tempo, 2) criar sua assinatura com base nas características do sinal e 3) associar essa assinatura com o identificador do dispositivo. A segunda etapa é divida em cinco passos, os quais estão ilustrados na Figura 5 e que são detalhados a seguir. Esses passos são baseados na metodologia descrita na Seção 3.

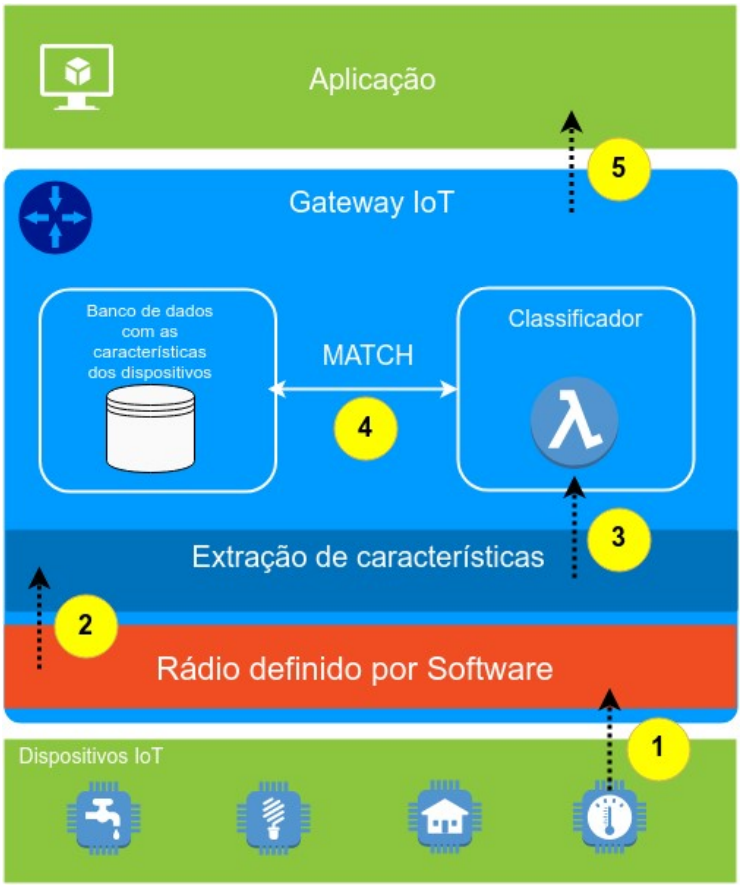


Figura 5. Autenticação no *gateway*, dispositivo já cadastrado

O primeiro passo é a transmissão do dispositivo IoT. A vantagem da técnica apresentada no trabalho é que não é necessária nenhuma alteração nos dispositivos para o processo de autenticação. Enquanto o sinal está sendo processado pelo gateway para gerar a pilha TCP-IP um clone é enviado para o processo de identificação.

O segundo passo é o processamento do sinal. Como exposto anteriormente, o Rádio Definido por software nos dá a possibilidade de capturar e processar o sinal de

dispositivos em sua faixa de transmissão. A variedade de dispositivos depende do suporte do rádio às tecnologias.

Com o sinal já capturado pelo SDR, o terceiro passo é a extração das características que serão usadas na classificação. Como descrito anteriormente as características são obtidas a partir da aplicação da transformada de Fourier nos dados capturados. A partir disso é obtido o vetor de magnitude do sinal.

No quarto passo, as características extraídas da fase anterior são comparadas com a assinatura do dispositivo previamente cadastrado. O banco de dados de características pode ser atualizado conforme o tempo para se obter melhor acurácia na classificação. Diversos fatores, como a interferência, podem influenciar no resultado.

A última fase é a tomada de decisão pela aplicação. Ao se identificar um dispositivo intruso duas políticas podem ser aplicadas. Em uma política menos rígida um alerta pode ser gerado para o administrador do *gateway* cabendo a ele tomar a decisão. Aplicando uma política mais rígida, a comunicação do dispositivo com o *gateway* é interrompida e é gerado um alerta para administrador. Dispositivos intrusos estão na área de cobertura do *gateway*, sendo que a distância máxima depende da tecnologia de transmissão sem fio.

6. Conclusões e trabalhos futuros

Neste trabalho, foi apresentada uma técnica baseada no uso da magnitude do sinal como característica única para criação de assinaturas de dispositivos. A técnica apresentou resultados satisfatórios e se mostra viável na autenticação de dispositivos quando não há alteração de sua localização ao criar a sua assinatura. Vimos que a amplitude do sinal é um ponto importante quando utilizada somente a magnitude como característica para diferenciação dos dispositivos. Além disso, a técnica é simples e de baixo custo. Apresentamos também uma análise sobre a integração da técnica a um *gateway* de comunicação IoT.

