Uma Avaliação do Impacto da Diferenciação de Tráfego na Internet das Coisas

Thiago Garrett[1], **Schahram Dustdar**[2], **Luis C. E. Bona**[1], **Elias P. Duarte Jr.**[1]

[1]Departamento de Informática
Universidade Federal do Paraná – Curitiba, PR – Brasil

[2]Distributed Systems Group
TU Wien – Viena – Áustria

{tgarrett,bona,elias}@inf.ufpr.br, dustdar@infosys.tuwien.ac.at

Abstract. *The Internet of Things (IoT) is expected to constitute a great portion of the Internet traffic in the future. In this context, it is important to ensure Network Neutrality, which states that all traffic must be treated equally, i.e., without traffic differentiation (TD). Unfair traffic management may result in a non-competitive market, affecting selectively the quality of experience of different IoT applications. In this paper, we study the impact of TD on common IoT traffic patterns, such as periodic updates and real-time notifications. We present simulation results, and discuss the vulnerabilities of IoT applications under TD.*

Resumo. *A Internet das Coisas (IoT) deve representar em breve uma porção significativa do tráfego da Internet. Neste contexto, é importante garantir a Neutralidade da Rede, que estabelece que todo tráfego deve ser tratado de forma igualitária, ou seja, sem diferenciação de tráfego (DT). Práticas discriminatórias podem afetar seletivamente a qualidade de experiência de diferentes aplicações IoT. Neste trabalho examinamos o impacto da DT em padrões de tráfego comuns na IoT, como atualizações periódicas e notificações em tempo real. Apresentamos resultados de simulações, e discutimos as vulnerabilidades de aplicações IoT à DT.*

1. Introdução

A Internet das Coisas (IoT) torna-se cada vez mais presente na vida moderna. Ela consiste em inúmeros dispositivos conectados (sensores e atuadores), os quais em conjunto produzem uma grande quantidade de dados e fornecem diversos serviços. Estimativas mostram que haverão aproximadamente 212 bilhões de dispositivos IoT em 2020 e aproximadamente 45% do tráfego da Internet será relacionado à IoT em 2022 [Al-Fuqaha et al. 2015]. Estas estimativas indicam que a IoT representará uma porção significativa da Internet no futuro, tanto em quantidade de dados trafegados quanto em participação no mercado.

A evolução da IoT terá certamente um grande impacto econômico em diversas áreas, trazendo novas oportunidades para fabricantes de dispositivos, provedores de acesso (*Internet Service Providers*, ISPs) e desenvolvedores de aplicativos [Al-Fuqaha et al. 2015]. Dispositivos "tradicionais" podem ser transformados em "inteligentes", ISPs podem expandir suas infraestruturas para suportar o crescimento do tráfego e oferecer novos serviços, assim como desenvolvedores podem criar usos inovadores para a quantidade enorme de dados produzidos. No entanto, a inovação e, portanto, o sucesso da IoT, podem ser prejudicados por práticas injustas de gerência de tráfego dos ISPs [Garrett et al. 2017]. Neste contexto, discutimos a Neutralidade da Rede (NR), que estabelece que ISPs devem tratar todo tráfego de forma igualitária, independentemente da sua origem, destino e/ou conteúdo, i.e., sem Diferenciação

de Tráfego (DT) [Garrett et al. 2018]. A DT pode afetar seletivamente a qualidade de experiência (*Quality of Experience*, QoE) de diferentes aplicativos IoT, resultando em um mercado não competitivo, já que uma diferença na QoE pode determinar o sucesso ou falha de um dispositivo ou aplicativo em relação aos concorrentes [Shin 2017]. Em uma Internet não neutra, novos dispositivos, aplicações ou serviços inovadores de pequenas empresas podem não ser capazes de competir com produtos mais estabelecidos de empresas maiores [Garrett et al. 2017]. Um ISP pode discriminar tráfego de fabricantes de dispositivos específicos (como marcas de sensores ou veículos), aplicações (como protocolos proprietários) ou origem/destinos (como clientes *premium*, fornecedores de nuvem, plataformas IoT).

