Assinatura Comportamental e Detecção de Anomalias Utilizando *K-means*

Wagner Senger
Universidade Tecnológica Federal do Paraná
Ponta Grossa-PR, Brasil
wagnersenger@gmail.com

Lourival Aparecido de Góis
Universidade.Tecnológica Federal do Paraná
Ponta Grossa-PR, Brasil
gois@utfpr.edu.br

RESUMO

Neste artigo é descrito um método de caracterização do padrão de comportamento de um recurso computacional utilizando o algoritmo de clusterização *k-means*. Através da coleta dos dados de utilização dos componentes internos de um recurso por uma janela de tempo, um elemento denominado Assinatura Comportamental é criado, o qual neste artigo é gerada através da analise do *cluster* executada pelo algoritmo *k-means*. O referido modelo que ainda é um trabalho em andamento apresenta uma abordagem diferenciada de outros modelos onde outros algoritmos são aplicados no seu lugar ou além do próprio algoritmo são utilizadas técnicas complementares em conjunto. A expectativa é criar um formado mais simples e leve, que passe por uma única etapa de processamento, diferente de outros métodos que necessitam de duas ou mais para se determinar a Assinatura Comportamental.

Palvras-chave

k-means, clusterização, detecção de anomalias, padrões de comportamento, assinatura comportamental

ABSTRACT

In this paper we describe a method to characterize a computacional resource behavior pattern using the clusterizing algorithm k-means. By collecting usage data from the resource's internal components in a time window, a element denominated Behavior Signature is created, that in this paper is generated through the cluster's analisis generated by the algorithm k-means. The current model is still a work in progress, and shows a different aproach of others models where another algorithms are applyed in his place or some other technics are used togheter it. The main focus is create a more simple and fast format, in a single step, differing from others who needs two or more steps to determine the Behavior Signature.

WPCCG '17 Outubro, 2017, Ponta Grossa, Paraná, Brasil
.

keywords

k-means, clusterizing, anomaly detection, behavior's pattern, bahavior's signature

1. INTRODUÇÃO

Áreas da computação que utilizam vários recursos computacionais com características diferentes como Grades Computacionais, Computação em Nuvem e Redes de Computadores entre outras, têm mudado a forma como estes equipamentos são utilizados. Seus funcionamentos proporcionam usos flexíveis de recursos e armazenamentos, permitindo que usuários evitem gastos excessivos com investimentos e manutenções [6].

Não somente nestas áreas, mas também sistemas que funcionam através de *Internet of Things* (IoT), a qual tem ganho muito espaço pelo crescimento dos dispositivos móveis, precisam de abordagens que promovam o crescimento da segurança através de mecanismos de detecção de uso indevido de equipamentos, já que frequentemente são expostos a ambientes hostis e inseguros [9].

Dentro desta perspectiva se faz necessário conhecer como cada recurso se comporta durante um período normal de utilização. Para esta finalidade é necessário inferir um padrão de comportamento para que através dele então se possa detectar uma possível anomalia no seu uso, sendo ela causada simplesmente por uma requisição de uso acima do comum ou então por uma falha parcial ou total no equipamento.

Alguns mecanismos de estabelecimento de padrões e detecção de anomalias ja têm sido avaliados e, neste artigo é proposta a criação de um novo mecanismo utilizando um algoritmo de clusterização que já é amplamente difundido principalmente na área de *Data Mining*, o *k-means* [10].

Este artigo está dividido em 3 seções, sendo a primeira abordando métodos correlatos de criação de padrões. Na segunda seção é demonstrada a metodologia proposta e a forma como o algoritmo é aplicado, bem como os resultados esperados, e na terceira as conclusões sobre o método.

2. TRABALHOS RELACIONADOS

Diferentes formas de identificação do padrão de comportamento de recursos já foram propostas, e em várias áreas elas têm suas aplicações testadas e validadas. É perceptível que este tema ainda instiga muitas outras pesquisas e aplicações, pois várias são as formas de se obter o resultado.

Em [5], os autores abordam três algoritmos para análise do fluxo de dados de rede dos recursos e criar o que foi chamado de "assinatura digital", a qual demonstra em um gráfico o

comportamento de um recurso ao longo do tempo. Os algoritmos utilizados foram o *Ant Colony Optimization* (ACO), *Holt-Winters*(HW) e *Principal Component Analysis*(PCA) e, após aplicados ao processo, avaliados os resultados. Os três algoritmos tiveram resultados muito próximos, e em parte do trabalho a complexidade de cada algoritmo e o volume de dados foi um diferencial entre eles, porém todos se mostraram suficientemente eficientes para serem aplicados em um ambiente de *cloud computing*.

