Uma Infraestrutura Ágil e Efetiva de Virtualização de Funções de Rede para a Internet das Coisas

Diogo M. F. Mattos[1], **Pedro B. Velloso**[2] **e Otto Carlos M. B. Duarte**[2]

[1]Mídiacom - Departamento de Engenharia de Telecomunicações
Universidade Federal Fluminense (UFF)
[2]Grupo de Teleinformática e Automação
Universidade Federal do Rio de Janeiro (UFRJ)

Resumo. *As restrições computacionais e de consumo de energia de objetos conectados à Internet das Coisas não os permitem oferecer serviços de redes mais complexos do que o simples envio de dados. Em cidades inteligentes, a impossibilidade de prover serviços de segurança e qualidade de serviço pode resultar, até mesmo, em desastres nos centros urbanos. Este artigo propõe a integração vertical de um serviço complexo de rede em uma nuvem através de uma infraestrutura de virtualização de funções de rede, ágil e efetiva, que provê domínios isolados de objetos conectados. A proposta desenvolve um nó de acesso que virtualiza os domínios em que os objetos se conectam à infraestrutura. Um protótipo de serviços de segurança e de qualidade de serviço foi implementado. A avaliação mostra que a virtualização não impacta no desempenho das funções virtuais de rede. A proposta provê segurança aos objetos, identificando tráfego malicioso com acurácia de 99,8%, evitando a negação de serviços essenciais, e garante a qualidade de serviço.*

Abstract. *Devices of Internet of Things suffer from severe processing and power constraints, which hinders offering complex network services, other than simple data transmission. In smart city scenarios, the lack of these services, such as security and quality of service, might lead to low performance that can result in disasters in urban centers. In this paper, we propose an agile and effective network function virtualization infrastructure of isolated domains of connected devices, which outsources network tasks from the devices to the networking cloud. The domain isolation is achieved by virtualizing the gateway access node to which IoT devices connect. We have deployed a prototype to provide security and quality of service to IoT applications. Preliminary results show that the gateway virtualization does not impact the performance of virtual network functions. Additionally, our proposal provides security for connected devices, identifying the mallicious traffic with 99.8% accuracy, avoiding denial of essential services, and ensuring quality of service.*

1. Introdução

Em um mundo cada vez mais interconectado, estima-se que atualmente 54% da população viva em cidades e que esse número alcance 66% em 2050 [United Nations, 2014]. Para responder a desafios decorrentes do crescimento acelerado

Este trabalho foi realizado com recursos do CNPq, CAPES, FAPERJ e FAPESP (2015/24514-9, 2015/24485-9 e 2014/50937-1).

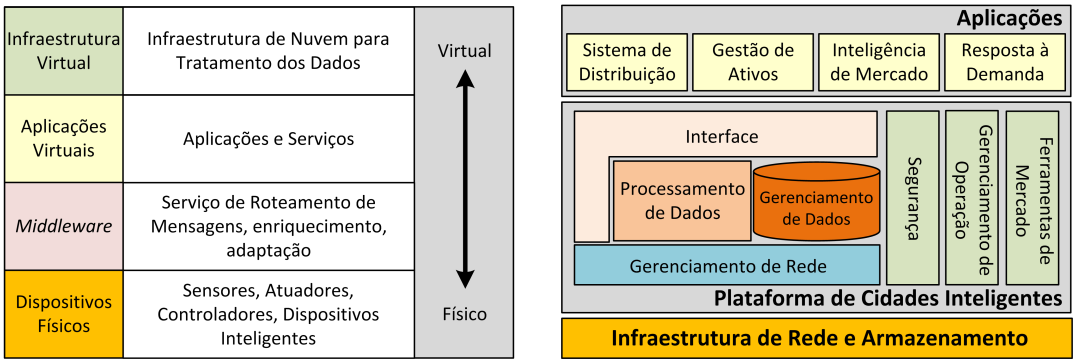
das cidades e alavancar as oportunidades geradas pela urbanização contínua, as políticas governamentais devem convergir esforços para focar na sustentabilidade das áreas urbanas. Uma alternativa para garantir a sustentabilidade é implantar e expandir os serviços públicos inteligentes, a distribuição de energia e água inteligentes, os serviços de saúde inteligentes e a governança das cidades baseada em plataformas de coleta de dados e tomada de decisões [Petrolo et al., 2017, Santana et al., 2017].

O desenvolvimento de plataformas para cidades inteligentes está associado ao sensoriamento, monitoramento e atuação sobre diversos objetos conectados no contexto urbano [Zhang et al., 2017] que, por sua vez, são uma aplicação do conceito de Internet das Coisas (*Internet of Things* - IoT) [Petrolo et al., 2017]. No entanto, a conexão dos objetos depende de dispositivos de comunicação que estão sujeitos a severas restrições de processamento e consumo de energia. Tais restrições impossibilitam o provimento de serviços de redes mais complexos como segurança e qualidade de serviço, sem os quais, grande parte das aplicações de cidades inteligentes têm o desempenho prejudicado ou até mesmo inviabilizado. Portanto, o objetivo principal deste trabalho é prover serviços complexos de redes para aplicações de IoT, através da terceirização das funções de redes para uma infraestrutura virtualizada na nuvem.

Este artigo propõe reduzir a carga do processamento dos objetos conectados através uma infraestrutura de virtualização de funções de rede para Internet das Coisas. A ideia principal é que cada domínio de IoT seja uma fatia vertical da rede de transporte que comporta desde o nó de acesso até a interface com o consumidor dos dados. Para tanto, a proposta desenvolve um nó de acesso sem-fio, chamado de *gateway*, que multiplexa o acesso à rede através de criação de pontos de acesso virtuais e conecta os objetos da rede sem-fio a uma infraestrutura de virtualização de funções de rede (*Network Function Virtualization Infrastructure* - NFVI). Na NFVI, são executadas funções virtuais de rede (*Virtual Network Function* - VNF) que assumem o processamento dos pacotes ao invés de deixá-lo para os objetos conectados ou para o *gateway*.