Neste artigo examinamos como a DT pode afetar diferentes padrões de tráfego da IoT. Trabalhos relacionados incluem estudos do impacto de *Machine-Type Communication* (MTC) em redes celulares e como ele concorre com *Human-type Communication* (HTC) pelos recursos de rede [Shafiq et al. 2012, Dawy et al. 2017]. Trabalhos que buscam detectar DT também tem relação com este artigo. Um *survey* abrangente sobre detecção de DT foi publicado recentemente [Garrett et al. 2018].

Primeiramente, apresentamos padrões de tráfego comuns gerados por aplicações IoT na Seção 2. Em seguida, resultados de simulação de cada padrão de tráfego sob diferentes cenários de DT são apresentados na Seção 3. Concluímos o artigo na seção 4.

2. Padrões de Tráfego IoT

O tráfego na IoT é composto principalmente de MTC [Al-Fuqaha et al. 2015] – ou comunicação *Machine-to-machine* (M2M). MTC caracteriza-se pela comunicação de vários dispositivos sem a necessidade de interação humana, em oposição à HTC. Na IoT, sensores, *gateways*, *middlewares* e serviços em nuvem comunicam-se de forma autônoma. A interação humana também está presente, como na entrada de comandos (como em casas inteligentes), ou durante situações críticas (como em alarmes de segurança).

O tráfego MTC geralmente é composto por fluxos curtos e esparsos de pacotes pequenos [Nikaein et al. 2013]. Já HTC é caracterizado por um fluxo contínuo de pacotes grandes. Em relação às redes de acesso, o MTC ocorre principalmente na direção de *upload* (dos dispositivos finais para a nuvem), enquanto a HTC na direção de *download* (da nuvem para os dispositivos finais). Exemplos de tráfego HTC incluem mensagens instantâneas, VoIP, *streaming* de vídeo/áudio, páginas Web e compartilhamento de arquivos.

Três padrões comuns de tráfego MTC foram identificados em [Nikaein et al. 2013]: *Periodic Update* (PU), *Event-Driven* (ED) e *Payload Exchange* (PE). Segundo os autores, esses padrões correspondem às funções da maioria dos aplicativos M2M. Aplicações IoT são, em geral, compostas por uma combinação desses padrões. O padrão **PU** consiste em enviar periodicamente relatórios para uma entidade central. O tráfego é gerado em um intervalo periódico, geralmente composto de pequenos pacotes de tamanho constante. No padrão **ED**, o tráfego é esporádico, gerado quando ocorre um evento. O tamanho dos dados pode variar dependendo da aplicação e da quantidade de informações de cada evento. Esse tipo de tráfego geralmente é em tempo real, especialmente quando os eventos se referem a situações que devem ser tratadas rapidamente. Já o padrão **PE** corresponde à transferência de quantidades maiores de dados. Geralmente ocorre após um evento ser notificado, caso esse evento necessite de mais informações para ser tratado. Por exemplo, um sistema de monitoramento de rios reporta periodicamente o nível da água (PU). Se o nível da água ultrapassar um determinado limiar, um alarme de inundação pode ser emitido (ED). Para lidar com este evento, um *streaming* de vídeo pode ser iniciado para acompanhar a situação em tempo real (PE).

3. Resultados

Nesta seção, descrevemos várias simulações que examinam o impacto da DT sobre os diferentes padrões de tráfego IoT. O objetivo destas simulações é verificar se a priorização pode resultar em um diferença de QoE significativa. Simulamos cada padrão em três diferentes cenários de DT, totalizando 9 simulações. Empregamos o *framework* de simulação OMNeT++[1]. Cada simulação dura 1800 segundos, configurados empiricamente.

Em cada simulação três tipos de tráfego são gerados simultaneamente: Tráfego de Fundo (TF), Tráfego de Prioridade Alta (TPA) e Tráfego de Prioridade Baixa (TPB). Estes três tipos de tráfego atravessam a mesma rede, a qual emprega um mecanismo de DT. Um roteador encaminha os diversos tipos de tráfego para seus destinos. Os *links* entre as fontes de tráfego e a rede têm largura de banda de 10 Mbps e um atraso de propagação de 10 ms, bem como os *links* entre o mecanismo de DT e o roteador e entre o roteador e os destinos. O atraso de propagação total é, portanto, 30 ms, e a taxa de saída máxima da rede é de 10 Mbps. Os TPA e TPB correspondem aos três padrões IoT (PU, ED e PE). O TF simula o tráfego já existente na Internet, de fontes que não sejam dispositivos e aplicativos IoT, o que pode levar a congestionamento. Implementamos essa priorização reservando uma pequena porção (1%) da largura de banda do *link* de saída da rede para o TPA, ou seja, o tráfego priorizado tem garantidamente pelo menos 100 Kbps de largura de banda.