Em [3] os mesmos algoritmos citados anteriormente foram testados na área de saúde e então houve uma diferença acentuada nos resultados, onde o PCA demonstrou uma maior efetividade tanto para caracterização do tráfego quanto para a detecção de anomalias.

Um trabalho que também utiliza clusterização como parte do método de identificação de anomalias foi descrito em [8], onde os autores utilizaram o algoritmo *k-means* para identificação de um padrão nos dados, porém, este foi aplicado em conjunto com um modelo denominado *Hidden Markov Model*(HMM), onde dados clusterizados pelo *k-means* eram fornecidos como entrada para este modelo, o qual calculava uma probabilidade e precisão para os dados fornecidos. Se a precisão calculada fosse maior que a dos dados já conhecidos então é decidido que os dados recebidos e o padrão conhecido combinam, sendo assim adicionados ao modelo de treinamento do algoritmo.

Em [1] a abordagem para determinar o padrão utiliza *Recurrent Neural Networks*(RNN), a qual é amplamente utilizada para detecção de padrões e, através de refinamentos sucessivos um padrão é estabelecido. Seu conceito considera que se sucessivos treinamentos geram um padrão refinado, o treinamento em dados já classificados pode reduzir o tempo necessário de treinamento, encaixando desta forma o RNN.

Na área de sensores sem fio, é proposto em [11] a criação de um módulo específico para detecção de anomalias, pois segundo o autor, em equipamentos que possuem poucos recursos de processamento, uma arquitetura de detecção de anomalias em tempo real pode necessitar de mais recursos do que o equipamento pode prover, prejudicando por sua vez o funcionamento normal do dispositivo.

A descoberta de padrões pode ser aplicada de várias maneiras em ambientes diferentes e ainda assim obter um resultado de alta qualidade, por isso, considerando estes estudos, neste artigo a abordagem proposta com o algoritmo *k-means* será aplicada de uma maneira diferenciada que será detalhada mais a frente, a fim de futuramente ser possível uma aplicação e testes de seu método.

3. METODOLOGIA

Durante o ciclo de vida de um recurso computacional, é comum que alterações na intensidade de uso ocorram, e mais que isso, ocorram de forma cíclica durante o tempo.

Em sistemas que funcionam em horário comercial por exemplo, desconsiderando processos externos como backup e movimentações de dados, entre outros, a maior carga de requisições recebidas se concentra dentro deste horário, havendo ainda uma possível diminuição durante o almoço. Com o tempo se torna possível prever que os recursos estarão com uma maior disponibilidade no almoço e fora do horário comercial, então, quando um recurso estiver com sua utilização fora desse padrão, existe a possibilidade de algo não estar em conformidade.

Ao se controlar o fluxo de dados de um equipamento, o termo ”anomalia do fluxo” dado a um período em que um ele se encontra fora do seu uso normal é bem difundida e cobre qualquer desvio das características do fluxo normal de um recurso [7], incluindo tráfego malicioso como ataques de *Distributed Denial-Of-Service* (DDoS), ou que utilize uma quantidade incomum da banda disponível ou ainda, o aumento natural da demanda sobre um determinado serviço.

Esta métrica de predição de comportamento é nomeada normalmente como ”tráfego normal” ou ”uso comum” de um recurso, sendo também referida como Assinatura Digital em alguns estudos [5] [3]. Devido a esta última nomenclatura possuir uma referência muito próxima às assinaturas de documentos eletrônicos, neste documento ela será definida como Assinatura Comportamental.

A referida Assinatura Comportamental permite que através de uma representação gráfica um operador possa visualizar o comportamento de um recurso computacional ao longo do tempo e, além disso, permite que um sistema através dela possa determinar o que é um comportamento comum e o que é uma anomalia. Este comportamento se refere ao uso de cada componente do recurso, podendo ser ele de processamento, rede, memória, armazenamento, etc. A definição de uma Assinatura Comportamental para um recurso é importante para que se determine um padrão, e com o tempo seja possível prever como ele irá se comportar em um determinado horário de funcionamento.

