FACULDADE DE TECNOLOGIA DA ZONA LESTE
ANÁLISE E DESENVOLVIMENTO DE SISTEMAS
METODOLOGIA DE PESQUISA CIENTÍFICO-TECNOLÓGICA

Bruno Bega Harnik - RA: 1110481823052
Fernanda Pinheiro Reis - RA: 1110481823022
Luiz Fernando Geraldo dos Santos - RA: 1110481823051

SÃO PAULO
2020

Artigo 1 - Design of Single-Sided Linear Induction Motor (SLIM) for Magnetic Levitation Railway Transportation

O artigo aborda os motores de indução lineares, seu funcionamento e sua aplicação no mercado. Diz que esse tipo de motor é equivalente ao motor de rotação, com a diferença de que é "cortado e alongado".

O principal objetivo do ensaio é observar um exemplar em tamanho reduzido, de laboratório, para fins educacionais.

Esse tipo de motor é bastante utilizado em sistemas de grande escala, como sistemas de transporte, manipulação e armazenamento de materiais em almoxarifado, transporte de passageiros, bombeamento de metal líquido, lançadores e aceleradores, operações de maquinário pesado, sistema aeroportuário de bagagens, entre muitos outros.

Esse tipo de motor parte do princípio de que são motores de indução rotativa, só que cortados e desenrolados, ou seja, sua indução dessa forma é longitudinal.

Os autores abordam no texto especificações técnicas sobre os componentes mecânicos dos motores e chegam à conclusão de que os vãos de ar são muito importantes para esse tipo de motor: Esses vãos precisam ser os menores possíveis para ter mais segurança e eficiência. A grossura do rotor também é muito importante, ao passo que quanto mais espesso é o imã, maior é o impulso e maior é o tamanho do vão de ar entre os ímãs, o que é indesejável. O autor fez uma experimentação teórica e também não abordou modelo de levitação e de regeneração.

A citação do artigo está descrita a seguir:

Min Min Oo. **Design of Single-Sided Linear Induction Motor (SLIM) for Magnetic Levitation Railway Transportation. International Journal of Systems Science and Applied Mathematics.** Vol. 3, No. 1, 2018, pp. 1-9. doi: 10.11648/j.ijssam.20180301.11

O autor seguiu corretamente as regras impostas pelo International Journal of Systems Science and Applied Mathematics para elaboração de artigos.

Artigo 2 - Availability and Reliability Analysis for Dependent System with Load-Sharing and Degradation Facility

Este artigo trata sobre disponibilidade e confiabilidade no processo de compartilhamento de cargas e facilidade de degradação em sistemas dependentes. Dois componentes interdependentes possuem facilidade de degradação onde o compartilhamento de carga é introduzido.

O sistema é composto por dois componentes conectados em paralelo e quando da falha em um componente ocorre falha no outro. As falhas e reparos são constantes ao passo que ambos os componentes são interdependentes e seguem uma distribuição exponencial bivariável.

Os modelos de Markov são utilizados para construir o modelo matemático do sistema.
A redundância paralela é um método comum utilizado para aumentar a confiabilidade do sistema e diminuir o período de falhas. Porém, as falhas são importantes para o sistema, nesse caso, pois segundo o autor, “cada componente tem dois estágios de falha: o primeiro estágio é a transição do estado ativo para o estado degradado que representa falha parcial da unidade. Já o segundo estágio é a transição do estado degradado para o estado de falha, que representa a completa carência.
O texto trata, então, do **MTBF** ("Mean Time Between Failures"), ou seja, o período médio entre falhas atribuído a um determinado dispositivo inserido em um sistema, para verificar seu nível de confiabilidade e de eficiência. Verifica, ainda, quais os cenários em nível de experimentação.
A conclusão é que em diversas situações, há dependência entre os componentes do sistema e isso indica que caso um apresente contínuas falhas, os outros também serão afetados. Os sistemas possuem uma interdependência de componentes. o modelo de Markov é utilizado e se mostra prestativo para avaliar a disponibilidade e a confiabilidade daquele sistema.
A citação do artigo está descrita a seguir:
Neama Salah Youssef Temraz. **Availability and Reliability Analysis for Dependent System with Load-Sharing and Degradation Facility**. International Journal of Systems Science and Applied Mathematics. Vol. 3, No. 1, 2018, pp. 10-15. doi: 10.11648/j.ijssam.20180301.12
O autor seguiu corretamente as regras impostas pelo International Journal of Systems Science and Applied Mathematics para elaboração de artigos.

