Descoberta de anomalias em dispositivos IoT usando Isolation Forest

Paulo Silas Severo de Souza, Wagner dos Santos Marques, Daniel Temp, Rumenigue Hohemberger, Fábio Diniz Rossi

[1]Instituto Federal Farroupilha (IF Farroupilha)
Campus Alegrete – RS – Brasil

{paulo.souza, wagner.marques}@email.com,

{daniel.temp, rumenigue.hohemberger, fabio.rossi}@iffarroupilha.edu.br

Abstract. *IoT environments can keep hundreds of geographically distributed sensors. Usually these sensors are not physically protected from unauthorized access. This means that such sensors can be compromised and manipulated to send incorrect data. In this paper, we propose the use of an anomalies detection algorithm, discovering sensors with different behavior compared to the others. The results showed that Isolation Forest can detect anomalous sensors at execution time, which allows the exclusion or verification of such sensor by the environment administrator.*

Resumo. *Ambientes IoT podem manter centenas de sensores geograficamente distribuídos. Geralmente, esses sensores não são fisicamente protegidos contra acesso não autorizado. Isso significa que tais sensores podem ser comprometidos, e manipulados a enviar dados incorretos. Neste artigo, propomos a utilização de um algoritmo de descoberta de anomalias, que descobre sensores com comportamento distinto em comparação com os demais. Os resultados mostraram que Isolation Forest consegue detectar sensores anômalos em tempo de execução, o que permite a exclusão ou verificação desse sensor pelo administrador do ambiente.*

1. Introdução

A popularização, miniaturização e o baixo custo de dispositivos eletrônicos, tais como sensores e atuadores, tecnologias de rede, e ambientes de larga escala como nuvens que podem armazenar e analisar uma grande quantidade de dados em tempo real, impulsionaram a área de Internet das Coisas (IoT - *Internet of Things*).

IoT [Gubbi et al. 2013] refere-se à implementação da comunicação máquina-para-máquina (M2M), e esse novo paradigma é entendido como uma infraestrutura de rede dinâmica, com capacidades de auto-configuração em tempo de execução, baseado em padrões de comunicação interoperáveis, onde "coisas" físicas e virtuais têm identidades, atributos, e personalidades, integradas dentro de uma rede de informações, frequentemente comunicando dados com usuários e seu ambiente.

Essas características fazem com que IoT seja uma proposta atraente para diversos domínios, visando saúde, segurança e sustentabilidade. Porém, tratando-se de um ambiente distribuído e heterogêneo, questões de segurança como integridade e autenticidade

devem ser levadas em consideração. Sensores, tanto podem enviar dados errados devido a alguma falha bizantina, quanto podem ter sido comprometidos e enviar dados errados com propósito bem específico de influenciar na análise dos dados pelos serviços de nuvem, que por consequência irão manipular atuadores de forma errônea.

A contribuição deste artigo consiste em utilizar um método computacional de aprendizagem de máquina chamado *Isolation Forest* [Liu et al. 2008] visando encontrar anomalias de padrões nos dados enviados pelos sensores IoT, e assim determinar quando um sensor está enviando valores muito diferentes de seus vizinhos. Caso o sensor anômalo seja detectado, este pode ser identificado para futura verificação. A escolha de *Isolation Forest* é devido ao fato deste ser um algoritmo de complexidade de tempo linear e baixo custo de memória, motivo que o torna ideal para análise de grandes quantidades de dados, que é uma característica de muitos ambientes IoT.

Este artigo está organizado da seguinte maneira: Na Seção 2 é apresentado um Referencial Teórico sobre Internet das Coisas e *Isolation Forest*; Na Seção 3 são listados alguns trabalhos relacionados; Na Seção 4 discutimos os resultados da aplicação do *Isolation Forest* sobre um conjunto de dados coletados em sensores IoT; e finalizamos na Seção 5 com nossas conclusões e trabalhos futuros.

