UNIVERSIDADE FEDERAL DE ITAJUBÁ - UNIFEI
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Modelagem de um Ataque Cibernético em um ambiente IEC 61850 usando Redes de Petri Coloridas

Milton Rafael da Silva

Itajubá, 4 de maio de 2018

UNIVERSIDADE FEDERAL DE ITAJUBÁ - UNIFEI
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Milton Rafael da Silva

Modelagem de um Ataque Cibernético em um ambiente IEC 61850 usando Redes de Petri Coloridas

Dissertação submetida ao Programa de Pós-Graduação em Engenharia Elétrica como parte dos requisitos para obtenção do Título de Mestre em Ciências em Engenharia Elétrica.

Área de Concentração: Automação e Sistemas Elétricos Industriais

Orientador: Prof. Dr. Luiz Edival de Souza

4 de maio de 2018

Itajubá

UNIVERSIDADE FEDERAL DE ITAJUBÁ - UNIFEI
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Modelagem de um Ataque Cibernético em um ambiente IEC 61850 usando Redes de Petri Coloridas

Milton Rafael da Silva

Dissertação aprovada por banca examinadora em 06 de Abril de 2018, conferindo ao autor o título de **Mestre em Ciências em Engenharia Elétrica.**

Banca Examinadora:
Prof. Dr. Leonardo de Mello Honório
Prof. Dr. Carlos Alberto Villegas Guerrero

Itajubá
2018

Milton Rafael da Silva
Modelagem de um Ataque Cibernético em um ambiente IEC 61850 usando Redes de Petri Coloridas / Milton Rafael da Silva. – Itajubá, 4 de maio de 2018-
73 p. : il. (algumas color.) ; 30 cm.

Orientador: Prof. Dr. Luiz Edival de Souza

Dissertação (Mestrado)
Universidade Federal de Itajubá - UNIFEI
Programa de pós-graduação em Engenharia Elétrica, 4 de maio de 2018.

1. Modelagem de Ataques Cibernéticos. 2. Redes de Petri Coloridas. 3. IEC 61850. 4. Análise de Segurança. I. Orientador : Prof. Dr. Luiz Edival de Souza. II. Universidade Federal de Itajubá (UNIFEI). IV. Título: Modelagem de um Ataque Cibernético em um ambiente IEC 61850 usando Redes de Petri Coloridas

CDU 07:181:009.3

Milton Rafael da Silva

Modelagem de um Ataque Cibernético em um ambiente IEC 61850 usando Redes de Petri Coloridas

Dissertação submetida ao Programa de Pós-Graduação em Engenharia Elétrica como parte dos requisitos para obtenção do Título de Mestre em Ciências em Engenharia Elétrica.

Trabalho aprovado. Itajubá, 06 de Abril de 2018:

Prof. Dr. Luiz Edival de Souza
Orientador

Prof. Dr. Leonardo de Mello Honório

Prof. Dr. Carlos Alberto Villegas Guerrero

Itajubá
4 de maio de 2018

Agradecimentos

Dedico este trabalho primeiramente a Deus, que sempre me abençoou e me deu forças para prosseguir, aos meus pais Milton e Eugenia, que sempre me apoiaram em minhas decisões, às minhas irmãs Natália e Ana Karla e a todos os meus familiares e amigos que sempre me acompanharam e me incentivaram em minha jornada.

Agradeço muito ao meu orientador Prof. Dr. Luiz Edival de Souza, pelos ensinamentos, correções, incentivos e orientações para desenvolver este trabalho. Também agradeço aos professores Carlos Waldecir de Souza, Carlos Alberto Murari Pinheiro, Paulo Fernando Ribeiro pelas discussões e apoios na elaboração dos meus trabalhos, além do professor Tales Cleber Pimenta, coordenador da Pós-Graduação em Engenharia Elétrica da UNIFEI, que sempre me apoiou em minhas decisões. Ao meu amigo Henrique Farias da Silva, que gentilmente me forneceu diversos artigos relativos à área de ataques cibernéticos em ambientes industriais, artigos fundamentais para a definição e desenvolvimento deste trabalho. Ao meu amigo Pedro Henrique Ferreira Machado, que sendo orientado de doutorado do Prof. Dr. Luiz Edival de Souza, sempre me auxiliou na produção dos meus trabalhos.