Artigo 3 - Influence of algorithmic abstraction and mathematical knowledge on rates of dropout from Computing degree courses

O artigo aborda a influência da abstração algorítmica e do conhecimento matemático na desistência dos estudantes em cursos de relacionados à área de Computação. O estudo, realizado na Universidade de Brasilia, em parceria com o INEP, identifica as causas de altas taxas de desistência em cursos relacionados a ciencias exatas.
Isso influencia muito na nota de avaliação da própria universidade: quanto maior a taxa dedesistência, menor é a nota da instituição.
A metodologia utilizada foi utilizar dados coletados pelo censo e pelo INEP entre 2010 e 2014. Foram observadas modificações na metodologia entre 2009 e 2010, então o estudo surgiu como uma tentativa de avaliar se o novo modelo de ensino tinha dado certo ou não. Os pesquisadores se utilizam de dados como idade, sexo, diferentes instituições para constituir as tabelas de análise.
Concluíram, então, que o número de inscrições por local era inversamente proporcional e que os índices de desistência para as áreas de conhecimento mais específicos eram maiores. Na maioria dos casos, os índices de desistência eram maiores para homens,

mas na área de computação, as taxas ficaram com números similares. Uma das dificuldades encontradas foi em matérias que possuíam relação com matemática.
A citação do artigo está descrita a seguir:
Hoed, R.M., Ladeira, M. & Leite, L.L. **Influence of algorithmic abstraction and mathematical knowledge on rates of dropout from Computing degree courses.** *J Braz Comput Soc* **24,** 10 (2018). https://doi.org/10.1186/s13173-018-0074-2

Artigo 4 - A hybrid approach for scalable sub-tree anonymization over big data using MapReduce on cloud

O artigo aborda métodos de proteção de dados e propõe um modelo híbrido de tratamento dos dados em um tipo de árvore que facilita o processo de preservação de privacidade. Os pesquisadores demonstram como dois processos que percorrem a árvore, se combinados, podem trazer maiores benefícios quando tratamos de privacidade de dados em big data, por exemplo.
Indicam o MapReduce, um framework de processamento de dados em larga escala, para comprovarem sua tese, então, eles aplicam tanto o TDS("especialização de cima para baixo" quanto o BUG("generalização de baixo para cima"), combinados no MapReduce, para ganhar escalabilidade ao explorar a capacidade do armazenamento em nuvem.
Falam sobre dois modelos de privacidade como parâmetros: k-anonymity, e l-adversity. Ambos indicam o grau de divulgação de informação privada sensível.
Para medir a eficiência da experimentação do modelo defendido, eles comparam os resultados dos testes que incluem somente TDS, somente BUG e HIB - híbrido, que inclui os dois processos. A experimentação, então, demonstrou resultados positivos quanto à aplicação do modelo híbrido, apesar do ambiente de cloud ainda ser bastante desafiador por sua grande quantidade de dados.
A citação do artigo está descrita a seguir:
X. Zhang,C. Liu,S. Nepal,C. Yang,W. Dou,J. Chen. **A hybrid approach for scalable sub-tree anonymization over big data using MapReduce on cloud.** Journal of Computer and System Sciences, Elsevier, 2014. http://dx.doi.org/10.1016/j.jcss.2014.02.007

Artigo 5 - Message matching-based greedy behavior detection in delay tolerant networks