Para determinar a Assinatura Comportamental do recurso computacional é necessário que os dados de utilização de seus componentes seja monitorada constantemente. A estratégia de monitoramento pode variar de acordo com a aplicação do método, podendo inserir os registros diretamente em um banco de dados ou simplesmente armazenando em um arquivo texto, sendo o intervalo de medição dos recursos variável de acordo com necessidade. Estes dados coletados são fornecidos como entrada para o algoritmo de clusterização *k-means*, o qual agrupa os valores e determina qual o padrão de utilização.

Como citado anteriormente, os recursos possuem uma utilização padrão para um determinado horário do dia, e além disso também possuem uma utilização diferenciada para cada dia da semana, podendo possuir um nível inferior em finais de semana ou feriados. Por isso é necessário que os dados avaliados sejam sempre comparados de acordo com o dia e horário em que ocorreram, por exemplo, o uso de memória de uma segunda-feira das 6h25m40s as 6h25m46s somente sera comparada com este mesmo intervalo de tempo, evitando a comparação de horário com um final de semana. Nesta janela de tempo os dados coletados durante um período serão juntos analisados para se determinar o padrão.

Para o algoritmo *k-means* é necessário informar o número de *clusters* que se deseja gerar, isso é referenciado pela letra k do seu nome, que é uma variação inferida pela necessidade de cada aplicação [2]. Os dados enviados para análise são aqueles agrupados na janela de tempo citada acima, e o número de *clusters* ideais para a definição do padrão pode variar para cada situação, por isso testes de refinamento são necessários afim de aperfeiçoar a precisão.

Para exemplificar o processo, na Fig. 1 é demonstrado uma coleta fictícia de um recurso computacional, demonstrando a leitura do percentual de uso de um dos componentes, como o processador, em relação ao tempo. Separando uma janela de tempo dessa amostra para análise como demonstrado na Fig. 2 pela área demarcada em verde, é possí-

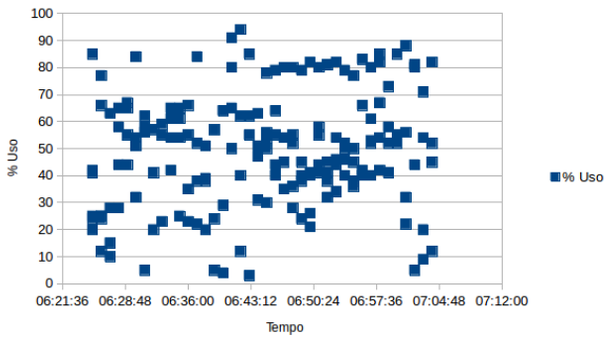

Figure 1: Coleta fictícia de dados do uso de um recurso.

vel perceber que a grande maioria dos valores encontram-se entre 30% e 65%.

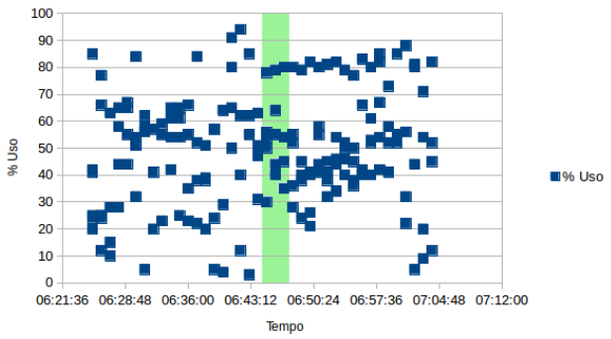

Figure 2: Janela de tempo da amostra e *cluster* com mais registros.

O algoritmo *k-means* recebendo os dados desta janela calcula um centroide para o número de *clusters* solicitados, e a partir dele os registros que possuem uma similar proximidade a ele passam a ser agrupados. A partir disto, sendo solicitado dois *clusters* ao algoritmo, o resultado de um procedimento de clusterização executado deve gerar os *clusters* como pode-se perceber na Fig. 3. Neste processo o que será levado em consideração como funcionamento padrão do recurso será o *cluster* com maior número de leituras registradas, no caso do exemplo abaixo o *cluster* vermelho possui grande parte dos registros, portanto será considerado como o padrão do recurso monitorado.

Tendo detectado o *cluster* com o funcionamento padrão do recurso pode-se passar para uma segunda etapa que é a de eliminação dos registros intermediários desta janela selecionada. Neste *cluster* haverá um registro em cada extremo, acima e abaixo, ou seja, permanecerão para análise o registro que estiver o percentual de uso mais alto e também o registro com percentual mais baixo dentro deste *cluster* selecionado, e estes limites irão determinar qual é a margem normal de funcionamento do recurso, sendo para o exemplo anterior de aproximadamente entre 30% es 65%.