O **TF** é gerado em um padrão HTC, já que o tráfego IoT compete com o HTC pelos recursos de rede [Shafiq et al. 2012] na Internet. Assim, ele é composto de vários fluxos contínuos de pacotes com tamanho e taxa variáveis. Cada fluxo consiste em pacotes com tamanhos aleatórios, variando de 250 a 1000 bytes. Os pacotes são enviados em intervalos aleatórios, que variam de 8 a 12 ms, resultando em uma taxa de envio média de 500 Kbps. Para avaliar como os padrões de tráfego IoT comportam-se com diferentes condições de TF e congestionamento, o TF é gerado em 4 níveis diferentes durante os 1800 segundos de simulação. Nos primeiros 100 segundos, não há TF. A partir dos segundos 100 a 500 da simulação, a taxa de envio do TF aumenta gradualmente (iniciando novos fluxos) até atingir a taxa máxima da rede (10 Mbps), aproximadamente. Em 1300s, o TF aumenta em cerca de 500 Kbps, e novamente em 1600s.

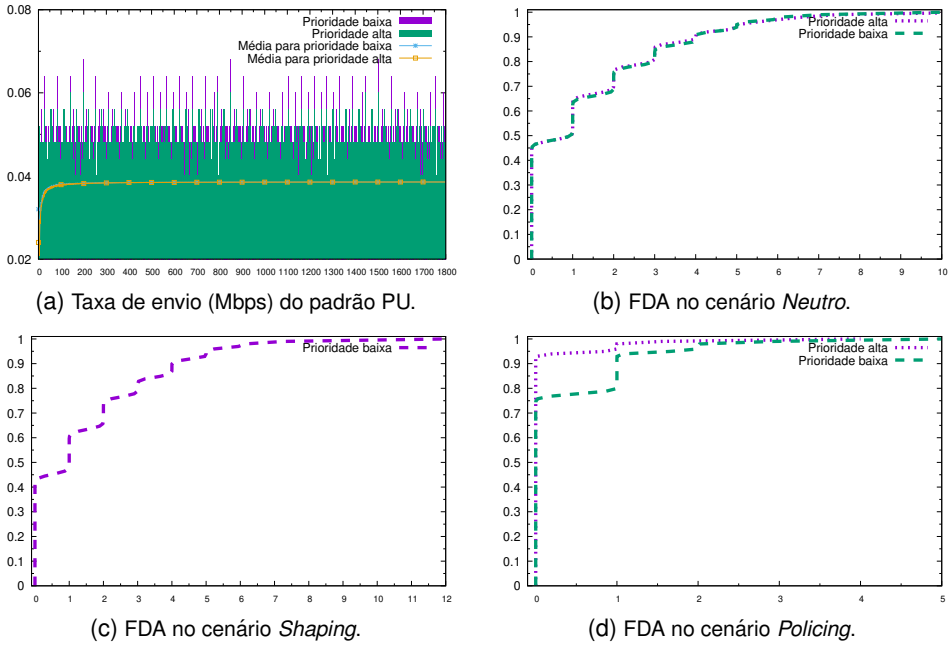
Implementamos os diferentes padrões de tráfego com base no modelo de tráfego MTC proposto em [Nikaein et al. 2013] e a caracterização de tráfego IoT apresentada em [Sivanathan et al. 2017]. Cada padrão difere em vários parâmetros: número de fontes de tráfego, tamanho dos pacotes, tamanho total dos dados, taxa de envio e intervalo entre transmissões. O padrão **PU** envia um pacote de tamanho constante a cada 5 segundos, utilizando o protocolo TCP. Empregamos 50 fontes de TPA e 50 de TPB gerando tráfego PU. O padrão **ED** envia rajadas curtas em tempos aleatórios. Uma rajada contém entre 1 a 900 pacotes TCP e representa a notificação de um evento. Empregamos 50 fontes de TPA e 50 de TPB gerando tráfego ED. Implementamos o padrão **PE** como fluxos contínuos de tráfego UDP, semelhante ao tráfego HTC empregado como TF. Utilizamos 30 fontes de cada prioridade, totalizando 60, gerando tráfego PE. Como esses padrões geralmente ocorrem após a notificação de um evento, iniciamos as transferências de PE da mesma maneira que o padrão ED.