Trabalhos anteriores focam em plataformas de coleta e tratamento de dados [Petrolo et al., 2017, Zhang et al., 2017, Santana et al., 2017] ou em modelos teóricos de como gerenciar as redes de IoT [Qin et al., 2014, Bizanis e Kuipers, 2016, Ojo et al., 2016]. A proposta deste artigo é a virtualização do nó de acesso dos domínios de IoT combinado com uma infraestrutura de virtualização de funções de rede ágil e efetiva na implantação das funções. A infraestrutura de virtualização é capaz de assumir funções de tratamento de pacotes, antes desempenhadas por objetos conectados, e, assim, realiza a classificação de tráfego e a reação a ataques implementadas como funções virtuais. Um protótipo da proposta foi implementado e a sua avaliação mostra que o atraso na comunicação entre o nó de acesso e a infraestrutura não é significativo e que a virtualização do ponto de acesso não impacta no desempenho das funções virtuais de rede. Os resultados mostram ainda que a VNF de classificação identifica o tráfego malicioso em um domínio IoT com acurácia de 99,8% e, também, outra VNF provê qualidade de serviço para os objetos conectados e evita a negação de serviços essenciais.

O restante do artigo está organizado da seguinte forma. O serviço de rede para a Internet das Coisas é detalhado na Seção 2. Na Seção 3, propõe-se a infraestrutura de virtualização de funções para Internet das Coisas. A avaliação da proposta discutida na Seção 4. A Seção 5 discute os trabalhos relacionados. A Seção 6 conclui o artigo.



(a) Esquema de uma plataforma para Internet das Coisas.

(b) Arquitetura de uma plataforma para cidades inteligentes.

Figura 1. Arquitetura de referência para implantação de cidades inteligentes. (a) Esquema do relacionamento entre dispositivos físicos e aplicações virtuais para prover serviços de Internet das Coisas. (b) Arquitetura de exemplo de cidade inteligente, em que a comunicação entre sensores e aplicações é intermediada interfaces de acesso à rede, processamento e armazenamento. A plataforma de cidades inteligentes age como um *middleware*.

2. O Serviço de Rede para Internet das Coisas

A arquitetura de referência para Internet das Coisas, Figura 1(a) evidencia a transição entre os dispositivos físicos e as abstrações em *software* para aplicações de IoT. Nesse sentido, o desenvolvimento de sensores, etiquetas de identificação e tecnologias de comunicação entre sensores são agrupadas na categoria de comunicação entre objetos. A interação entre as aplicações e os objetos no mundo real são intermediadas por um *middleware*, um *software* de adaptação de requisições para cada tipo de objeto [Santana et al., 2017]. A ideia básica do *middleware* é abstrair os objetos em microsserviços e prover serviços mais complexos através da composição dos microsserviços simples. As aplicações, por sua vez, usam os serviços providos e gerenciados pelo *middleware* para sensoriar dados ou atuar em diferentes contextos. Contudo, nessa visão, oculta-se as especificidades do serviço de rede necessárias para cada tipo de aplicação. Assim, aplicações em tempo real, como as industriais [Wang et al., 2016], usam o mesmo serviço da rede de transporte que aplicações com requisitos menos estritos de latência, mas sensíveis à privacidade dos dados.

Considerando as redes de acesso, é possível definir redes de curto, médio e longo alcance para atender os objetos conectados. Entre os meios de acesso de curto alcance destacam-se as tecnologias baseadas em Bluetooth Low Energy (BLE) e Zigbee que apresentam como principais características o uso da frequência base de 2.4 GHz e o baixo consumo de energia. Comparando o BLE e o Zigbee, o BLE é mais eficiente em termos energéticos, já que o consumo de energia por bit transmitido é menor [Al-Fuqaha et al., 2015], o que implica maior custo de *hardware* do BLE. Em redes de médio alcance, destaca-se o uso do WiFi (IEEE 802.11) como protocolo de acesso [Li et al., 2011], devido a popularização de equipamentos compatíveis e a facilidade de desenvolvimento de aplicações. Ao se considerar redes de longo alcance, em grandes cidades é comum o uso de redes de celulares 3G/4G para o sensoriamento e aquisição de dados. Essa alternativa apresenta alta taxa de transmissão, mas implica grande gasto energético dos dispositivos e necessidade de cobertura de rede de celu-

lar. Em áreas com pouca infraestrutura e para aplicações que não requerem altas taxas de transmissão, os protocolos LoraWAN [Adelantado et al., 2017] e ZigFox[1] são alternativas ao uso de redes de celulares para conectar objetos. Ambas tecnologias usam bandas estreitas para cobrir grandes áreas de alcance, com baixo consumo de energia e, consequentemente, baixa taxa de bits transmitidos. Vale ressaltar ainda o uso do protocolo 6LowPAN [Yibo et al., 2011] como protocolo de rede para baixo consumo de energia. O protocolo de rede 6LowPAN define encapsulamento e mecanismos de compressão de cabeçalho. O padrão suporta diversas tecnologias de acesso, como Ethernet, IEEE 802.11 e IEEE 802.15.4. Na camada de aplicação, o protocolo para serviços Web na Internet das Coisas, definido pelo IETF, é o Protocolo de Aplicação Restrita (*Constrained Application Protocol* - CoAP). O CoAP é um protocolo de transferência de dados sem estados que inclui um subconjunto de funcionalidades do HTTP. O CoAP foi reprojetado para operar com baixo poder de processamento e com restrição de gasto de energia em objetos conectados para comunicação entre dispositivos (*Machine to Machine* - M2M) [Bahia e Campista, 2017, Colitti et al., 2011].

As tecnologias habilitadoras da Internet das Coisas aplicadas ao sensoriamento e à governança de cidades caracterizam as cidades inteligentes [Santana et al., 2017]. A Figura 1(b) resume uma infraestrutura de referência para cidades inteligentes. No contexto de cidades inteligentes, o serviço de rede passa a ter um papel fundamental no transporte dos dados dos objetos até a plataforma de processamento e armazenamento de dados. Estas plataformas, mostradas na Figura 1(b), normalmente são realizadas através da computação em nuvem e fornecem interfaces entre as aplicações de gerenciamento e governança da cidade e os dados coletados. Paralelamente, aplicações de gerenciamento e controle em tempo real, como ferramentas de mercado, gerenciamento de operações e gestão de segurança, devem operar sobre dados sensoreados com latência mínima e, assim, devem ter acesso direto aos dados. Vale ainda ressaltar que a infraestrutura de rede de transporte passa a ser responsável pela adaptação entre diferentes protocolos de comunicação entre objetos, assim como por filtrar e agregar os dados monitorados.