Por fim, gostaria de agradecer a servidora Leandra Dias Pinto Martins, da Assessoria Financeira da PRPPG (Pró-Reitoria de Pesquisa e Pós-Graduação) da UNIFEI, sempre pronta a me auxiliar e muito correta na gestão dos recursos financeiros, e a CAPES e ao CNPq pelo apoio financeiro para desenvolver este trabalho.

"E, se clamares por entendimento, e por inteligência suplicares, aos brados; se buscares a sabedoria como quem procura a prata, e como tesouros escondidos a procurares, então, compreenderás o que significa o temor do SENHOR e acharás o conhecimento de Deus. Porquanto é o Senhor quem concede sabedoria, e da sua boca procedem a inteligência e o discernimento"

(Provérbios 2:3-6)

Resumo

No padrão IEC 61850, define-se a transmissão dos pacotes de mensagens *Sampled Values* (SV) no processamento da comunicação, que são valores amostrados de medidas elétricas, e estas mensagens são realmente importantes e críticas na automação de sistemas de potência. Com relação à análise de segurança das redes de comunicação, uma ferramenta muito útil são as Redes de Petri Coloridas (CPNs), porque elas modelam processos assíncronos e concorrentes, o que caracteriza o funcionamento das redes de comunicação, além de permitir a análise de atrasos em sistemas temporizados.

Assim, com base neste contexto e sabendo-se que o valor correto das medidas dos valores amostrados (*Sampled Values*) é realmente crítico na transmissão de mensagens no contexto IEC 61850, para que atue corretamente a automação dos sistemas elétricos de potência, modela-se em três cenários IEC 61850 um ataque cibernético usando as CPNs, que visa modificar os dados a serem transmitidos antes de serem empacotados como uma mensagem SV, o que é realmente crítico para a operação do sistema.

Além disso, modela-se uma classificação para os pacotes de mensagens enviados, para que seja possível determinar quais pacotes foram atacados pelo ataque cibernético, ou quais pacotes não foram corretamente enviados ao seu destino final. Os resultados correspondem ao ataque cibernético modelado, mostrando a eficácia do método de modelagem proposto. Por fim, são sugeridas algumas técnicas de mitigação deste tipo de ataque cibernético.

Palavras-chaves: Modelagem de Ataques Cibernéticos, Redes de Petri Coloridas, IEC 61850, Análise de Segurança.

Abstract

In the IEC 61850 standard, transmission of Sampled Values(SV) message packets is defined in the communication processing, which are related to the sampling process of electrical measurements, and these messages are really important and critical in the automation of power systems. Related to the security analysis of communication networks, a very useful tool is the Colored Petri Net (CPN), because it models asynchronous and concurrent processes, which characterizes the functioning of communication networks, besides allowing the analysis of delays in timed systems.

So, based on this context and knowing that the correct value of the sampled value measurements is really critical in the transmission of messages in the IEC 61850 context, because it guarantees the correct functioning of the automation in the electric power systems, it is modeled in three IEC 61850 different scenarios a cyber-attack using CPN that aims to modify the data to be transmitted before it is packed as a SV message, what is really critical for the operation of the system.

In addition, a classification for sent packets is modeled so that it is possible to determine which packets were attacked by the cyber attack, or which packets were not correctly sent to their final destination. The results corresponded to the modeled cyber-attack, showing the efficacy of the proposed modeling method.Finally, some mitigation techniques are suggested for this type of cyber-attack.