A artigo fala sobre a detecção de comportamento ganancioso de nós em redes tolerantes a atraso, seu objetivo é de que seja feita a detecção do comportamento ganancioso através da correspondência de mensagens entre cada nó da rede. Os autores abordam a natureza dos nós de uma rede e como ocorre o comportamento destes nós em ambientes roteados, onde pode ocorrer o comportamento ganancioso, o que consiste em nós que transmitam preferencialmente pacotes de acordo com o seu benefício no roteamento, prejudicando os demais nós. Através de um experimento onde introduziram uma subcamada de pacotes confiáveis, para aprimorar a segurança da arquitetura destas redes, reduzir a sobrecarga de recursos em um único nó através de um método de detecção de mensagens que utiliza esta subcamada implementada. Foram apresentados 3 tipos de comportamentos gananciosos detectados por parte dos nós: um onde os nós priorizam o encaminhamento de mensagens e com isso obter mais oportunidades de transmissão, o segundo onde a maioria das vantagens de transmissão baseadas em crédito dependentes de tamanho do caminho de entrega, se observou que quanto menor o caminho, mais creditos os nós intermediarios dentro deste caminho recebem, 3 onde verifica-se que as redes com tolerância a atraso possuem recursos limitados, sendo assim as mensagens que requerem mais tempo de transmissão irão consumir mais recursos, então para economizar seus recursos, os nós gananciosos retransmitem preferencialmente mensagens que necessitam menor tempo de transmissão. Concluiu-se que a maioria dos protocolos de roteamento nas redes com tolerancia a atraso exigem que cada nó retransmite honestamente as mensagens, mas alguns nos violam este princípio, e foi feita a implantação de um módulo inteligente e confiável que detecta comportamento ganancioso e pode oferecer um ambiente de roteamento justo e para nós que obedecem o princípio justo.

G. Wang. **Message matching-based greedy behavior detection in delay tolerant networks**. China. Elsevier Inc. Journal of Computer and System Sciences 80 (2014) 903–915. http://dx.doi.org/10.1016/j.jcss.2014.02.001

O autor seguiu corretamente as diretrizes do Journal of Computer System Sciences, da editora Elsevier, sob licença privada.

Artigo 6 - Self-adaptive federated authorization infrastructures

O Artigo aborda a infraestrutura de autorização em redes de dados onde os recursos necessitam ser protegidos e como se dá a construção desta proteção a medida em que estas redes se expandem. a proposta foi de um protótipo controlador SAAF que simula o comportamento malicioso dentro de uma rede deste tipo a fim de analisar como ocorre procedimento de proteção. Os autores fizeram a experimentação da estrutura de autorização SAAF, a qual pode ser anexada a infra-estruturas de autorização existentes,

através das suposições: A infraestrutura de autorização pode gerar logs de suas ações? Provedores de identidade podem autorizar o SAAF a modificar as atribuições de atributo do usuário, mas caso não seja possível, os provedores de identidade podem aceitar notificações do SAAF sobre atribuições errôneas? E em casos de abuso destas atribuições podem remover e adicionar novos atributos aos usuários e notificar o SAAF quando estas alterações forem completadas?

Através do controlador SAAF foi feito o monitoramento e a adaptação de infra-estrutura de autorização, o qual atualiza um modelo que representa regras de atribuição de acesso e captura estatística sobre o uso da infraestrutura. Promovendo a busca por comportamentos maliciosos, o qual, assim que encontrado é eliminado através de soluções personalizadas.

Os estudos resultaram em dois tipos de soluções, uma onde as solicitações individuais de atributos de sujeito ao serem efetuadas, este sujeito tem os atributos removidos e substituídos por um instantâneo retirado antes e depois da execução desta solicitação. O segundo afeta todos com o atributo de permissão, independentemente da identificação do usuário, remove a permissão a permissão ABAC / RBAC o que permite que o atributo de usuário execute a permissão de acesso de acordo com os contratos da política de segurança.

A citação do artigo está descrita a seguir:

C. Bailey, Zhang, D.W. Chadwick, R. de Lemos. **Comparative study on point and line thermographic inspection for fiber orientation assessment of randomly oriented strand material**. Elsevier Inc. Journal of Computer and System Sciences 80 (2014) 935–952. http://dx.doi.org/10.1016/j.jcss.2014.02.003

Os autores seguiram corretamente as diretrizes do Journal of Computer System Sciences, da editora Elsevier, sob licença privada.

