

FERRAMENTA EM SOFTWARE PARA PRÉ-PROCESSAMENTO DE TRÁFEGO DE REDES PROFINET

AFONSO C. TURCATO¹, ANDRÉ L. DIAS², DENNIS BRANDÃO³, ROGÉRIO A. FLAUZINO⁴

¹ Doutorando em Engenharia Elétrica, EESC-USP, São Carlos, afonso.turcato@usp.br

² Doutorando em Engenharia Elétrica, EESC-USP, São Carlos, andre.dias@usp.br

³ Professor do Departamento de Elétrica e Computação, EESC-USP, São Carlos, dennis@sc.usp.br

⁴ Professor (orientador) do Departamento de Elétrica e Computação, EESC-USP, São Carlos, raflauzino@sc.usp.br

Área de conhecimento (Tabela CNPq): 1.03.04.03-7 Software Básico

Apresentado no
2º Congresso de Pós-Graduação do IFSP
06 a 09 de novembro de 2017 - Cubatão-SP, Brasil

RESUMO: A grande aceitação dos protocolos de comunicação industrial baseados no padrão *Real Time Ethernet* pela indústria desperta o interesse da comunidade científica em estudar seus pontos chaves. Há, entretanto, uma incompatibilidade entre os softwares envolvidos no processo de coleta e tratamento dos dados transmitidos. Este artigo tem por objetivo apresentar o desenvolvimento de um software que facilita a integração entre os dois principais softwares utilizados na análise do tráfego da rede: o Wireshark para a captura do tráfego e o Matlab para o processamento dos mesmos. Complementarmente, o software também apresenta informações do protocolo PROFINET com o intuito de otimizar o processamento dos dados. Os resultados encontrados indicam que, com a utilização do software, o tempo de análise é bastante reduzido permitindo que os pesquisadores, usuários do programa, tenham um esforço reduzido e possam focar seus estudos na análise do tráfego propriamente dita.

PALAVRAS-CHAVE: profinet; wireshark; matlab; captura de tráfego;

A SOFTWARE TOOL FOR PRE-PROCESSING OF PROFINET NETWORK TRAFFIC

ABSTRACT: The great acceptance of the industrial communication protocols based on the standard real time Ethernet by industry arouses the interest of the scientific community in studying its key points. There is, however, a mismatch between the software involved in the process of collecting and handling the transmitted data. This article aims to present the development of a software that facilitates integration between the two main softwares used in the analysis of network traffic: Wireshark for the capture of traffic and MATLAB for processing them. In addition, the software also features PROFINET protocol information with the purpose of optimizing data processing. The results found indicate that, with the use of the software, the analysis time is greatly reduced allowing researchers, users of the program to have a reduced effort and can focus their studies on the traffic analysis itself.

KEYWORDS: profinet; wireshark; matlab; traffic sniffing;

INTRODUÇÃO

Há uma grande discussão no cenário atual da Indústria 4.0, processamento de enormes quantidades de dados, informações e decisões obtidas e tomadas em tempo real, redução de custos e otimização da produção. No cenário da indústria moderna, um dos pontos essenciais para a integração dos processos envolvidos diz respeito aos protocolos de comunicação industrial (SESTITO, 2016).

Para atender as demandas cada vez mais rígidas da indústria, os protocolos baseados em *Real Time Ethernet* (RTE) tornaram-se cada vez mais sofisticados. As normas IEC - 61158 e IEC – 61784 padronizaram, entre outros, o protocolo PROFINET. Estima-se que atualmente este protocolo já possua 10 milhões de nós instalados (PROFIBUS & PROFINET International (PI), 2017).

Do ponto de vista dos estudos da comunidade científica, na última década (2008-2017), foram produzidos cerca de 90 trabalhos relacionados ao PROFINET. Todos estes precisam, de certa forma, da coleta e processamento dos dados de comunicação (captura dos dados da rede).

Pode-se afirmar que todos os trabalhos, que abordaram algum tipo de análise quantitativa dos dados, empregaram o software Wireshark (BABIKYAN, 2010). Há vários formatos que este programa consegue exportar seus dados, como: PCAP (formato padrão *tcpdump*), CSV (*Comma-Separated Values*), dentre outros.

Quando se trabalha no processamento dos dados coletados com o software Matlab, existem inúmeras maneiras de importá-los, sendo que arquivos no formato MAT tem sua manipulação mais prática.

Assim, no contexto apresentado, este trabalho tem por finalidade apresentar o desenvolvimento de uma ferramenta dedicada à conversão de capturas realizadas pelo software Wireshark (arquivos PCAP) em arquivos MAT, que são de fácil manipulação pelo software Matlab. Ademais, a ferramenta proposta também realiza um pré-processamento das informações inerentes ao protocolo PROFINET de modo a otimizar o processamento dos dados. A esse software desenvolvido foi dado o nome de ProfinetAnalysis.