Key-words: Modeling of Cyber-Attacks, Colored Petri Nets (CPN), IEC 61850, Security Analysis.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

AES	*Advanced Encryption Standard*
AH	*Authentication Header*
APT	*Advanced Persistent Threat*
ARP	*Address Resolution Protocol*
CPN	*Colored Petri Net*
DoS	*Denial-of-Service*
DDoS	*Distributed Denial-of-Service*
DMS	*Distribution Management System*
EMS	*Energy Management System*
EPRI	*Electric Power Research Institute*
ESP	*Encapsulating Security Payload*
HAN	*Home Area Network*
HMAC	*Hash Message Authentication Code*
HMI	*Human Machine Interface*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
ICS-CERT	*Industrial Control Systems Cyber Emergency Response Team*
IEC	*International Electrotechnical Commision*
IED	*Intelligent Electronic Device*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IPsec	*Internet Protocol Security*
ISM	*Industrial, Scientific and Medical band*

ML	*Makup Language*
MU	*Merging Unit*
NAN	*Neighborhood Area Network*
NIST	*National Institute of Standards and Technology (U.S. Department of Commerce)*
OSI	*Open Systems Interconnection*
PKI	*Public Key Infrastructure*
PLC	*Programmable Logic Controller*
POTS	*Plain Old Telephone Service*
RdP	*Redes de Petri*
RTU	*Remote Terminal Unit*
SCADA	*Supervisory Control and Data Acquisition*
SIEM	*Security Information and Event Management*
SONET	*Synchronous Optical Network*
SPN	*Stochastic Petri Nets*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
SV	*Sampled Values*
TC	*Transformador de Corrente*
TCP	*Transmission Control Protocol*
TP	*Transformador de Potencial*
UCA	*Utility Communications Architecture*
URL	*Uniform Resource Locator*
USB	*Universal Serial Bus*
VLAN	*Virtual Local Area Network*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*

Sumário

1 Introdução

1.1 Considerações iniciais

Nas redes inteligentes de transmissão e distribuição de energia baseadas em comunicação interativa entre todas as partes da cadeia de conversão de energia, conhecidas como *Smart Grids*, existem redes de comunicação que permitem a transferência de dados entre seus componentes. O intercâmbio de dados, a topologia de rede, o controle descentralizado, a segurança, são características inerentes aos sistemas de comunicação e também são uma parte importante das redes inteligentes no setor de energia elétrica.

Para que a informação seja enviada e recebida de maneira correta, confiável e eficiente, é necessária a padronização na comunicação dos dados. Para alcançar esse objetivo, foi criado o padrão IEC 61850. Referenciado em (4), a IEC 61850 propõe padrões para os serviços e formatos de dados trocados em uma rede de equipamentos de sistemas elétricos.

A segurança das *Smart Grids* foi amplamente reconhecida como um problema importante com implicações potencialmente catastróficas nesse cenário (5), (6), (7), (8), (9), (10). Além disso, os ataques cibernéticos podem aproveitar a acessibilidade através das *neighborhood area networks* (NANs) ou *home area networks* (HANs) para comprometer ou controlar recursos eletrônicos de forma remota (11). Com a Internet e as telecomunicações modernas, agora é fácil para grupos geograficamente distribuídos coordenarem ataques simultâneos (11).

No cenário da modelagem de ataques cibernéticos, as Redes de Petri e suas variações têm se tornado ferramentas muito importantes para estudar vários tipos de processos assíncronos e concorrentes (12), (13), (14). A utilidade das Redes de Petri para modelos de ataques cibernéticos foi apontada primeiro talvez por McDermott (15). Ele observou que as Redes de Petri são melhores para capturar ações simultâneas na progressão de um ataque (11). Dalton et al. sugeriu a utilização de Redes de Petri Estocásticas generalizadas para a modelagem de ataques cibernéticos (16). As Redes de Petri Estocásticas são um tipo de Redes de Petri temporizadas onde as transições ocorrem ("disparam") após tempos aleatórios. Em seus trabalhos, os atrasos de transição foram assumidos como exponencialmente distribuídos, o que convenientemente transformou a Rede de Petri Estocástica em uma Cadeia de Markov de tempo contínuo equivalente. A abordagem parece ter sido motivada pela análise direta do estado estacionário possível para as Cadeias de Markov, mas o fato de assumir atrasos exponenciais de transição não foi claramente justificado (11).