2. Referencial Teórico

Nesta seção, são apresentados os conceitos fundamentais sobre o ambiente e a tecnologia empregadas nesse trabalho. A primeira parte apresenta a conceituação e taxonomia de IoT, seguido de uma discussão sobre *Isolation Forest* - o algoritmo de aprendizagem de máquina utilizado para analisar o conjunto de dados disponibilizado pelo ambiente de IoT.

2.1. Internet das Coisas

O alcance quase infinito da IoT ampliou o espectro de possibilidades de monitoria e atuação sobre os mais diversos ambientes. Isso deve-se ao aumento da capacidade e o baixo custo de sensores e plataformas de prototipação, que permitem o gerenciamento de várias métricas, desde pequenos sensores de temperatura até complexos objetos em uma cidade inteligente. A Figura 1 apresenta a interação dos componentes de um ambiente de IoT, onde sensores são analisados por serviços de nuvem, e a comunicação dos dados entre estes dois componentes é realizada através de rede.

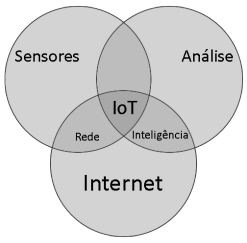

Figura 1. Inter-relação entre os componentes de um ambiente IoT.

IoT ainda é uma área em expansão, portanto uma classificação mais consistente sobre seus dispositivos e camadas ainda não existe. Entre as taxonomias aceitas, nós

utilizamos a baseada em [Busemann et al. 2012], que apresenta os sensores eletrônicos e sistemas embarcados como a primeira camada. Estes sensores e sistemas embarcados se comunicam com dispositivos de borda (*edge devices*) via rede, e por sua vez estes dispositivos enviam os dados recebidos dos sensores para ambientes de nuvem.

O envio dos dados dos dispositivos de borda para a nuvem, geralmente, não é síncrono, e é decidido através de políticas que primam por certas métricas como desempenho, economia de energia, etc. Os ambientes de nuvem, também chamados de AaaS (*Analytics-as-a-Service*) recebem os dados, analisam utilizando modelos estatísticos e intervêm novamente sobre o ambiente, gerenciando atuadores [Wang 2012].

Portanto, IoT pode ser entendido como um novo paradigma suportado pela ideia de ubiquidade, que permite que dispositivos independentes interajam entre si, permitindo tomada de decisão em tempo real, e automaticamente ajustando o ambiente dependendo da resposta de tais dispositivos. Porém, devido a distribuição geográfica dos sensores, a tarefa de verificação da integridade física destes não é uma tarefa trivial, e isso apresenta algumas ameaças e desafios endereçados neste trabalho.

2.2. Isolation Forest

Existem várias técnicas que permitem identificar dispositivos com algum tipo de falha ou comprometimento. Porém, a maioria delas é computacionalmente custosa, pois os algoritmos fazem uma leitura recursiva sobre todos os dispositivos, e em ambientes largamente distribuídos como IoT, pode se tornar uma tarefa impossível.

Isolation Forest [Liu et al. 2008] é uma técnica de aprendizagem de máquina que permite uma análise com complexidade de tempo linear e pouco uso de memória. Isso significa que no pior caso, o tempo acompanha o crescimento dos dados a serem processados, e pouco uso de memória também impacta indiretamente em desempenho.

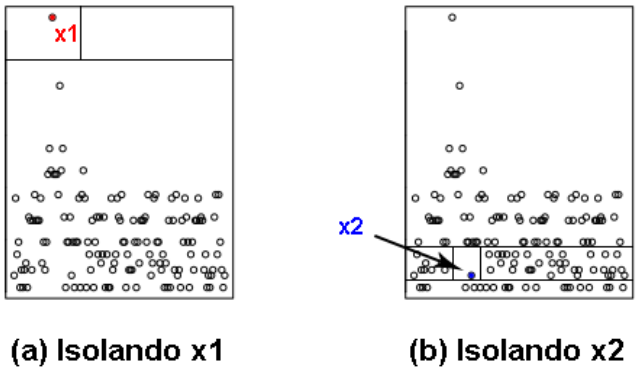

Figura 2. Particionamento de pontos: normal x anomalia.