3. A Infraestrutura Proposta

Os requisitos de rede dos objetos conectados em um cenário de Internet das Coisas são mais críticos do que redes convencionais em função da integração vertical das aplicações, chamados de silos, e da magnitude da comunicação entre dispositivos (*Machine to Machine* - M2M) [Omnes et al., 2015]. Segurança, mobilidade, escalabilidade, adequação a políticas e qualidade de serviço são requisitos essenciais e críticos de serem providos por objetos com restrições de processamento e gasto de energia. Nesse sentido, a infraestrutura proposta age de forma a prover um serviço de rede baseado no encadeamento de funções [Sanz et al., 2017] capaz de executar funções virtuais de rede (*Virtual Network Function* - VNF) terceirizadas pelos objetos conectados. Para tanto, a proposta introduz a ideia de um *gateway* virtualizado no equipamento de acesso dos objetos conectados ao ambiente de virtualização de rede, mostrado na Figura 2. Ao conectar os objetos à infraestrutura de virtualização de redes, o *gateway* executa somente o encaminhamento dos quadros que chegam a ele pelas interfaces virtuais de rede e todo processamento dos pacotes, adaptação de protocolos, conformação de políticas, qualidade de serviço ou

[1] http://makers.sigfox.com/.

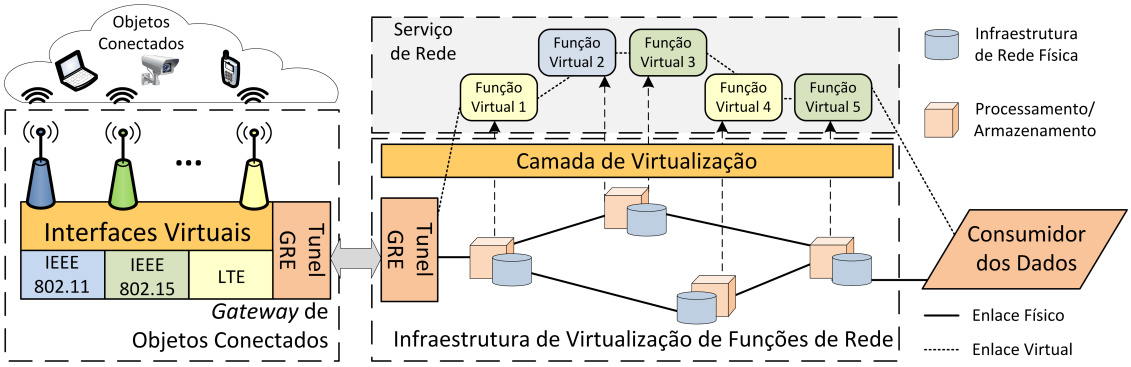


Figura 2. A infraestrutura de virtualização de funções de rede para Internet das Coisas. O *Gateway* de Objetos Conectados abstrai o método de acesso através de interfaces virtuais conectadas por túnel à Infraestrutura de Virtualização de Funções de Rede (NFVI). O *gateway* envia os quadros direto para a NFVI.

análise de conteúdo, é realizado pela infraestrutura de virtualização de redes através de funções virtuais de rede.

3.1. O *Gateway* de Acesso

A ideia principal do *gateway* é criar interfaces virtuais que ajam como diferentes pontos de acesso virtuais para diferentes domínios de objetos conectados. O *gateway* é realizado sobre um *hardware* que possui recursos físicos para implantar interfaces virtuais de rede, seja uma interface sem-fio IEEE 802.11, IEEE 802.15.4, uma estação base LTE ou outras tecnologias. Por simplicidade, neste trabalho considera-se um *gateway* equipado com uma placa de rede sem-fio IEEE 802.11n. Dessa forma, os objetos se conectam às redes cujo acesso é provido pelo *gateway*. No entanto, a função do *gateway* resume-se a prover a realização física do ponto de acesso, o que está alinhado com as propostas de redes 5G e C-RAN (*Cloud Radio Access Network*) [Checko et al., 2015]. Após a conexão, todos os quadros são encaminhados para infraestrutura de virtualização de redes através de um túnel GRE[2] (*Generic Routing Encapsulation*). Vale ressaltar que a conexão entre o *gateway* e a infraestrutura de virtualização de redes pode ocorrer através da Internet e, portanto, está sujeita a atrasos e perda de pacotes.

A virtualização das interfaces de rede sem-fio é realizada através da criação de um ponto de acesso virtual no *gateway*, usando a aplicação `hostapd`[3] em consonância com os utilitários `iw-utils`[4]. Dessa forma, a configuração dos pontos de acesso virtuais permite que um mesmo *gateway* forneça serviço de conectividade a diferentes domínios de IoT, garantindo assim o isolamento na camada física já que cada ponto de acesso virtual pode possuir suas próprias credenciais de autenticação e acesso. Com credenciais de acesso distintas, o participante de um domínio de IoT não é capaz de bisbilhotar os demais domínios virtuais, já que a criptografia na camada física é diferente para cada ponto de acesso virtual.

3.2. A Infraestrutura de Virtualização de Redes

A virtualização de funções de rede (*Network Function Virtualization* - NFV) caracteriza-se pela adoção de tecnologias de computação em nuvem, em especial da tec-

[2]Acessível em https://tools.ietf.org/html/rfc2784.
[3]Disponível em https://w1.fi/hostapd/.
[4]Disponível em http://drvbp1.linux-foundation.org/ mcgrof/rel-html/iw/.

nologia de virtualização, no domínio de redes de transporte, permitindo a virtualização de funções de rede implementadas em *software* [Medhat et al., 2017]. A Figura 2 mostra a infraestrutura de virtualização de redes baseada na arquitetura de referência de gerência e orquestração de funções virtuais de rede (*Network Function Virtualization MANagement and Orchestration* - NFV-MANO) [ETSI, 2014]. Na NFVI, os recursos físicos da rede são abstraídos em recursos virtuais e, nos ambientes virtuais, funções virtuais de rede são implementadas em *software* e encadeadas para prover serviços de rede complexos. O comportamento do serviço de rede para cada silo de IoT depende do encadeamento de diferentes VNFs.

Ao chegar um novo pacote na NFVI, esse pacote é direcionado a uma das cadeias de funções de serviço (*Service Function Chain* - SFC) existentes na infraestrutura. Uma cadeia de funções de serviço consiste no sequenciamento de funções virtuais de rede pelas quais o pacote deve seguir. Vale ressaltar que o sequenciamento correto das funções, assim como a escolha adequada das funções na cadeia, definem o comportamento do serviço de rede que o pacote encontra ao atravessar a NFVI. Para direcionar os pacotes para a cadeia de funções de serviço correta, a NFVI emprega um classificador logo após a entrada do pacote. O classificador marca o pacote com a etiqueta correta da SFC responsável por tratar o pacote.