Os três cenários de DT são: *Neutro*, *Shaping* e *Policing*. No cenário **Neutro**, não é realizada nenhuma DT. Os pacotes são encaminhados na ordem em que chegaram, e em caso de fila cheia os novos pacotes são descartados. No cenário **Shaping**, baseado em *traffic shaping*, a taxa reservada (100 Kbps) é garantida enfileirando os pacotes prioritários que

[1] `https://www.omnetpp.org/`

estiverem dentro desta taxa em um fila separada e encaminhando-os primeiro. Já no cenário **Policing**, baseado em *traffic policing*, os pacotes prioritários dentro da taxa reservada nunca são descartados, enquanto os demais pacotes são descartados caso excedam a taxa de saída máxima da rede (10 Mbps).

Apresentamos abaixo os resultados obtidos. Devido à restrição de espaço, apresentamos apenas os resultados referentes às métricas mais relevantes para cada padrão. Para o padrão **PU**, analisamos a quantidade *Retransmission Timeouts* (RTOs) do protocolo TCP durante as simulações. A Figura 1 mostra a taxa de envio agregada e a Função Distribuição Acumulada (FDA) da quantidade de RTOs de cada prioridade em cada cenário de DT. Cada FDA corresponde à proporção de tempo durante o qual o número correspondente de RTOs ocorreu. No cenário *Neutro*, as FDAs para ambas as prioridades foram similares. No cenário *Shaping*, o TPA não apresentou RTOs, enquanto o TPB teve pelo menos um RTO durante cerca de metade da simulação. No cenário *Policing*, o TPA pelo menos um RTO durante cerca de 10% do tempo de simulação, enquanto o TPB durante cerca de 25%.



(a) Taxa de envio (Mbps) do padrão PU.

(b) FDA no cenário *Neutro*.

(c) FDA no cenário *Shaping*.

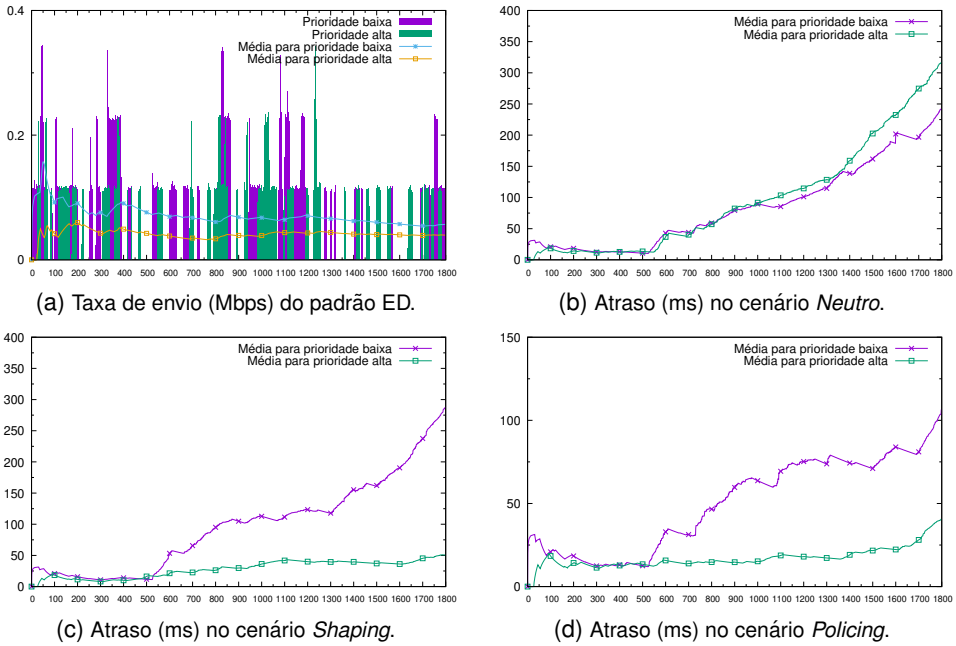
(d) FDA no cenário *Policing*.

Figura 1. Taxa de envio e FDAs do número de RTOs para o padrão PU.