Artigo 7 - Um Mapeamento Sistemático sobre Acessibilidade e Usabilidade no Desenvolvimento de Jogos Digitais para Idosos

O estudo aborda a atuação de jogos digitais na terceira idade, avaliando quesitos de acessibilidade e a usabilidade. Analisam, assim, diversos comparativos e ensaios com ambos os quesitos. Aparentemente, segundo o estudo, a usabilidade é mais aceita do que a acessibilidade no público alvo.

A jogabilidade é um fator desafiador para esse tipo de público, pois a maioria dos jogos exige que tenhamos agilidade. Por isso, os autores mapearam em literaturas quesitos como abordagem, pesquisa e coleta de evidências durante o desenvolvimento de jogos. O estudo traz ainda a informação de que a acessibilidade e a usabilidade para idosos em jogos digitais só é abordada nas fases finais do desenvolvimento ou quando é considerada como requisito de acessibilidade. Os resultados indicam que há mais literatura a respeito a usabilidade do que em acessibilidade. Esse estudo evidenciou que há ainda muitas lacunas nos centros de pesquisa com relação a esse tipo de

preocupação. Os autores sugerem que centros de pesquisa brasileiros explorem esse assunto, pois há muito espaço ainda para pesquisas nessa linha.
A citação do artigo está descrita a seguir:
Santos, F. S., Salgado, A. L. and Fortes, R. P. M. (2018). **A systematic mapping of accessibility and usability in the process of development of digital games for the elderly (Um Mapeamento Sistemático sobre Acessibilidade e Usabilidade no Desenvolvimento de Jogos Digitais para Idosos)**. iSys: Revista Brasileira de Sistemas de Informação (Brazilian Journal of Information Systems), 11(2), 63-90.
Os autores seguiram corretamente as condições para submissão de publicação do iSys, a Revista Brasileira de Sistemas de Informação.

Artigo 8 - Classificação Automática de Códigos NCM Utilizando o Algoritmo Naïve Bayes

O artigo aborda a descrição do desenvolvimento de um categorizador automático que setoriza os produtos de acordo com os códigos oficiais de nomenclatura Comum do Mercosul (NCM). O experimento trata de assuntos de Machine Learning e se utiliza do algoritmo Naive Bayes em conjunto com uma massa de dados de notas fiscais para treinamento de máquina.
Se utilizam de Nota Fiscal Eletrônica ao Consumidor (NFC-e)
A pesquisa foi feita com o propósito de diminuir as divergências existentes na descrição e código de produtos emitidos sob o NCM. O estudo então visa contribuir no campo da tecnologia, com machine learning, e no socioeconômico, para auxiliar setores sociais, governamentais em combate à corrupção.
O teorema de Bayes inclui conceitos de probabilidade condicional e sua inversa, incluindo hipótese pela observação de uma evidência e da probabilidade da evidência dada pela hipótese. Esses algoritmos são classificadores probabilísticos.
O estudo foi, então, motivado em aplicar os resultados da classificação automática textual e de código. Os autores chegaram à conclusão de que é mais difícil classificar em um sistema NCM pois sua hierarquia é mais profunda do que um sistema harmonizado, com hierarquia mais rasa. Os autores possuem planos futuros de terminarem as pesquisas para verificar se o fator idioma também influencia na dificuldade de treinamento de algoritmo a partir de uma massa de dados apresentada.
A citação do artigo está descrita a seguir:
Batista, R. A., Bagatini, D. D. S. & Frozza, R. (2018). **Automatic Classification of NCM Codes Using the Naïve Bayes Algorithm (Classificação Automática de Códigos NCM Utilizando o Algoritmo Naïve Bayes)**. iSys: Revista Brasileira de Sistemas de Informação (Brazilian Journal of Information Systems), 11(2), 4-29.
Os autores seguiram corretamente as condições para submissão de publicação do iSys, a Revista Brasileira de Sistemas de Informação.