A marcação da cadeia de função de serviços pode ser realizada com o protocolo de cabeçalho de serviço de rede (*Network Service Header* – NSH) [Kulkarni et al., 2017, Quinn e Elzur, 2017]. O direcionamento do tráfego para a SFC correta baseia-se em dois campos principais do protocolo, o SPI e o SI. O SPI, *Service Path Identifier*, identifica o caminho de serviço que o pacote deve seguir. Nesse contexto, um caminho de serviço é a sequência de funções virtuais que compõem o encadeamento de funções. O campo SI, *Service Index*, identifica em qual posição do caminho de serviço o pacote se encontra e, assim, permite identificar qual é a função virtual de rede correta para tratá-lo no momento. Contudo, as implementações disponíveis para o protocolo NSH ainda são iniciais e o desempenho alcançado não é satisfatório [Sanz et al., 2017]. Portanto, uma alternativa viável para estabelecer um caminho de serviço coerente e com bom desempenho é o uso de outros protocolos de encapsulamento bem estabelecidos, tais como GRE e VXLAN, para criar o encadeamento de funções de serviço. Neste trabalho, usa-se o protocolo GRE para implementar o encadeamento de funções de serviço.

3.3. As Funções Virtuais de Rede

As funções virtuais de rede consistem de ambientes virtuais que executam funções de tratamento de pacotes. Em uma arquitetura tradicional de Internet das Coisas, essas funções são exercidas pelos objetos conectados ou pelo *gateway* de acesso da rede de objetos conectados à Internet. Na infraestrutura proposta, tanto os objetos conectados quanto o *gateway* não necessitam de recursos para exercer as funções de rede, pois essas são terceirizadas para a NFVI sob a forma de funções virtuais de rede. Neste trabalho, as funções virtuais de rede são implementadas em máquinas virtuais executando Linux Ubuntu 16.04 e com suporte ao comutador por *software* Open vSwitch[5].

Propõem-se ainda duas VNFs dedicadas ao ambiente de IoT. A primeira classifica o tráfego de cada domínio de IoT entre legítimo ou malicioso através de algoritmos de

[5]Disponível em http://docs.openvswitch.org/

aprendizado de máquina. A segunda aplica políticas de qualidade de serviço ao tráfego através do encaminhamento de fluxos por filas com recursos previamente definidos. O encaminhamento dos fluxos para as filas corretas é executado por regras em um comutador por *software* instanciado como função virtual de rede.

3.4. O Consumidor dos Dados

O consumidor dos dados na infraestrutura proposta é qualquer agente que acesse objetos conectados. No caso de uma câmera de vigilância IP, por exemplo, o consumidor de dados pode ser um portal *web* que acessa as imagens capturadas pela câmera e encaminhadas e tratadas pela NFVI. Nesse caso, a NFVI enriquece o serviço de rede de transporte fazendo *cache* do fluxo de dados vindo da câmera e também adaptando o fluxo de dados da câmera para o padrão suportado pelos usuários finais ou pelo portal *web*. No caso de os objetos conectados serem uma rede de sensores e atuadores, o consumidor dos dados pode ser um *middleware* para IoT que se conecta diretamente à NFVI, sem a necessidade de gerenciar e controlar o acesso dos sensores à rede.

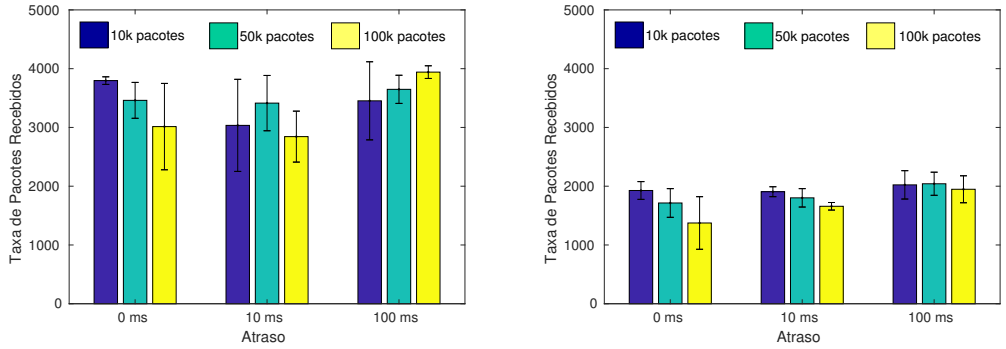
A implementação da infraestrutura proposta considera a *Open Platform for Network Function Virtualization* (OPNFV) como infraestrutura de virtualização de rede que é a plataforma de referência da arquitetura de NFV padronizada pela *European Telecommunications Standards Institute* (ETSI). A gerência da camada de virtualização é realizada pelo OpenStack. Para classificar, marcar o fluxo de entrada na NFVI e encaminhá-lo para a cadeia de funções corretas, utilizou-se o Open vSwitch.

4. Resultados Experimentais

O protótipo da infraestrutura de virtualização de redes para Internet das Coisas proposta foi desenvolvido baseado na plataforma OPNFV. O ambiente instalado sobre a OPNFV conta com quatro nós equipados com processador Intel Core i7-4770, 3.40 GHz, 32 GB de RAM e placa de rede Intel *gigabit*. A configuração do ambiente é organizada com um nó agindo como controlador de gerenciamento da nuvem OpenStack e controlador de rede definida por *software* OpenDaylight; os três outros nós são dedicados à virtualização de processamento e memória, através do Linux KVM, e ao armazenamento distribuído em disco através do Ceph. Todas as versões de *software* usados no ambiente são as de referência da distribuição do OPNFV Danube 3.0[6]. O *gateway* de acesso dos objetos conectados ao ambiente OPNFV foi implementado sobre um computador equipado com processador Intel Core i7-2600, 16 GB de RAM, uma placa de rede Intel *gigabit*, para acesso à NFVI, e placa de rede sem-fio, IEEE 802.11n, Ralink RT2870 USB, para criação dos pontos de acesso virtuais. Durante a avaliação do protótipo, foram usados como objetos conectados dois computadores portáteis, equipados com processador Intel Core i5-2410M, 6 GB de RAM e interface de rede sem-fio embutida, e uma câmera IP, sem-fio, D-Link DCS-5020L.

A avaliação da proposta é dividida em quatro etapas. A primeira etapa verifica o desempenho da conexão da rede de objetos à infraestrutura de virtualização de rede em cenários em que há diferentes atrasos na comunicação entre o *gateway* e a NFVI. O atraso adicionado simula a conexão entre *gateway* e NFVI como uma conexão através de uma rede de larga escala (WAN) e é adicionado com uma variação de 10% através da

[6]Disponível em https://www.opnfv.org/software/downloads/release-archives/danube-3-0.