As Redes de Petri coloridas chamaram atenção para os ataques cibernéticos porque

são mais expressivas do que as Redes básicas de Petri. Na Rede básica de Petri, todas as fichas são indistinguíveis umas das outras. Nas Redes de Petri coloridas, as fichas carregam valores de dados representados por cores que permitem que diferentes atacantes sejam distinguidos com identidades separadas no modelo (11). Wu et al. sugeriu o uso de Redes de Petri coloridas para modelagem de ataques hierárquicos (17). Um ataque representado em um alto nível é uma Rede de Petri colorida simples, em que certas transições têm detalhes ocultos. Os detalhes ocultos dessa transição podem ser vistos em uma subpágina associada que é uma Rede de Petri colorida separada (11).

Em relação ao sistema de potência de energia elétrica, as Redes de Petri foram aplicadas para mostrar interdependências entre as infraestruturas de energia elétrica e as comunicações pré-existentes (18), (19), (20). Além disso, Calderaro et al. (21) apresentou um método baseado em Rede de Petri para identificar e localizar falhas na rede inteligente. Chen et al. (11) propôs um novo método hierárquico para construir uma Rede de Petri grande a partir de uma série de Redes de Petri pequenas para modelar os ataques cibernético-físicos na rede inteligente (14). Dahl e Wolthusen sugeriram o uso de Redes de Petri coloridas temporizadas por intervalos, em que as fichas carregam etiquetas de tempo e o atraso de disparo das transições são limitados por intervalos de tempo especificados (22). A preocupação deles é o ataque temporizado dependente de múltiplos atacantes contra possíveis alvos múltiplos (11).

Nesses modelos de Rede de Petri, os lugares representam todos os estados possíveis de sistemas de energia e comunicação e as transições representam ações que afetam as mudanças de estado. Ou seja, as interdependências são contabilizadas de forma direta, combinando dispositivos elétricos e de comunicação em uma única Rede de Petri (11).

Assim, neste trabalho, com base em todos os trabalhos anteriores, e conhecendo-se as peculiaridades da norma IEC 61850, propôs-se modelar e analisar o impacto de um ataque cibernético em três cenários diferentes, com *merging units* que publicam mensagens *Sampled Values*, uma *switch* para troca de pacotes e armazenamento, e um analisador de rede para verificar e classificar os pacotes enviados. Este ataque cibernético visa modificar a transmissão das mensagens de valores amostrados (ataque cibernético de modificação de dados) e avaliar o impacto delas nos sistemas de comunicação do sistema de energia elétrica. Também propôs-se uma modelagem de uma classificação para os pacotes de mensagens enviados, para que seja possível determinar quais pacotes foram atacados pelo ataque cibernético, ou quais pacotes não foram corretamente enviados ao seu destino final. A modificação de dados, também conhecida como *diddling* de dados ou inserção de dados, envolve a alteração de dados antes de serem processados em seu destino final (1).

1.2 Justificativa

A modelagem de um ataque cibernético em um ambiente industrial ou nas subestações de energia elétrica permite investigar soluções que diminuam os riscos de falha de comunicação, criar estratégias para modelar e encontrar pontos críticos no sistema de comunicação, além de possibilitar uma prévia avaliação do sistema. Por exemplo, é possível prever algumas condições que só seriam sentidas em um processo de colapso do sistema elétrico. Outras condições podem facilmente ser testadas como, ampliação de rede, mudança de arquitetura de rede, reconfiguração de dispositivos e assim por diante.

Além disso, através do desenvolvimento de modelos automatizados de ameaças, tanto em ambientes industriais quanto em subestações de energia elétrica, pode-se abordar e identificar os passos mais prováveis para a execução de um ataque cibernético nestas situações. Há alguns sistemas de monitoramento contínuo que criam automaticamente simulações de todas as etapas de um ataque potencial e fornecem as recomendações sobre a melhor forma de interrompê-lo. Entre estas recomendações, pode-se ter a eliminação de senhas em textos simples para dispositivos específicos, ou a implementação de uma melhor segmentação da rede.