Em nosso contexto, isolar significa separar uma instância dos resto das instâncias. Se levarmos em consideração que uma anomalia consiste em uma instância com comportamento diferente das demais, esta é mais suscetível ao isolamento. Anomalias apresentam duas características: são minoria dentro de um conjunto de dados; apresentam um valor ou atributo muito diferente das outras instâncias normais. Baseado nisso, *Isolation*

Forest cria árvores aleatórias de sub-conjuntos de dados, e as anomalias são isoladas mais perto da raiz, enquanto pontos normais são isolados mais profundamente na árvore.

Através do recurso de particionamento, o algoritmo ganha desempenho, pois não precisa percorrer todo o *dataset* para detectar instâncias anômalas. Além disso, problemas como efeitos de *masking* e *swamping*, que são ocasionados pela análise simultânea de grandes quantidades de dados, são evitados. *Masking* caracteriza-se pela existência de muitas instâncias anômalas, que induz o algoritmo a detectar estas como instâncias normais. Já o efeito de *swamping* ocorre quando instâncias normais são identificadas como anômalas. Tal efeito geralmente é ocasionado quando instâncias normais e anômalas estão muito próximas.

A Figura 2 mostra o particionamento de um ponto normal versus uma anomalia. Anomalias são mais suscetíveis ao isolamento e, portanto, têm comprimentos de trajeto curto. Dada uma distribuição de Gauss, (a) o ponto normal x1 requer doze partições aleatórias para ser isolado; (b) uma anomalia x2 requer apenas quatro. Sendo o particionamento recursivo representado por uma estrutura em árvore, a quantidade de partições necessárias para isolar um ponto é equivalente ao comprimento do percurso desde o nó raiz até o nó folha.

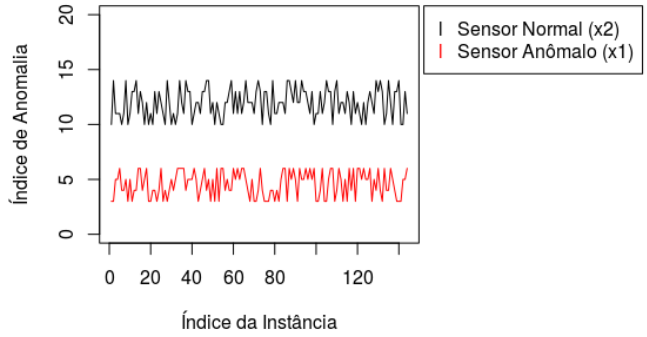

Figura 3. Convergência da média do comprimento dos caminhos.

Nós podemos ver na Figura 3 que a média dos tamanhos dos caminhos de x1 e x2 convergem quando a quantidade de árvores aumenta. Uma vez que cada partição é gerada aleatoriamente, árvores individuais são gerados com diferentes conjuntos de partições. Isso mostra que anomalias estão tendo comprimentos de percurso mais curto do que instâncias normais. Portanto, para problemas dimensionais que contêm um grande número de atributos irrelevantes, *Isolation Forest* pode alcançar um ótimo desempenho na detecção de anomalias.

3. Trabalhos Relacionados

Existe necessidade que os dados enviados por um dispositivo de IoT, como por exemplo sensores, tenham sua integridade garantida. Isso assegura que os dados foram realmente enviados pelo sensor indicado. Além de uma questão de integridade, esse controle consiste em uma questão de autenticidade e privacidade. Quanto a isso, várias solução são propostas [Dunn et al. 2012] [Tang et al. 2012]. Tais soluções podem ser consideradas bastante úteis nos cenários atuais. Porém, muitas destas soluções são baseadas em

revogação de dados [Peterson et al. 2005], que consiste em eliminar todo o conjunto de dados comprometido. Baseado nisso, existem várias técnicas de revogação de dados propostas na criptografia clássica [Boneh and Lipton 1996] [Shafagh et al. 2015], e a maioria delas se baseia na ideia de que, caso uma chave de codificação não possa mais ser acessada, todo o conjunto de dados deve ser excluído.