Para o padrão **ED**, analisamos o atraso fim-a-fim. A Figura 2 mostra a taxa de envio agregada e o atraso fim-a-fim médio apresentado por pacotes de cada prioridade em cada cenário. O atraso fim-a-fim médio aumentou de forma similar para ambas as prioridades no cenário *Neutro* durante a simulação à medida que o TF aumentou. Nos outros dois cenários, no entanto, o atraso fim-a-fim médio aumentou significativamente mais para o TPB.

Para o tráfego **PE**, analisamos a taxa de transferência. No entanto, a taxa reservada (100 Kbps) não resultou em um impacto significativo para esta métrica. Assim, executamos nossas simulações novamente, empregando uma taxa reservada maior, 10% do link de saída, ou seja, 1 Mbps. A Figura 3 mostra a taxa de envio agregada e a taxa de transferência para cada prioridade em cada cenário. É possível observar que a taxa média para o TPA aumentou nos cenários *Shaping* e *Policing*, em relação ao cenário *Neutro*. Esse aumento é mais notável após os 1300 segundos de simulação, quando o TF atinge seu terceiro nível.

Discutimos abaixo o impacto da DT nos diferentes padrões de tráfego, com base nos



(a) Taxa de envio (Mbps) do padrão ED.

(b) Atraso (ms) no cenário *Neutro*.

(c) Atraso (ms) no cenário *Shaping*.

(d) Atraso (ms) no cenário *Policing*.

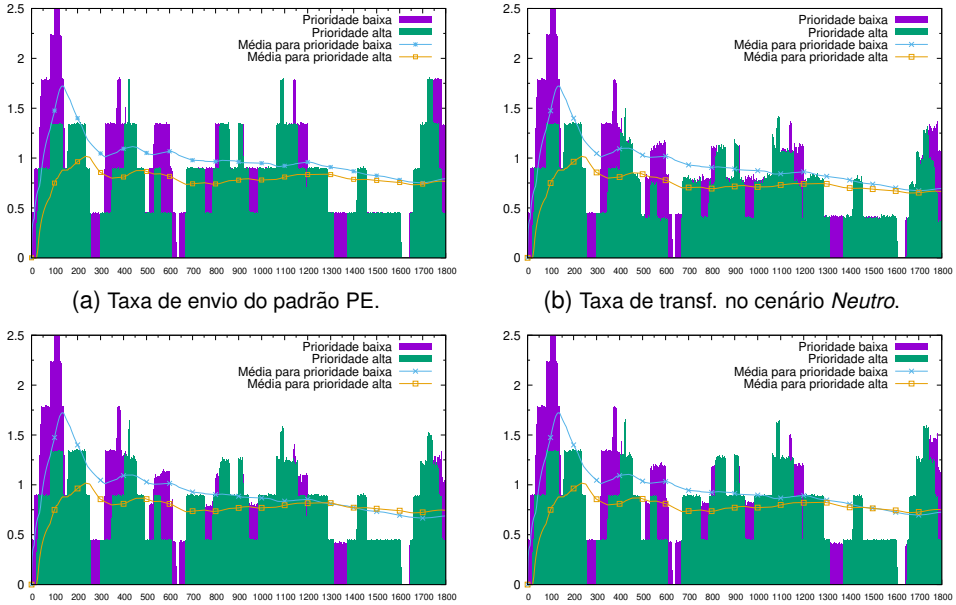
Figura 2. Taxa de envio e atraso fim-a-fim médio para ED durante os 1800s da simulação.

resultados obtidos. Os resultados mostram que mesmo uma pequena taxa reservada (1%) pode ser suficiente para criar uma diferença significativa na QoE percebida por usuários finais, o que pode resultar em concorrência desleal. No padrão **PU**, uma maior quantidade de retransmissões (devido a perda de pacotes) pode aumentar significativamente a quantidade de dados transmitidos em longos períodos de tempo. Assim, um dispositivo priorizado, por exemplo, pode apresentar um menor consumo de energia do que os concorrentes. Já no padrão **PE**, a DT pode ter um impacto significativo dependendo da aplicação. A diferença na taxa de transferência pode resultar em diferenças de QoE para *streaming* de vídeo, por exemplo.