Embora não tenha sido avaliado, a técnica apresentada é capaz de distinguir assinaturas de diferentes tecnologias de comunicações. Avaliar essa propriedade e sua acurácia são alguns trabalhos futuros planejados. Também pretendemos avaliar a técnica de maneira mais ampla, considerando diversos cenários que podem influenciar no processo de identificação, por exemplo, interferência com outros dispositivos, obstáculos que impactam na característica do sinal e incluir um número maior de características capazes de influenciar na diferenciação dos dispositivos como, largura de banda e frequência do pico de amplitude.

Referências

Barbeau, M., Hall, J., and Kranakis, E. (2006). Detection of rogue devices in bluetooth networks using radio frequency fingerprinting. In *proceedings of the 3rd IASTED International Conference on Communications and Computer Networks, CCN*, pages 4–6. Citeseer.

Bezawada, B., Bachani, M., Peterson, J., Shirazi, H., Ray, I., and Ray, I. (2018). IoTSense: Behavioral Fingerprinting of IoT Devices. *arXiv preprint arXiv:1804.03852*.

Bihl, T. J., Bauer, K. W., and Temple, M. A. (2016). Feature Selection for RF Fingerprinting With Multiple Discriminant Analysis and Using ZigBee Device Emissions. *IEEE Transactions on Information Forensics and Security*, 11(8):1862–1874.

Blossom, E. (2004). Gnu radio: tools for exploring the radio frequency spectrum. *Linux journal*, 2004(122):4.

BNDES (2017). Produto 8: Relatório do plano de ação. Technical report, Banco Nacional do Desenvolvimento Social (BNDES).

Brik, V., Banerjee, S., Gruteser, M., and Oh, S. (2008). Wireless device identification with radiometric signatures. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pages 116–127. ACM.

Choe, H. C., Poole, C. E., Andrea, M. Y., and Szu, H. H. (1995). Novel identification of intercepted signals from unknown radio transmitters. In *Wavelet Applications II*, volume 2491, pages 504–518. International Society for Optics and Photonics.

Danev, B. and Capkun, S. (2009). Transient-based identification of wireless sensor nodes. In *Proceedings of the 2009 International Conference on Information Processing in Sensor Networks*, pages 25–36. IEEE Computer Society.

Danev, B., Zanetti, D., and Capkun, S. (2012). On physical-layer identification of wireless devices. *ACM Computing Surveys (CSUR)*, 45(1):6.

Gomez, C. and Paradells, J. (2010). Wireless home automation networks: A survey of architectures and technologies. volume 48, pages 92–101. IEEE.

Hall, J., Barbeau, M., and Kranakis, E. (2005). Radio frequency fingerprinting for intrusion detection in wireless networks. *IEEE Transactions on Defendable and Secure Computing*, 12:1–35.

J. Gubbi, R. Buyya, S. M. M. P. (2013). Internet of things (iot): A vision, architectural elements, and future directions in future generation computer systems. volume 29, pages 1645–1660.

Jolliffe, I. (2011). Principal component analysis. In *International encyclopedia of statistical science*, pages 1094–1096. Springer.

LABORA, T. (2017). SOFTware-defined gateWAY and fog computing for IoT.

Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J. D., Ochoa, M., Tippenhauer, N. O., and Elovici, Y. (2017). Profiliot: a machine learning approach for iot device identification based on network traffic analysis. In *Proceedings of the Symposium on Applied Computing*, pages 506–509. ACM.

Nawir, M., Amir, A., Yaakob, N., and Lynn, O. B. (2016). Internet of things (iot): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)*, pages 321–326.

of Homeland Security, U. D. (2016). Strategic principles for securing the internet of things (iot). pages 1–17.

Toonstra, J. and Kinsner, W. (1995). Transient analysis and genetic algorithms for classification. In *WESCANEX 95. Communications, Power, and Computing. Conference Proceedings., IEEE*, volume 2, pages 432–437. IEEE.

Verma, G., Yu, P., and Sadler, B. M. (2015). Physical layer authentication via fingerprint embedding using software-defined radios. *IEEE Access*, 3:81–88.

Xu, T., Wendt, J. B., and Potkonjak, M. (2014). Security of iot systems: Design challenges and opportunities.

Zhao, K. and Ge, L. (2013). A survey on the internet of things security. In *Computational Intelligence and Security (CIS), 2013 9th International Conference on*, pages 663–667. IEEE.

Zhu, Q., Wang, R., Chen, Q., Liu, Y., and Qin, W. (2010). Iot gateway: Bridgingwireless sensor networks into internet of things. In *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, pages 347–352. Ieee.