MATERIAL E MÉTODOS

Os materiais utilizados para o desenvolvimento do software ProfinetAnalysis foram: arquivos de captura de tráfego de rede PROFINET (THOMAS, 2013) oriundos de instalações montadas no Laboratório de Automação Industrial (LAI) do departamento de Engenharia Elétrica da Escola de Engenharia de São Carlos EESC-USP, arquivos esses obtidos por meio da utilização do programa Wireshark. Para o desenvolvimento do código, foi utilizado o programa MS Visual Studio 2015 (MICROSOFT, 2015) escolhendo-se o ambiente de programação C# devido a familiaridade dos pesquisadores com essa linguagem de programação e, da compatibilidade da biblioteca de captura de rede utilizada. Para a interpretação dos arquivos binários gerados pelo Wireshark foi utilizada a biblioteca Winpcap (WINPCAP, 2017) em conjunto com a biblioteca SharpPcap (SHARPPCAP, 2017). Para análise do tráfego capturado e testes sobre o funcionamento do software desenvolvido, foi utilizado o programa Matlab (MATHWORKS, 2017).

A metodologia utilizada foi a de se executar, previamente, uma ampla pesquisa em busca de soluções equivalentes existentes para a conversão automática de arquivos no formato PCAP (formato gerado pelo Wireshark) em formato MAT (formato binário padrão utilizado pelo *workspace* do Matlab). Não foi encontrada nenhuma solução com esse propósito. Algumas possibilidades encontradas permitiam apenas que os formatos utilizados fossem outros e/ou que a conversão fosse feita de forma manual (abre-se o arquivo de captura pelo Wireshark, seleciona-se os pacotes desejados, exporta-os para o formato CSV e, posteriormente importa-os no Matlab). No entanto, essa forma manual demanda muito esforço quando são utilizados arquivos de captura com milhões de pacotes do tráfego de rede, caso este, comum em redes Profinet.

Assim, após a etapa inicial de pesquisa, iniciou-se uma segunda pesquisa com o propósito de obter conhecimento sobre como interpretar/manipular os arquivos PCAP e MAT. Feita essa pesquisa, iniciou-se a etapa de codificação utilizando-se os materiais mencionados anteriormente e, posteriormente, a etapa de testes.

RESULTADOS E DISCUSSÃO

Na Figura 1 é apresentado o fluxo de como os dados são carregados no programa (por meio dos arquivos PCAP), são processados (pelas respectivas rotinas implementadas através das bibliotecas citadas) e, ao final, arquivos do tipo MAT e TXT são gerados.

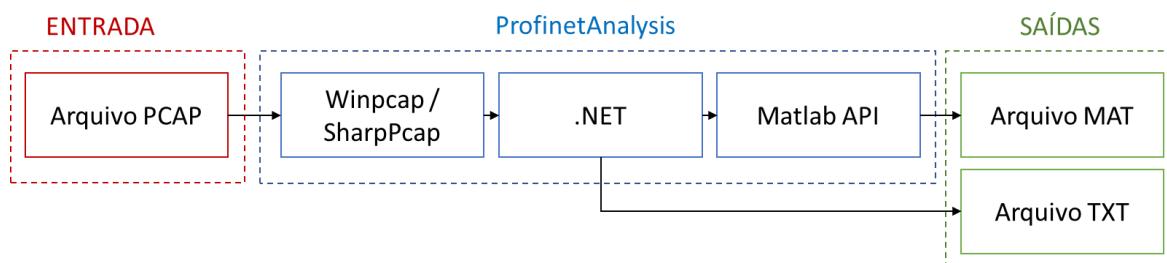


FIGURA 1. Sequência do fluxo das informações do software ProfinetAnalysis

O arquivo MAT é o arquivo gerado por meio da API do Matlab que já possui o formato compatível para ser importado diretamente no workspace do próprio Matlab. Para isso, utiliza-se o comando `load()` do próprio Matlab. Toda a informação contida no arquivo de captura de tráfego é carregada no workspace por meio da variável `packetRawData`. A Figura 2 ilustra um exemplo deste caso.

Workspace				
Name	Value	Min	Max	
packetRawData	<5500x1 cell>			

FIGURA 2. Workspace do Matlab com a variável que contém o todo o tráfego capturado (5500 pacotes).

O arquivo TXT é um arquivo formato “texto puro” que já apresenta ao usuário uma pequena síntese das informações dos equipamentos da rede Profinet cujo o tráfego foi capturado, tais como: *MAC Address*, tamanho do *buffer* em bytes, quantidade de pacotes transmitidos/recebidos, baudrate estimada em Mbps, valor médio do TDE (*Time Data Exchange*) em μ s, desvio padrão do TDE em μ s, valor médio do *jitter* em μ s e desvio padrão do *jitter* em μ s. *Jitter* é definido como variações de pequena duração, não acumulativas nos instantes significativos de um sinal digital da sua posição ideal no tempo (UNION, 1993). A Tabela 1 apresenta um exemplo dessa síntese gerada pelo software.