Existe a possibilidade de algumas das leituras não serem incorporadas aos *clusters* gerados, dentro de um processo de clusterização estes elementos recebem o nome de *outliers*, ou ruídos, que são elementos que possuem uma natureza

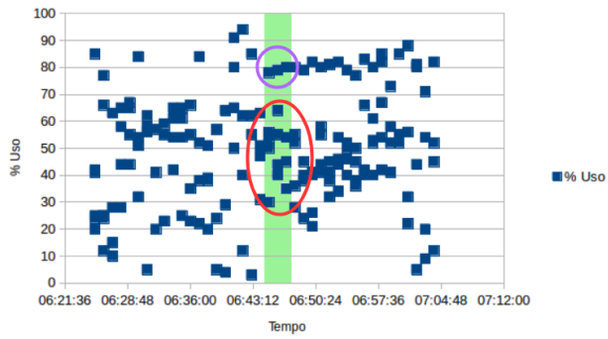

Figure 3: Clusters gerados na janela de tempo selecionada.

incerta, apresentam um comportamento inesperado ou então propriedades anormais [4], por isso não se enquadram em nenhum dos agrupamentos. Estas leituras são comuns, pois dentro do ciclo de operação de um recurso existem picos ou quedas de processamento momentâneas que podem ocorrer.

Após passar por todas as janelas do intervalo de tempo e processar os dados, serão identificados todos os registros de limite acima e abaixo dos *clusters*, que traçarão a margem de funcionamento normal do recurso computacional, ou no caso como definido anteriormente, a Assinatura Comportamental. Este resultado pode ser visto na Fig. 4.

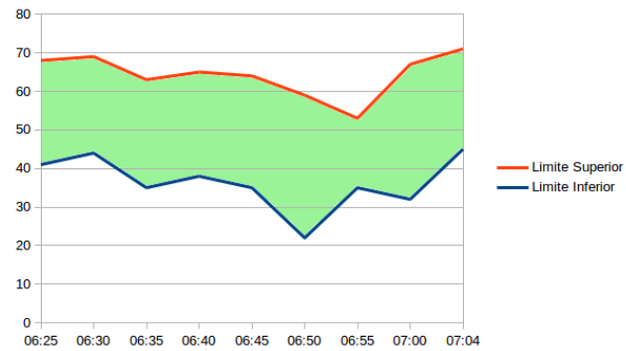

Figure 4: Assinatura Comportamental do recurso computacional.

Dentro da área de detecção de anomalias, graficamente esta Assinatura Comportamental pode servir como base para análise de um comportamento por um operador, porém para um sistema é necessário que seja levado em consideração um pouco mais do que simplesmente observar se uma leitura está dentro ou fora da margem de operação.

Como citado anteriormente, é possível que picos de execução apareçam no decorrer do ciclo de operação de um recurso, por isso não é correto avaliar uma leitura isoladamente, visto que até mesmo a Assinatura Comportamental é composta de vários registros de leituras.

Na Fig. 5 pode-se perceber que algumas das leituras não se enquadram na Assinatura Comportamental do recursos, porém isso não é motivo suficiente para determinar que um recurso está com seu funcionamento fora do padrão. Nesta figura existem dois pontos isolados fora da Assinatura, um laranja e outro preto, os quais representam picos naturais do

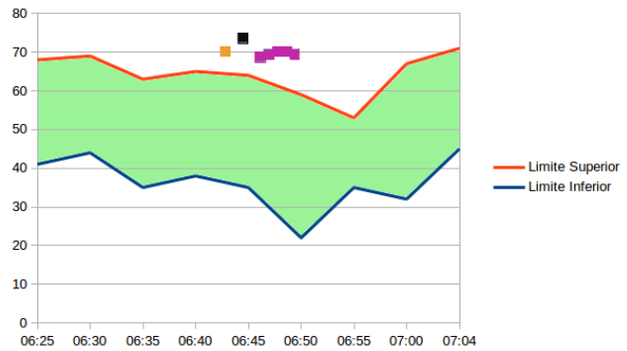

Figure 5: Assinatura Comportamental comparada a *outliers*.

processamento do recurso e neste sentido devem ser compreendidos apenas como ocorrências extraordinárias ao comportamento. Porém existe uma sequência de leituras em rosa que podem ser um indício de uma anormalidade no funcionamento do recurso, visto que estas além de estarem a mais tempo no mesmo nível de processamento, também atravessam mais de uma janela de leitura processada anteriormente.