Artigo 9 - Comparative study on point and line thermographic inspection for fiber orientation assessment of randomly oriented strand material

materiais compostos são materiais mais leves, por isso, são mais utilizados em aeromodelos (aeronaves). O estudo aborda métodos não destrutivos baseados em termografia infravermelha para avaliação da orientação da fibra. Dois métodos são utilizados: o primeiro é uma inspeção ponto a ponto baseado em elipsometria termal pulsada enquanto o segundo é uma linha aproximada baseada em inspeção pontual a laser combinada com redes artificiais neurais.

Os resultados são comparados de partes aleatoriamente escolhidas.

Utilizam-se de termografia infravermelha (IRT) pois é uma tecnologia segura que possui alta taxa de inspeção e geralmente não necessita de contato. É utilizado para diagnóstico e para monitoramento em diversos campos como em componentes elétricos, construções entre outras. Os autores, na experimentação, estão analisando imagens de terreno e compõem seu estudo com diversos gráficos e comparativos de uma área escolhida ao acaso. A elipsometria termal pulsada é um método que diminui o dano térmico do material fotográfico processado.

Os autores realizaram diversos experimentos acerca das duas abordagens, o que incluem técnicas de tratamento térmico e de conceitos extremamente técnicos. Concluíram então que dentre os 3 tipos de imagem analisados, PCT, PPT e DTT, a melhor técnica foi a de PCT, que tende a projetar as informações mais significativas presentes na massa de dados.

A citação do artigo está descrita a seguir:

Fernandes, H., Zhang, H., Figueiredo, A.A. *et al.* **Comparative study on point and line thermographic inspection for fiber orientation assessment of randomly oriented strand material**. *J Braz Comput Soc* **24,** 7 (2018). https://doi.org/10.1186/s13173-018-0071-5

Os autores atenderam corretamente as especificações definidas pela Jornal of the Brazilian Computer Society e publicadas sob licença open source da Springer.

Artigo 10 - Software control flow error detection and correlation with system performance deviation

O artigo aborda a detecção de erro no fluxo de controle de softwares e sua correlação com o desvio de desempenho em sistemas, com o objetivo de identificar essas falhas e como saná-las através do uso do Postgresql (Sistema de banco de dados Open Source) injetando aleatoriamente erros nos sistema para observá-los e mitigar ou proteger o sistema contra esse tipo de falha. Foram utilizadas 10 versões de programas diferentes, com algumas leves alterações no código sem erros de compilação, onde cada versão era executada e monitorada com 10 conjuntos de dados experimentais diferentes e com o

uso da biblioteca de ferramentas de arquitetura reversa, a qual nos permite obter informações sobre a arquitetura do software. assim foi feita a injeção de código de acordo com a arquitetura descoberta. em contrapartida as tecnicas que usam representações de BCFG, esta abordagem foi capaz de diminuir e identificar alguns riscos com mais precisão, validando o controle de fluxo dentro dos softwares. Os resultados mostraram que a capacidade de identificar componentes relacionados no sistema e padrões de estado de erro para para desvio de desempenho do sistema. Foi verificado que este experimento, com este modelo de controle de fluxo apresentou menor sobrecarga de desempenho em comparativo aos modelos já utilizados, ajudando na localização do componente responsável por cada erro de fluxo de controle. Trouxeram uma abordagem experimental completa e eficaz, ao utilizarem uma ferramenta de software para análise dos resultados e validá los.
A citação do artigo está descrita a seguir:
A. Shalan, M. Zulkernine. **Software control flow error detection and correlation with system performance deviation**. Elsevier Inc. Journal of Computer and System Sciences 80 (2014) 953–972. http://dx.doi.org/10.1016/j.jcss.2014.02.004
Os autores seguiram corretamente as diretrizes do Journal of Computer System Sciences, da editora Elsevier, sob licença privada.