(a) Pacotes de 64 bytes.

(b) Pacotes de 1200 bytes.

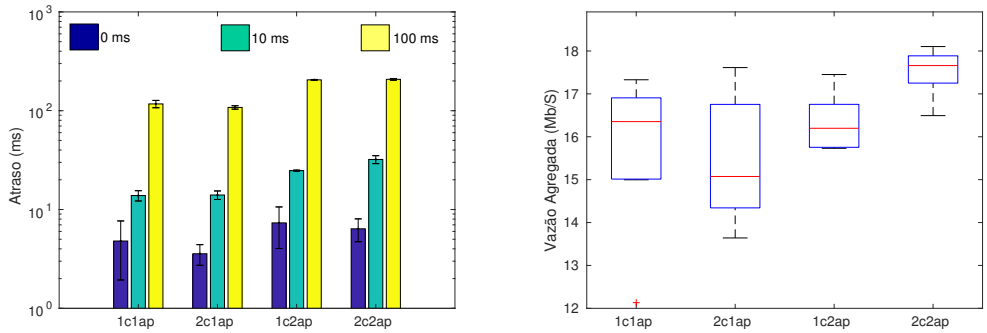
Figura 3. Taxa de pacotes de recebidas pelo consumidor de dados ao realizar envios em taxas superiores à capacidade do enlace sem-fio. O atraso entre o *gateway* e a infraestrutura de virtualização de rede não influencia nas taxas alcançadas. Os experimentos foram realizados com fluxos UDP com pacotes pequenos (a) 64 bytes e pacotes grandes (b) 1200 bytes.

ferramenta `tc` (*Traffic Control*[7]). A segunda etapa avalia a sobrecarga da virtualização da interface de rede sem-fio. A terceira etapa compara o desempenho de três algoritmos de classificação baseados em aprendizado de máquina para identificar tráfego malicioso e tráfego legítimo na rede de objetos conectados. Por fim, a quarta etapa da avaliação testa a efetividade da infraestrutura de virtualização de rede proposta para proteger a rede de objetos conectados de ataques e prover qualidade de serviço a tráfegos prioritários. Todos os resultados apresentados são médias com intervalo de confiança de 95%.

Na primeira etapa da avaliação, os experimentos visam aferir a taxa máxima de pacotes enviadas pelos objetos conectados e recebidas por consumidores de dados. Nesse experimento, como objeto conectado foi usado o computador portátil. A Figura 3 compara as taxas máximas obtidas para o envio de 10 mil, 50 mil e 100 mil pacotes/s, para pacotes pequenos de 64 B e pacotes grandes de 1.200 B. Vale ressaltar que na infraestrutura criada a unidade de transferência máxima (MTU) foi configurada para 1.280 B devido às sobrecargas com encapsulamentos. O envio de pacotes foi realizado através da criação de fluxos UDP com taxa de pacotes/s constante. Na Figura 3(a) verifica-se que a taxa máxima de pacotes que o *gateway* alcança é de 4.000 pacotes/s, independentemente da taxa de envio do nó. Verifica-se ainda que o atraso entre o *gateway* e a NFVI pouco influencia na taxa de pacotes alcançada. Ao utilizar-se pacotes maiores, 1200 B, o fator limitante foi taxa de transmissão alcançada pela placa de rede sem-fio do *gateway*. Verificando a taxa de transmissão real alcançada pela placa de rede sem-fio, configurada para operar no modo 802.11g, a taxa obtida foi de aproximadamente 18 Mb/s.

A segunda etapa da avaliação foca na virtualização da rede sem-fio. A avaliação considera quatro cenários simples de aplicação da infraestrutura de virtualização para IoT. O primeiro cenário contempla o caso em que há um computador conectado a um ponto de acesso virtual (`1c1ap`); o segundo, 2 computadores em um único ponto de acesso virtual (`2c1ap`); o terceiro, 1 computador em 2 pontos de acesso virtuais (`1c2ap`); e, por fim, o último cenário em que há 2 computadores conectados há 2 pontos de acesso virtuais (`2c2ap`). A Figura 4(a) mostra a variação no atraso percebido pelos objetos conectados

[7]Documentação em http://lartc.org/manpages/tc.txt.



(a) Atraso com virtualização do sem-fio. (b) Banda com virtualização do sem-fio.

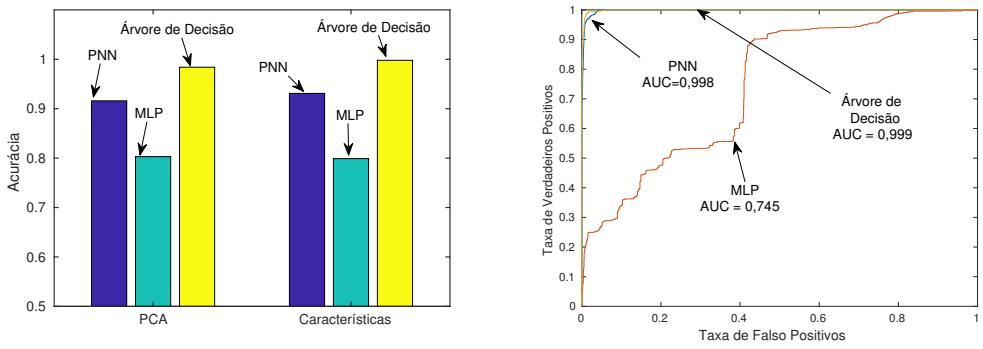
Figura 4. Virtualização do enlace sem-fio. Avaliação dos cenários com 1 computador e 1 ponto de acesso virtual (`1c1ap`); 2 computadores e 1 ponto de acesso virtual (`2c1ap`); 1 computador e 2 pontos de acesso virtuais (`1c2ap`); e 2 computadores e 2 pontos de acesso virtuais (`2c2ap`). a) O acrescimo no atraso percebido pelos dispositivos conectados é inferior a 10 ms, mesmo quando o atraso entre o *gateway* e a NFVI é de 100 ms. (b) A banda agregada ao usar 2 computadores e 2 pontos de acesso virtuais é, na média, superior aos demais casos.

em cada cenário quando há o acréscimo de latência entre o *gateway* e a NFVI. Nota-se que o atraso percebido pelos nós é mais significativo quando não há latência na conexão do *gateway* (0 ms), já que o tempo de comunicação entre o *gateway* e a NFVI somado à sobrecarga de virtualização da rede sem-fio introduz uma latência da ordem de 10 ms. Conforme ocorre o aumento do atraso entre *gateway* e NFVI, o atraso introduzido pela virtualização torna-se menos significativo. O segundo experimento dessa etapa verifica a banda agregada alcançada pelos objetos em cada cenário, Figura 4(b). A banda agregada não é afetada pela virtualização da rede sem-fio para pacotes de 1200 B. A banda agregada aumenta no cenário com dois pontos de acesso e dois computadores. Tal comportamento deve-se ao fato de que ao realizar a virtualização, o escalonamento entre os nós sem-fio é realizado pelo núcleo do sistema operacional do *gateway* em detrimento da realização do escalonamento pelo controlador da placa de rede sem-fio que apresenta um controlador com baixo poder de processamento.