Dentro desta abordagem é possível que um sistema analise o comportamento de um recurso, identifique e gere um padrão para o seu funcionamento natural e também faça análise em tempo real de alguma anomalia, o que permite que não somente problemas de aumento anormal de uso de recursos sejam analisados e reportados, como também quedas de equipamentos.

Não são somente anomalias acima da Assinatura Comportamental que são nocivas ao funcionamento de um sistema, a diminuição anormal do uso dos recursos pode denotar uma queda em algum serviço ou componente, fato que em determinados casos pode ser ainda mais impactante para os usuários.

4. CONCLUSÃO

Vários são os métodos dentro da detecção de anomalias e definição do comportamento padrão de recursos, e neste artigo se apresenta uma abordagem diferenciada, a qual oferece uma métrica para determinar uma área possível de utilização de um recurso e estabelecê-la como comum, através da Assinatura Comportamental, assim como a sua criação de um método de etapa única através da aplicação do algoritmo *k-means*.

Com esta Assinatura, se torna possível perceber mais claramente qual é a faixa em que o equipamento trabalha e também predizer com base em um histórico anterior qual será a faixa em que ele estará em um determinado momento, possibilitando ações de melhoria ou ainda de incentivo de utilização de momentos em que o serviço se encontra com o uso em baixa.

Os resultados do modelo poderão ser avaliados através da averiguação da Assinatura Comportamental criada e a sua moldagem referente ao fluxo de uso normal do sistema, assim permitindo detectar momentos de utilização fora do padrão, e ainda averiguar se esta apresenta alertas que não condizem com uma utilização regular, ou seja, falsos positivos para uma anomalia. Poderá ser considerada como uma boa alternativa se os níveis de falso positivos forem inferiores aos apresentados em outros estudos aplicados nesta área.

Apesar de testes ainda não terem sido executados com a metodologia, o algoritmo aplicado já é de ampla utilização em áreas como *Data Mining* e Grades Computacionais, por tanto se espera um resultado satisfatório tanto de desempenho quanto de qualidade de resultados.

5. REFERÊNCIAS

[1] A. Bhattacharyya, S. A. J. Jandaghi, S. Sotiriadis, and C. Amza. Semantic aware online detection of resource anomalies on the cloud. In *2016 IEEE 8th International Conference on Cloud Computing Technology and Science*. IEEE, January 2017.

[2] P. S. Bradley and U. M. Fayyad. Refining initial points for k-means clustering. pages 91–99. Morgan kaufmann, 1998.

[3] L. F. Carvalho, G. F. Jr., M. V. O. de Assis, J. J. P. C. Rodrigues, and M. L. P. Jr. Digital signature of network segment for healthcare environments support. In *15th International Conference On E-Health Networking, Application & Services*, pages 299–309. IEEE, October 2014.

[4] F. Jiang, Y. Sui, and C. Cao. An information entropy-based approach to outlier detection in rough sets. *Expert Systems with Applications*, 37:6338–6344, September 2010.

[5] M. L. P. Jr., G. F. Jr., and L. F. Carvalho. Digital signature to help network management using flow analysis. *International Journal of Network Management*, 26:76–94, May 2015.

[6] C.-Y. Lin, Y.-A. Chen, Y.-C. Tseng, and L.-C. Wang. A flexible analysis and prediction framework on resource usage in public clouds. *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, pages 309–316, February 2013.

[7] J. Moraney and D. Raz. Efficient detection of flow anomalies with limited monitoring resources. In *2016 12th International Conference on Network and Service Management (CNSM)*. IEEE, January 2017.

[8] Y. Ohno, M. Sugaya, A. van der Zee, and T. Nakajima. Anomaly detection system using resource pattern learning. In *2009 Software Technologies for Future Dependable Distributed Systems*. IEEE, January 2009.

[9] H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri. A lightweight anomaly detection technique for low-resource iot devices: A game-theoretic methodology. In *2016 IEEE International Conference on Communications (ICC)*. IEEE, May 2016.

[10] P.-N. Tan, M. Steinbach, and V. Kumar. *Introduction to Data Mining*. Pearson Addson-Wesley, 2006.

[11] M. Usman. Agent-enabled anomaly detection in resource constrained wireless sensor networks. In *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, Jun 2015.