No entanto, em ambientes IoT, onde existe uma grande quantidade de dados obtidos através de sensores, é plausível esperar que embora o ambiente esteja comprometido, a maioria dos dados advindos dos sensores ainda contenham informações úteis e válidas. Alguns trabalhos propõem o desenvolvimento *frameworks* seguros que incluem mecanismos de segurança para cada camada de um ambiente de IoT [Rahman et al. 2016]. Outros trabalhos implementam segurança diretamente no canal de comunicação entre os dispositivos que compõem o ambiente de IoT [Ukil et al. 2013].

Diferentemente dos trabalhos anteriores, nossa proposta visa utilizar aprendizagem de máquina [Manadhata 2015] com o objetivo de analisar questões de segurança nos dados enviados por sensores em um ambiente de IoT. Alguns trabalhos já se utilizam desse tipo de técnica para endereçar tais questões, como em [Bovet et al. 2014] [Shahriar and Rahman 2015]. Porém, a maioria deles utiliza aprendizagem de máquina sobre séries estáticas de dados. Nossa proposta avalia uma série temporal, em que os dados são enviados em intervalos de tempo síncronos, e analisados em tempo real. Esse é o motivo de utilizarmos *Isolation Forest*, pois é a técnica com melhor desempenho entre todas as outras disponíveis.

4. Cenário e Avaliações

Foram analisados sensores de temperatura instalados em celeiros para armazenamento de grãos. A escolha deste cenário justifica-se pela importância representada pela etapa de armazegem sobre o processo de produção agrícola. Neste contexto, o controle eficiente da umidade é essencial, pois tal propriedade afeta diretamente na qualidade dos grãos. Salienta-se que oscilações de temperatura podem ocasionar o acúmulo de umidade em determinadas regiões do celeiro, favorecendo o desenvolvimento de fungos, insetos, e outros organismos responsáveis pela deterioração dos grãos. Assim, percebe-se a relevância do controle climático nestes ambientes [Citolin 2012].

O *dataset* utilizado na avaliação é composto por dados advindos de 100 sensores que informam a temperatura do celeiro a cada 5 minutos, através de sinais *wireless*. Inicialmente, foram analisadas 12h de medição, que geraram 14400 instâncias (144 de cada sensor). Sensores normais mantiveram-se entre 30ºC e 32ºC. Dois sensores foram configurados para comportar-se de forma anômala: um durante toda a medição (mantendo-se entre 14ºC e 20ºC), e outro somente na 3ª hora (com temperaturas entre 46ºC e 50ºC). O algoritmo conseguiu detectar as anomalias presentes nestes dois sensores. Tal eficácia é resultado do particionamento do conjunto total de dados realizado pelo *Isolation Forest*, formando modelos parciais. Isto permite a detecção de anomalias analisando somente parte dos dados, o que aumenta o desempenho e evita falhas como os efeitos de *masking* e *swamping*.

O processo de análise foi dividido em duas etapas: (i) busca por sensores que apresentaram somente comportamento anômalo, conforme exposto na Figura 4(a); e (ii) busca por sensores que mostraram anomalia somente em determinados momentos (reali-