Na terceira e na quarta etapas da avaliação da proposta, considera-se um caso de uso da infraestrutura de virtualização para IoT em que a rede de objetos conectados é compartilhada entre usuários de rede sem-fio, por exemplo celulares inteligentes, e objetos com acesso à Internet, como uma câmera IP. Nesse caso de uso, todos os objetos conectados são susceptíveis a ataques e à infecção por *malware*. Assim, uma possível proteção da rede é instanciação de uma função de rede capaz de classificar o tráfego em legítimo ou tráfego malicioso e posterior adequação do tráfego a políticas.

A classificação do tráfego entre legítimo e malicioso depende do treinamento e da avaliação de algoritmos de classificação baseados em aprendizado de máquina. Para tanto, foi criado um conjunto de dados de treinamento e teste composto de dados legítimos e dados de ataques rotulados[8]. Os dados legítimos foram coletados durante o uso quotidiano de câmeras IP e de usuários de rede sem-fio no Grupo de Teleinformática e Automação (GTA/UFRJ). Em especial, as câmeras foram acessadas para gerar flu-

[8]O conjunto de dados pode ser obtido através de contato com os autores.



(a) Acurácia da classificação. (b) Curva ROC para a classe de ataque.

Figura 5. Avaliação de algoritmos de aprendizado de máquina para a classificação de tráfego IoT quando usando PCA para redução de dimensionalidade e usando todas as características. a) A acurácia do classificador baseado em Árvores de Decisão é superior à Rede Neural Probabilística e à Rede Neural com Múltiplas Camadas. b) Comparação das taxas de falsos positivos e verdadeiros positivos dos classificadores.

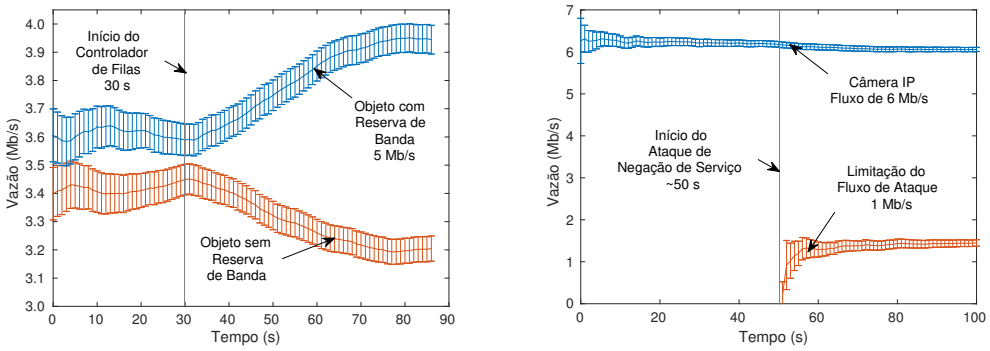
xos de vídeo contínuo, acesso a servidores FTP para transferência de vídeos e fotos e sincronização de data pelo *Network Time Protocol* (NTP). Os dados de ataque foram obtidos dos traços coletados por Garcia *et al.* em um estudo sobre o comportamento de *botnets* [García et al., 2014]. O conjunto de dados é composto por fluxos identificados pela tupla de endereço IP de origem e de destino, portas de origem e destino e protocolo de transporte [Andreoni Lopez et al., 2017]. As características usadas para geração do conjunto de dados são o subconjunto das características numéricas fornecidas pela aplicação de análise de traços de rede `flowtbag`[9], acrescidas de marcações para os 10 serviços mais acessados, em número de fluxos. Esses serviços representam 1% de todos os serviços acessados no conjunto de dados.

Tabela 1. Classificação com Árvores de Decisão e redução de dimensionalidade.

	VP	FP	VN	FN	Precisão	Sens.	Espec.
Malicioso	14.208	290	3.995	0,00	0,98	1,00	0,93
Normal	3.995	0	14.208	290	1,00	0,93	1,00

A Figura 5(a) compara a acurácia de três algoritmos de classificação: rede neural probabilística (`PNN`); rede neural com múltiplas camadas (`MLP`) e árvores de decisão (`Árvores de Decisão`). Os algoritmos foram executados para todas as características e para o cenário em que a dimensionalidade do problema foi reduzida usando-se a análise de componentes principais (PCA). Nota-se que a classificação usando árvores de decisão treinadas com o algoritmo de *gradient boosting* apresenta a melhor acurácia quando comparada com redes neurais. Tal comportamento é esperado dada a natureza discreta dos dados dos fluxos, em que a segmentação binária dos dados, conforme é feita pelo algoritmo de árvore de decisão, leva a regras de classificação acuradas. Quando compara-se a relação entre taxa de verdadeiros positivos e falsos positivos dos algoritmos de classificação, curva ROC mostrada na Figura 5(b), as árvores de decisão apresentam uma área abaixo da curva (AUC) muito próxima a 1, indicando que a classificação dos da-

[9]https://github.com/DanielArndt/flowtbag



(a) Diferenciação entre fluxos.

(b) Ataque de negação de serviço na rede.

Figura 6. Diferenciação entre fluxos no cenário de IoT. a) Dois objetos conectados compartilham a rede sem-fio e enviam tráfego UDP constante a 5 Mb/s. Em 30 s, o controlador de recursos de banda é ativado. Um objeto tem 5 Mb/s garantido por política e o outro só tem um mínimo garantido de 1 Mb/s. b) Cenário de ataque de negação de serviço na rede de sensores com uma câmera IP e um nó. O fluxo classificado como legítimo da câmera IP tem mínimo de 6 Mb/s garantidos pela política de filas. O fluxo não-legítimo é limitado a 1 Mb/s.

dos não incorre na geração de falsos positivos, nem falsos negativos, para a classe de ataque. A redução da dimensionalidade para apenas 8 componentes principais manteve 99% da informação do conjunto de dados e tem acurácia praticamente igual à classificação com todas as características. A Tabela 1 mostra o desempenho das árvores de decisão, com dimensionalidade reduzida pelo PCA, em uma avaliação cruzada em 10 rodadas[10]. A acurácia nominal desse foi de $0,998$, com sensibilidade de $1,0$ no tráfego malicioso.