TABELA 1. Exemplo de informações geradas pelo software desenvolvido para uma rede com 10 equipamentos.

#	MAC Address	Buffer	Pacotes	Baudrate	TDE	DP TDE	Jitter	DP Jitter
1	00:0A:86:4D:2E:F7	40	4537	0.32	1999.993	0.063	0.036	0.052
2	00:1B:1B:6F:DE:08	40	4537	0.32	1999.993	0.06	0.035	0.049
3	00:1B:1B:D1:E7	40	71	0.005	127999.542	0.061	0.458	0.061
4	00:1B:1B:9B:61:93	40	71	0.005	127999.542	0.056	0.458	0.056
5	00:1B:1B:9C:2C:90	40	71	0.005	127999.542	0.046	0.458	0.046
6	00:1B:1B:A4:4F:86	40	4537	0.32	1999.993	0.064	0.036	0.053
7	00:1B:1B:A5:4D:51	40	71	0.005	127999.543	0.066	0.457	0.066
8	00:1B:1B:A5:4E:E9	40	70	0.005	127999.541	0.051	0.459	0.051
9	00:1B:1B:A5:4E:FA	40	70	0.005	127999.542	0.036	0.458	0.036
10	00:1B:1B:AA:7A:D7	40	71	0.005	127999.542	0.042	0.458	0.042

CONCLUSÕES

Protocolos baseados em *Real Time Ethernet* estão cada vez mais sendo aplicados na indústria, em especial o PROFINET possui posição de destaque. É natural que aumente a demanda por profissionais capacitados e, consequentemente, mais estudos por parte da comunidade científica para fornecer as respostas corretas. A lacuna descrita por este trabalho consiste na integração de dois softwares amplamente empregados para o processamento dos dados obtidos: o Wireshark e o Matlab.

A proposta deste trabalho foi desenvolver uma ferramenta para conversão de arquivos PCAP, oriundos do Wireshark, para arquivos MAT, formato binário oficial do Matlab.

Como discutida, a importância do ProfinetAnalysis fundamenta-se em facilitar pesquisas futuras. A ferramenta está sendo utilizada com êxito nas pesquisas do Laboratório de Automação Industrial da Universidade de São Paulo e futuramente será disponibilizada para uso da comunidade científica.

AGRADECIMENTOS

Os autores agradecem o suporte acadêmico e a estrutura de pesquisa do Laboratório de Automação Industrial da Escola de Engenharia de São Carlos-USP e ao engenheiro Guilherme Serpa Sestito da empresa Toledo&Souza (<http://toledoesouza.com>) pelas contribuições, validações e testes realizados com o software.

REFERÊNCIAS

- BABIKYAN, A. Wireshark. 2010. Disponível em: < <https://www.wireshark.org/lists/wireshark-users/201011/msg00028.html>>. Acesso em: 17 Maio 2017.
- MATHWORKS. Pcap files. 2017. Disponível em: <<https://www.mathworks.com/matlabcentral/answers/40864-pcap-files>>. Acesso em: 17 Maio 2017.
- MICROSOFT. Visual Studio 2015. 2015. Disponível em: < <https://msdn.microsoft.com/pt-br/library/dd831853.aspx>>. Acesso em: 07 Maio 2017.
- PROFIBUS & PROFINET International (PI) (2017) About PI. Disponível em: <<http://www.profibus.com/pi-organization/about-pi/>>. Acesso em: 11 Fev 2017.
- SESTITO, G.S.; TURCATO, A.C.; DIAS, A.L., et al. Case of study of a Profinet network using ring topology. Em: Proceedings of the International Symposium on Consumer Electronics, ISCE. 2016.
- SHARPCAP. Official repository - Fully managed, cross platform (Windows, Mac, Linux) .NET library for capturing packets. 2017. Disponível em: <<https://github.com/chmorgan/sharppcap>>. Acesso em: 28 Junho 2017.
- THOMAS, P. An Introduction to PROFINET Frame Analysis using Wireshark - V1.0. 2013. Disponível em: <<https://profibusgroup.files.wordpress.com/2013/01/w4-profinet-frame-analysis-peter-thomas.pdf>>. Acesso em: 21 Maio 2017.
- UNION, I. T. General Aspects of digital transmission systems – Vocabulary of digital transmission and multiplexing, and pulse code modulation (PCM) terms. 1993.
- WINPCAP, 2017. The industry-standard windows packet capture library. Disponível em: <<https://www.winpcap.org/>>. Acesso em: 28 Jun 2017.