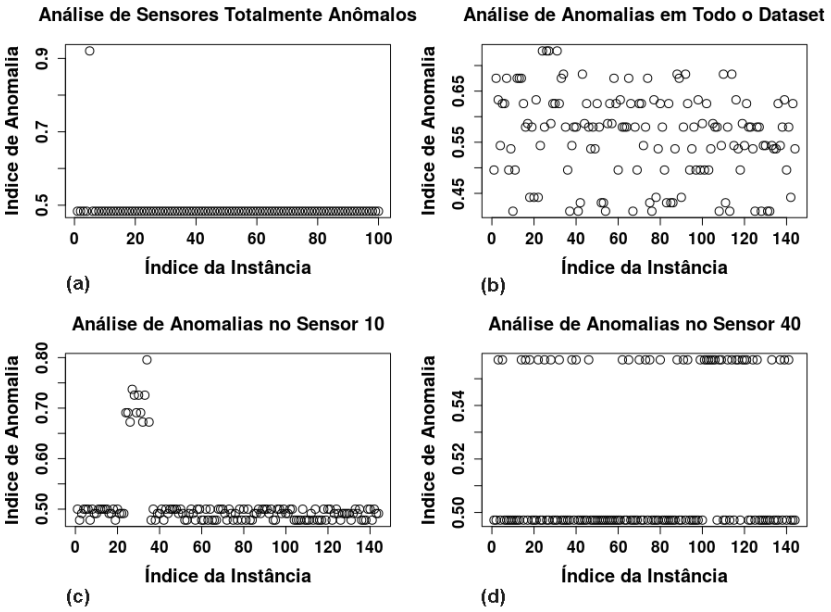

Figura 4. Representação da análise de anormalidade nas instâncias, sob diferentes perspectivas. Os gráficos (a) e (b) mostram análises gerais, ao passo que os itens (c) e (d) expõem verificações por anomalias em sensores específicos.

zada individualmente, sensor por sensor), conforme exemplificado nos itens (c) e (d) da Figura 4. Os sensores 10 (que demonstrou comportamento anômalo na 3ª hora) e 40 (que teve comportamento normal) foram escolhidos para exemplificar a análise por sensores parcialmente anômalos. Salienta-se que um conjunto de dados pode ser considerado normal caso todas suas instâncias apresentem índice de anomalia próximo de 0.5, como no caso do sensor 40 [Liu et al. 2008].

Tabela 1. Análise do tempo de execução do algoritmo em relação a *datasets* de diferentes tamanhos.

Número de Sensores	Instâncias por Sensor	Tempo de Execução
100	144	0.001s
1.000	144	0.002s
5.000	144	0.013s
10.000	144	0.036s
20.000	144	0.046s
40.000	144	0.100s

Também foram realizados testes de desempenho a fim de verificar o tempo de execução do algoritmo em diferentes cenários. Foram usados *datasets* com 100, 1.000, 5.000, 10.000, 20.000 e 40.000 sensores, tendo cada um destes 144 instâncias. Os testes demonstraram a linearidade do desempenho do *Isolation Forest* nestes conjuntos de

dados, como ilustrado na Tabela 1.

Os resultados mostraram que *Isolation Forest* pode mostrar sensores com comportamento anômalo, além de apresentar desempenho, no pior caso, compatível com o incremento no tamanho dos dados. Isso mostra que essa técnica apresenta uma grande vantagem para análises em ambientes IoT.

5. Conclusões e Trabalhos Futuros

IoT são ambientes largamente distribuídos, heterogêneos, com novas características que trazem grandes desafios para a área de segurança. Especificamente quanto à integridade dos dados que trafegam entre os dispositivos, a segurança ainda não é um requisito fundamental. Como sistemas de gerenciamento dos ambientes de IoT podem modificar o ambiente através da manipulação de atuadores, os dados advindos dos sensores devem ser confiáveis. Por exemplo, um ataque sobre sensores de umidade e temperatura em uma plantação, podem interferir diretamente sobre a decisão em sistemas de irrigação, e impactar na produtividade. IoT para eHealth [Abie and Balasingham 2012] é uma área ainda mais sensível no contexto de ataque a sensores que irão decidir como atuadores devem se comportar.

Portanto, a contribuição deste trabalho consiste em utilizar uma técnica de aprendizagem de máquina chamada *Isolation Forest* visando identificar dispositivos com comportamento anômalo, que possam estar enviando dados errados ao serviço de gerenciamento do ambiente. O algoritmo conseguiu detectar a presença dos dispositivos completamente ou parcialmente anômalos. Além disso, os testes mostraram o desempenho linear do *Isolation Forest* mediante análise de *datasets* com diferentes tamanhos. Com isto, constatou-se a relevância do uso deste algoritmo na detecção de anomalias em ambientes IoT. Como trabalhos futuros, nós pretendemos melhorar o algoritmo para suportar de maneira mais eficiente séries temporais com múltiplas dimensões.