Por fim, na quarta etapa, avalia-se a capacidade de a infraestrutura de virtualização proposta tomar contramedidas e aplicar políticas aos pacotes. A Figura 6(a) mostra o resultado do experimento em que dois computadores portáteis conectados à rede sem-fio têm acesso a qualidade de serviço (QoS) distintas. A diferenciação do serviço é provida por uma VNF através do direcionamento do tráfego dos nós para filas distintas. As filas são implementadas em um comutador por *software* Open vSwitch. No experimento, ambos os nós executam um fluxo TCP na vazão máxima que alcançam. Um dos nós é direcionado a uma fila com garantia mínima de recurso de banda a 5 Mb/s. O outro nó tem uma garantia mínima de 1 Mb/s. A Figura 6(a) ressalta que após 30 s, os limites das filas são configurados e os fluxos passam a ser conformados pelos limites, garantindo ao tráfego de maior recurso reservado banda total, útil mais encapsulamento, próxima aos 5 Mb/s, em detrimento do outro nó que não possui recursos dedicados.

A Figura 6(b) mostra o cenário em que uma câmera IP está enviando um fluxo de vídeo contínuo TCP de aproximadamente 6 Mb/s quando ocorre um ataque de negação de serviço (DoS). O ataque de negação de serviço é configurado como um fluxo UDP de 20 Mb/s. No entanto, mesmo a câmera tendo uma configuração de *hardware* inferior ao computador portátil atacante, a função de rede virtualizada consegue garantir a taxa de transmissão estável para a câmera, enquanto limita o tráfego classificado como malicioso a aproximadamente 1 Mb/s, evitando assim a degradação do serviço provido pela câmera.

[10]VP: Verdadeiro Positivo; FP: Falso Positivo; VN: Verdadeiro Negativo; FN: Falso Negativo; Sens.: Sensibilidade; Espec: Especificidade.

5. Trabalhos Relacionados

Petrolo *et al.* argumentam que cidades inteligentes é uma aplicação de Internet das Coisas no domínio das cidades e destacam os benefícios da integração de diversos dispositivos conectados. Os autores definem o conceito de Nuvem de Coisas (*Cloud of Things* – CoT) que consiste no uso de ambientes de computação em nuvem para prover uma plataforma de integração de silos de dados de IoT [Petrolo et al., 2017]. Santana *et al.* ratificam a ideia de cidades inteligentes composta por objetos conectados e argumentam que a quantidade de dados gerados em cidades inteligentes é grande e requer uso de técnicas próprias para *Big Data* [Santana et al., 2017]. Assim, Santana *et al.* vislumbram a arquitetura de cidades inteligentes como uma agregação de processamento em nuvem com sistemas ciber-físicos (*Cyber-Physical Systems* – CPS).

Atzori *et al.* comparam as características de sistemas de identificação por rádio frequência (RFID) , redes de sensores sem fios e redes de RFID. Os autores evidenciam que os sistemas RFID são pequenos, de baixo custo e energia não é limitante. As redes de sensores sem fio apresentam alta cobertura de rádio e a comunicação não requer a presença de um leitor, enquanto nos sistemas RFID, leitor e sensor são assimétricos. As redes de sensores RFID possibilitam a detecção, computação e comunicação em um sistema passivo [Atzori et al., 2010]. Por sua vez, Adelantado *et al.* investigam as limitações do padrão LoRaWAN [Adelantado et al., 2017]. Assim, cada rede de acesso diferente para os dispositivos de IoT apresenta características e requisitos de redes distintos.

Quin *et al.* propõem um *middleware* baseado em redes definidas por *software* para Internet das Coisas. A ideia consiste em prover múltiplos ambientes de rede para IoT para atender demandas de rede com diferentes requisitos [Qin et al., 2014]. Para tanto, a proposta monitora a rede e usa cálculo de rede para prever a mudança no desempenho. A proposta Black SDN, por sua vez, propõe o uso de redes definidas por *software* para prover segurança em redes de IoT através da criptografia tanto do conteúdo quanto dos cabeçalhos dos pacotes [Chakrabarty et al., 2015].

Bizanis e Kuipers investigam o emprego de virtualização e redes definidas por *software* em ambientes de Internet das Coisas [Bizanis e Kuipers, 2016]. Os autores concluem que a virtualização de rede e as redes definidas por *software* são facilitadores da Internet das Coisas, mas focam somente no uso dessas tecnologias como forma de gerenciar os fluxos gerados por objetos conectados. Ojo *et al.* defendem que arquiteturas e protocolos de rede tradicionais são ineficientes para suportar o alto nível de escalabilidade, a grande quantidade de tráfego e a mobilidade dos dispositivos de IoT. Além disso, é difícil gerenciar a quantidade de dados gerada, o que pode causar problemas e interrupções na rede [Ojo et al., 2016]. Assim, os autores propõem que a rede de transporte de dados de IoT seja gerenciada com aplicações sobre as redes definidas por *software* e com funções de rede implementadas em funções virtuais de rede. Contudo, os autores não focam na criação de domínios de IoT isolados que compreendam desde o acesso até o consumo.

A infraestrutura de rede de transporte proposta nesse artigo baseia-se em um *gateway* simples que encaminha todos os pacotes dos objetos conectados para um ambiente de virtualização de funções de rede. Diferentemente das propostas anteriores, esse trabalho foca na rede de transporte dos dados, independentemente, do *middleware* ou da plataforma de IoT utilizados. As funções exercidas pela rede de transporte compreendem o encaminhamento de pacotes, a adequação a políticas e a adaptação de dados.

6. Conclusão

O número de objetos conectados é cada vez maior e a criticidade dos dados trafegados também. Contudo, as redes de transporte de dados para Internet das Coisas é preterida em relação à aquisição e ao processamento dos dados. Esse artigo propôs uma infraestrutura de virtualização de funções de rede que permite a implantação ágil e efetiva de funções virtuais. A proposta desenvolveu a ideia de um nó de acesso virtualizado capaz de criar domínios independentes de objetos conectados. Em cada domínio são aplicadas funções de rede independentes e ajustadas para os requisitos de desempenho e segurança de cada aplicação de Internet das Coisas. Um protótipo da infraestrutura proposta foi desenvolvido e avaliado. Os resultados demonstram que o nó de acesso virtualizado não introduz perda de desempenho para o acesso dos objetos conectados. Verificou-se ainda que a latência entre o nó de acesso e a infraestrutura pode ser substancialmente alta sem que haja perdas de desempenho. Por fim, foi desenvolvido um caso de uso da infraestrutura proposta, em que uma função virtual de rede foi capaz de classificar o tráfego entre legítimo ou malicioso com 99,8% de acurácia e, em seguida, uma outra função virtual garantiu qualidade de serviço ao tráfego legítimo e limitou um ataque de negação de serviço impedindo que o serviço essencial de uma câmera IP fosse degradado.