Argumentamos que o padrão **ED** é o mais afetado pela DT, pois é importante que notificações em tempo real cheguem a tempo. Por exemplo, consideremos o seguinte cenário. Uma pessoa que dirige um carro inteligente está utilizando uma aplicação de navegação, a qual apresenta ao usuário a rota mais rápida até o destino desejado. Um eventual acidente na rota atual pode causar um engarrafamento. Em tal situação, o carro inteligente pode receber uma notificação sobre o acidente, fazendo com que o aplicativo de navegação forneça uma rota mais rápida ao usuário. Caso esta notificação atrase, o usuário já pode ter alcançado o engarrafamento ao recebê-la, momento no qual já pode ser impossível desviar. Assim, a DT pode resultar em melhores tempos de resposta na ocorrência de eventos para dispositivos e aplicativos priorizados. No exemplo acima, se o tráfego de dados de/para carros de um fabricante for priorizado em relação a outros, os atrasos menores podem causar uma diferença significativa de QoE, o que pode afetar a decisão do consumidor ao comprar um carro novo.

4. Conclusão

A priorização do tráfego de um fabricante ou provedor de serviços específico pode resultar em concorrência desleal, dificultando a inovação e, portanto, o sucesso da IoT. Neste artigo, estudamos o impacto da DT na IoT, no contexto de NR. Descrevemos os padrões mais comuns de tráfego na IoT encontrados na literatura e apresentamos resultados de simulação, mostrando como diferentes prioridades, para cada padrão de tráfego, comportaram-se em diferentes cenários de DT. Concluímos que mesmo uma priorização pequena pode resultar em uma diferença significativa na QoE percebida por usuários finais. Também concluímos



(a) Taxa de envio do padrão PE.

(b) Taxa de transf. no cenário *Neutro*.

(c) Taxa de transf. no cenário *Shaping*.

(d) Taxa de transf. no cenário *Policing*.

Figura 3. Taxas de envio e de transferência (Mbps) para PE durante os 1800s da simulação.

que o padrão ED é o mais afetado por DT, dada a sua natureza em tempo real.

Trabalhos futuros incluem a concepção de uma estratégia de monitoramento para detectar DT na IoT. Esta estratégia de monitoramento deve considerar os diferentes padrões de tráfego IoT e como eles são afetados pela DT. Destaca-se que as técnicas existentes para medir e detectar DT de HTC podem não ser adequadas para IoT. Além disso, a IoT fornece um ambiente prolífico para realizar medições relacionadas à NR. Pode ser possível aproveitar a grande quantidade de dispositivos para auxiliarem no próprio monitoramento.

Referências

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surveys Tuts.*, 17(4):2347–2376.

Dawy, Z., Saad, W., Ghosh, A., Andrews, J. G., and Yaacoub, E. (2017). Toward Massive Machine Type Cellular Communications. *IEEE Wireless Commun.*, 24(1):120–128.

Garrett, T., Dustdar, S., Bona, L. C. E., and Duarte Jr., E. P. (2017). Ensuring Network Neutrality for Future Distributed Systems. In *Int. Conf. Distributed Computing Systems (ICDCS)*, pages 1780–1786.

Garrett, T., Setenareski, L. E., Peres, L. M., Bona, L. C. E., and Duarte, E. P. (2018). Monitoring Network Neutrality: A Survey on Traffic Differentiation Detection. *IEEE Commun. Surveys Tuts.*, PP(99):1–1.

Nikaein, N., Laner, M., Zhou, K., Svoboda, P., Drajic, D., Popovic, M., and Krco, S. (2013). Simple Traffic Modeling Framework for Machine Type Communication. In *Int. Symp. Wireless Communication Systems*, pages 1–5.

Shafiq, M. Z., Ji, L., Liu, A. X., Pang, J., and Wang, J. (2012). A First Look at Cellular Machine-to-machine Traffic: Large Scale Measurement and Characterization. *SIGMETRICS Perform. Eval. Rev.*, 40(1):65–76.

Shin, D.-H. (2017). Conceptualizing and Measuring Quality of Experience of the Internet of Things: Exploring How Quality Is Perceived by Users. *Information & Management*, 54(8):998–1011.

Sivanathan, A., Sherratt, D., Gharakheili, H. H., Radford, A., Wijenayake, C., Vishwanath, A., and Sivaraman, V. (2017). Characterizing and Classifying IoT Traffic in Smart Cities and Campuses. In *IEEE Conf.Computer Communications Workshops (INFOCOM WKSHPS)*.