Artigo 11 - A security framework in G-Hadoop for big data computing across distributed Cloud data centres

O estudo aborda a utilização do framework Hadoop, disponibilizado pela Apache Foundation, que roda o sistema MapReduce em um sistema segmentado (cluster). o G-Hadoop é uma extensão do hadoop que permite que as tarefas sejam executadas em diversos clusters, mas como ele apenas reutiliza a arquitetura do Hadoop, só deveria rodar em um cluster. Os autores do artigo desenvolvem, então, um novo sistema de segurança baseado no G-Hadoop com uma abordagem de chave de acesso única. Sugerem, ainda, inúmeros mecanismos de segurança para projeter o G-Hadoop de ataques tradicionais dee segurança.
O G-Hadoop possui uma arquitetura de nós, assim como a maioria dos sistemas em nuvem. O framework de segurança desenvolvido contém um protocolo SSL de segurança, o Globus Security Infrastructure e ainda o Java security solutions.
O framework possui uma instância de usuário, credenciais de proxy e de slave nodes separadas e sessões de usuário como principais características.
Difere da maioria dos outros artigos pois desenvolve algo mais concreto, um software ou plugin para software. Traz, portanto, uma medida de se prevenir contra os principais ataques como MITM, replay e delay e provê uma comunicação segura do G-Hadoop com conexões públicas de internet.
A citação está disponível a seguir:
L. Wang, J. Chen *et al*. **A security framework in G-Hadoop for big data computing**

across distributed Cloud data centres. Journal of Computer and System Sciences, Elsevier Inc. 80 (2014) 994–1007.
Os autores seguiram corretamente as diretrizes do Journal of Computer System Sciences, da editora Elsevier, sob licença privada.

Artigo 12 - A survey of emerging threats in cybersecurity

O artigo aborda o crescimento exponencial dos cyber attacks na internet. Isso ocorre, principalmente, pelo aumento no acesso à internet. Há um desenvolvimento mais massivo de malwares e de novas técnicas de ataques.
Os principais tipos de malware adquiridos pelos usuários são Trojans (73,31%) adquiridos por Spam, Phishing e adquiridos por downloads, os autores constatam.
Os malwares, a princípio, eram escritos com a finalidade de testar as vulnerabilidades dos sistemas, o que é ainda correto, de certa forma. Exemplificam também que há malwares para hardware, softwares e para redes e para cada tipo de ataque existe uma medida de segurança equivalente. A modificação na utilização das redes tambémém influência no aumento no número de ataques. Por exemplo, com a utilização do celular , há mais ataques pelos web browsers e voltados a dispositivos que não são os computadores de mesa e sim os portáteis, como celular e tablets.
Existem diversas áreas de pesquisa que têm sua atenção voltada a isso: privacidade, internet da nova geração, sistemas seguros, segurança na usabilidade, entre outros temas abordados para direcionar o desenvolvimento de medidas protetivas na internet. O foco está, hoje, na privacidade de dados.
A pesquisa foca, então, em dois aspectos dos sistemas de informação, que são entender as vulnerabilidades nas tecnologias e potenciais ameaças que estão ainda por vir.
esta experimentação foi inteiramente teórica e de análise.
A citação está disponível a seguir:
J. Jang-Jaccard, S. Nepal. **A survey of emerging threats in cybersecurity.** Journal of Computer and System Sciences, Elsevier Inc. CSIRO ICT Centre, Australia. 80 (2014) 973–993.
Os autores seguiram corretamente as diretrizes do Journal of Computer System Sciences, da editora Elsevier, sob licença privada.