Referências

[Adelantado et al., 2017] Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia-Segui, J. e Watteyne, T. (2017). Understanding the limits of LoRaWAN. volume 55, p. 34–40.

[Al-Fuqaha et al., 2015] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. e Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376.

[Andreoni Lopez et al., 2017] Andreoni Lopez, M., Silva, R. S., Alvarenga, I., Rebello, G., Sanz, I. J., Lobato, A., Mattos, D., Duarte, O. C. M. B. e Pujolle, G. (2017). Collecting and characterizing a real broadband access network traffic dataset. Em *2017 1st Cyber Security in Networking Conference (CSNet'17)*, Rio de Janeiro, Brazil.

[Atzori et al., 2010] Atzori, L., Iera, A. e Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15):2787 – 2805.

[Bahia e Campista, 2017] Bahia, J. G. e Campista, M. E. M. (2017). Um mecanismo de controle de demanda no provimento de serviços de iot usando coap. Em *Workshop de Gerência e Operação de Redes e Serviços (WGRS 2017) do SBRC'2017*.

[Bizanis e Kuipers, 2016] Bizanis, N. e Kuipers, F. A. (2016). SDN and virtualization solutions for the Internet of Things: A survey. *IEEE Access*, 4:5591–5606.

[Chakrabarty et al., 2015] Chakrabarty, S., Engels, D. W. e Thathapudi, S. (2015). Black SDN for the Internet of Things. Em *2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems*, p. 190–198.

[Checko et al., 2015] Checko, A., Christiansen, H. L., Yan, Y., Scolari, L., Kardaras, G., Berger, M. S. e Dittmann, L. (2015). Cloud RAN for mobile networks: A technology overview. *IEEE Communications Surveys Tutorials*, 17(1):405–426.

[Colitti et al., 2011] Colitti, W., Steenhaut, K. e De Caro, N. (2011). Integrating wireless sensor networks with the web. *Extending the Internet to Low power and Lossy Networks (IP+ SN 2011)*.

[ETSI, 2014] ETSI (2014). ETSI GS NFV-MAN 001: Network functions virtualisation; management and orchestration. Relatório técnico.

[García et al., 2014] García, S., Grill, M., Stiborek, J. e Zunino, A. (2014). An empirical comparison of botnet detection methods. *Computers & Security*, 45(Supplement C):100 – 123.

[Kulkarni et al., 2017] Kulkarni, S., Arumaithurai, M., Ramakrishnan, K. K. e Fu, X. (2017). Neo-NSH: Towards scalable and efficient dynamic service function chaining of elastic network functions. Em *20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*, p. 308–312.

[Li et al., 2011] Li, L., Xiaoguang, H., Ke, C. e Ketai, H. (2011). The applications of WiFi-based wireless sensor network in Internet of Things and Smart Grid. Em *2011 6th IEEE Conference on Industrial Electronics and Applications*, p. 789–793.

[Medhat et al., 2017] Medhat, A. M., Taleb, T., Elmangoush, A., Carella, G. A., Covaci, S. e Magedanz, T. (2017). Service function chaining in next generation networks: State of the art and research challenges. *IEEE Communications Magazine*, 55(2):216–223.

[Ojo et al., 2016] Ojo, M., Adami, D. e Giordano, S. (2016). A SDN-IoT architecture with NFV implementation. Em *2016 IEEE Globecom Workshops (GC Wkshps)*, p. 1–6.

[Omnes et al., 2015] Omnes, N., Bouillon, M., Fromentoux, G. e Grand, O. L. (2015). A programmable and virtualized network IT infrastructure for the Internet of Things: How can NFV SDN help for facing the upcoming challenges. Em *2015 18th International Conference on Intelligence in Next Generation Networks*, p. 64–69.

[Petrolo et al., 2017] Petrolo, R., Loscrì, V. e Mitton, N. (2017). Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms. *Transactions on Emerging Telecommunications Technologies*, 28(1).

[Qin et al., 2014] Qin, Z., Denker, G., Giannelli, C., Bellavista, P. e Venkatasubramanian, N. (2014). A software defined networking architecture for the Internet-of-Things. Em *2014 IEEE Network Operations and Management Symposium (NOMS)*, p. 1–9.

[Quinn e Elzur, 2017] Quinn, P. e Elzur, U. (2017). Network service header. Internet-Draft draft-ietf-sfc-nsh-12, IETF Secretariat. `http://www.ietf.org/internet-drafts/draft-ietf-sfc-nsh-12.txt`.

[Santana et al., 2017] Santana, E. F. Z., Chaves, A. P., Gerosa, M. A., Kon, F. e Milojicic, D. (2017). Software platforms for smart cities: Concepts, requirements, challenges, and a unified reference architecture. *Accepted for publication in ACM Computing Surveys*.

[Sanz et al., 2017] Sanz, I. J., Alvarenga, I., Lopez, M. A., Mauricio, L. A. F., Mattos, D., Rubinstein, M. e Duarte, O. C. M. B. (2017). Uma avaliação de desempenho de segurança definida por software através de cadeias de funções de rede. Em *XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg'2015)*.

[United Nations, 2014] United Nations (2014). World urbanization prospects: The 2014 revision, highlights. Department of Economic and Social Affairs. *Population Division, United Nations*.

[Wang et al., 2016] Wang, S., Wan, J., Zhang, D., Li, D. e Zhang, C. (2016). Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination. *Computer Networks*, 101(Supplement C):158 – 168.

[Yibo et al., 2011] Yibo, C., Hou, K. M., Zhou, H., l. Shi, H., Liu, X., Diao, X., Ding, H., Li, J. J. e de Vaulx, C. (2011). 6LoWPAN stacks: A survey. Em *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, p. 1–4.

[Zhang et al., 2017] Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J. e Shen, X. S. (2017). Security and privacy in Smart City applications: Challenges and solutions. *IEEE Communications Magazine*, 55(1):122–129.