Referências

Abie, H. and Balasingham, I. (2012). Risk-based adaptive security for smart iot in ehealth. In *Proceedings of the 7th International Conference on Body Area Networks*, BodyNets '12, pages 269–275, ICST, Brussels, Belgium, Belgium. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Boneh, D. and Lipton, R. J. (1996). A revocable backup system. In *Proceedings of the 6th Conference on USENIX Security Symposium, Focusing on Applications of Cryptography - Volume 6*, SSYM'96, pages 9–9, Berkeley, CA, USA. USENIX Association.

Bovet, G., Ridi, A., and Hennebert, J. (2014). Virtual things for machine learning applications. In *Proceedings of the 5th International Workshop on Web of Things*, WoT '14, pages 4–9, New York, NY, USA. ACM.

Busemann, C., Gazis, V., Gold, R., Kikiras, P., Kovacevic, A., Leonardi, A., Mirkovic, J., Walther, M., and Ziekow, H. (2012). Enabling the usage of sensor networks with service-oriented architectures. In *Proceedings of the 7th International Workshop on Middleware Tools, Services and Run-Time Support for Sensor Networks*, MidSens '12, pages 1:1–1:6, New York, NY, USA. ACM.

Citolin, R. S. (2012). Sistema de termometria para silos.

Dunn, A. M., Lee, M. Z., Jana, S., Kim, S., Silberstein, M., Xu, Y., Shmatikov, V., and Witchel, E. (2012). Eternal sunshine of the spotless machine: Protecting privacy with ephemeral channels. In *Proceedings of the 10th USENIX Conference on Operating Systems Design and Implementation*, OSDI'12, pages 61–75, Berkeley, CA, USA. USENIX Association.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013). Internet of things (iot): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.*, 29(7):1645–1660.

Liu, F. T., Ting, K. M., and Zhou, Z.-H. (2008). Isolation forest. In *Proceedings of the 2008 Eighth IEEE International Conference on Data Mining*, ICDM '08, pages 413–422, Washington, DC, USA. IEEE Computer Society.

Manadhata, P. K. (2015). Machine learning for enterprise security. In *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security*, AISec '15, pages 1–1, New York, NY, USA. ACM.

Peterson, Z. N. J., Burns, R., Herring, J., Stubblefield, A., and Rubin, A. D. (2005). Secure deletion for a versioning file system. In *Proceedings of the 4th Conference on USENIX Conference on File and Storage Technologies - Volume 4*, FAST'05, pages 11–11, Berkeley, CA, USA. USENIX Association.

Rahman, A. F. A., Daud, M., and Mohamad, M. Z. (2016). Securing sensor to cloud ecosystem using internet of things (iot) security framework. In *Proceedings of the International Conference on Internet of Things and Cloud Computing*, ICC '16, pages 79:1–79:5, New York, NY, USA. ACM.

Shafagh, H., Hithnawi, A., Droescher, A., Duquennoy, S., and Hu, W. (2015). Talos: Encrypted query processing for the internet of things. In *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*, SenSys '15, pages 197–210, New York, NY, USA. ACM.

Shahriar, M. S. and Rahman, M. S. (2015). Urban sensing and smart home energy optimisations: A machine learning approach. In *Proceedings of the 2015 International Workshop on Internet of Things Towards Applications*, IoT-App '15, pages 19–22, New York, NY, USA. ACM.

Tang, Y., Ames, P., Bhamidipati, S., Bijlani, A., Geambasu, R., and Sarda, N. (2012). Cleanos: Limiting mobile data exposure with idle eviction. In *Proceedings of the 10th USENIX Conference on Operating Systems Design and Implementation*, OSDI'12, pages 77–91, Berkeley, CA, USA. USENIX Association.

Ukil, A., Bandyopadhyay, S., Bhattacharyya, A., and Pal, A. (2013). Lightweight security scheme for vehicle tracking system using coap. In *Proceedings of the International Workshop on Adaptive Security*, ASPI '13, pages 3:1–3:8, New York, NY, USA. ACM.

Wang, H. W. (2012). Integrity verification of cloud-hosted data analytics computations. In *Proceedings of the 1st International Workshop on Cloud Intelligence*, Cloud-I '12, pages 5:1–5:4, New York, NY, USA. ACM.