Artigo 13 - Trust enhanced distributed authorisation for web services

O artigo aborda um arquitetura de autorização distribuída para uma plataforma de webservices, com noçoes de confiança rígida e flexível para determinar se a plataforma é confiavél para autorização, com um modelo de confiança proposto no trabalho.
Foi feita uma implementação de um modelo de arquitetura, onde havia um contexto de autorização para web services; A partir de uma extensa análise, foram elaboradas as amostras de alguns cenários onde pode-se observar que a arquitetura de autorização

distribuída aprimorada (TEDA) obteve diversas vantagens sobre os sistemas de autorização existentes, esta possui melhor desempenho em relação aos demais sistemas já em uso pois, incorpora mudanças baseadas na plataforma na qual está executando, além de utilizar recursos de credenciais de usuário, pois até o momento do estudo, não se sabe se há sistema com conceitos e eficiência semelhantes.
Constatou-se que a autorização distribuída, em vista de proteger o acesso a recursos, provou-se eficaz, na TEDA, determina-se quais valores avaliativos são permitidos para que se autorize ou não o acesso a um serviço, sendo o valor base definido com base na política de requisitos de autorização, considerando-se que sistemas críticos como bancos, podem estabelecer valores muito altos para base da política de requisitos. Foram explorados também questões de problemas de autorização de usuários e plataformas interdependentes uns dos outros, considerando-se algumas combinações e verificada a eficiência da TEDA nestes quesitos.
Os autores concluíram que esse tipo de arquitetura de autorização por confiança, integrada a autorização de usuário e plataforma é capaz de tomar melhores decisões de autorização de acesso a serviços, através da exploração de resultados obtidos em serviços web distribuídos.

A citação está disponível a seguir:
V. Varadharajan, N. Tarr. **Trust enhanced distributed authorisation for web services.** Journal of Computer and System Sciences, Information and Networked Systems Security Research, Macquarie University, Sydney, Australia. 80 (2014) Journal of Computer and System Sciences 80 (2014) 916–934. http://dx.doi.org/10.1016/j.jcss.2014.02.002
Os autores seguiram corretamente as diretrizes do Journal of Computer System Sciences, da editora Elsevier, sob licença privada.

Artigo 14 - Internet traffic clustering with side information

O artigo aborda de maneira semi-supervisionada os clusters de tráfego de internet e identifica que experimentos com o mundo real, utilizando o modelo Gaussiano, apresentaram uma significante melhora nos tráfegos dos clusters.
A análise teórica abordada, com
Os autores concluem de maneira sucinta, definindo que há uma grande quantidade de informação “cache” nos fluxos de tráfego, o que acabam por “sujar” os percursos de dados. Propuseram, então, um sistema semi supervisionado de clustering variantes do algoritmo EM. Propuseram, ainda, quantitizar os fluxos e melhorar a qualidade dos clusters. Os experimentos foram obtidos a partir de rastros deixados na internet, no mundo real.
A citação está disponível a seguir:

Y. Wang, Y. Xiang, J. Zhang, W. Zhou, B. Xie. **Internet traffic clustering with side information.** Journal of Computer and System Sciences, Elsevier Inc. 80 (2014) 1021–1036.
Os autores seguiram corretamente as diretrizes do Journal of Computer System Sciences, da editora Elsevier, sob licença privada.

Artigo 15 - Special Issue: Dependable and Secure Computing

O artigo 15, na verdade, é um "sketch", um assunto extra da revista, que fala sobre o crescimento da dos sistemas de computador e, consequentemente, de seu uso e de seus métodos de segurança. Fala sobre as frequentes falhas que ocorrem nesses sistemas por problemas de configuração, sobrecarga ou até mesmo malwares.
Diz que o primeiro papel tem a proposta de um método de sistema de mensagens equivalentes, chamado de MMBD, onde um módulo mobile é introduzido para evitar comportamento ávido. O trecho, diz, então, um resumo de todos os assuntos abordados naquela edição da revista científica, esta que têm como objetivo disseminar estudos sobre cibersegurança e tecnologia desenvolvida para a mesma abordagem.
A página não está de acordo com as diretrizes de publicação, pois não é um texto acadêmico e sim uma introdução, um sumário em formato texto. Ainda sim, é constituída de título, corpo e consideração final.
Sua citação também não é padrão, mas podemos fazê-la da seguinte maneira:
J. Chen, J. Liu. **Special Issue: Dependable and Secure Computing.** Elsevier Inc. Journal of Computer and System Sciences 80 (2014) 902.