Neste trabalho será utilizada a ferramenta de modelagem Redes de Petri Coloridas para modelar um ataque cibernético de modificação de dados em um sistema de comunicação baseado na norma IEC 61850.

1.3 Objetivos deste trabalho

O objetivo deste trabalho é modelar e analisar o impacto de um ataque cibernético utilizando o formalismo matemático das Redes de Petri Coloridas, em três arquiteturas distintas com *merging units* que publicam mensagens de *Sampled Values*, uma *switch* para troca de pacotes e armazenamento, e um analisador de rede para verificar os pacotes enviados.

Este ataque cibernético visa modificar a transmissão das mensagens de valor amostradas (modificação de dados) e avaliar o impacto delas nos sistemas de comunicação do sistema de energia elétrica. Modelou-se também uma classificação para os pacotes de mensagens enviados, para determinar quais pacotes foram atacados pelo ataque cibernético, ou quais pacotes não foram corretamente enviados ao seu destino final.

1.4 Estrutura do trabalho

A dissertação está estruturada em cinco capítulos na seguinte disposição. No Capítulo 2, faz-se uma fundamentação teórica do trabalho em questão, apresentando as

definições de diversos tipos de ataques cibernéticos, as proteções de IP e métodos de criptografia, as técnicas de mitigação e os pontos potenciais de ataque em uma rede de comunicações no ambiente industrial. Além disso, são definidas as Redes de Petri (RdP) e as Redes de Petri Coloridas (CPN) e apresenta-se o *software CPN Tools*. Neste capítulo também é apresentado brevemente a norma IEC 61850. Abordam-se os conceitos relacionados às mensagens *Sampled Values* (SV) e aos requisitos temporais.

O Capítulo 3 trata da modelagem em Redes de Petri Coloridas. São descritos os vários modelos que compõem a arquitetura apresentada, além da modelagem do ataque cibernético de modificação de dados proposto neste trabalho e da classificação para os pacotes de mensagens enviados.

Os resultados das simulações e suas respectivas análises são apresentados no Capítulo 4. Este capítulo também ressalta as avaliações sobre a metodologia utilizada e os resultados obtidos.

Por fim, o capítulo 5 apresenta as conclusões gerais, considerações finais e contribuições desta dissertação, além de sugerir alguns trabalhos futuros que podem ser desenvolvidos com base neste trabalho.

2 Fundamentação teórica

2.1 Introdução

Neste capítulo serão definidos os vários tipos de ataques cibernéticos já conhecidos na literatura. Ataques cibernéticos são definidos como os métodos ou meios pelos quais os *hackers* ou atacantes utilizam, como o controle de sistemas de comunicação, dispositivos, programas e redes de computadores e acesso a certos dados, para atingir seus objetivos, com intenção maliciosa.

Conforme definição de (23), *hacker* "é um indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores. Graças a esses conhecimentos, um *hacker* frequentemente consegue obter soluções e efeitos extraordinários, que extrapolam os limites do funcionamento normal dos sistemas como previstos pelos seus criadores; incluindo, por exemplo, contornar as barreiras que supostamente deveriam impedir o controle de certos sistemas e acesso a certos dados".

O conhecimento de ataques cibernéticos é muito importante para que sejam evitados ou mitigados. Há vários tipos de ataques cibernéticos que devem ser entendidos para garantir que seja aplicada uma metodologia de segurança apropriada.

2.2 Definições de Ataques Cibernéticos e Pontos Potenciais de Ataque

Identificar os ataques cibernéticos através de possíveis locais em que possam ser executados é importante para a segurança de um sistema de energia. O *site* do Programa de Segurança dos Sistemas de Controle de Segurança Interna dos Estados Unidos contém muitos recursos para identificar vulnerabilidades e pontos potenciais de ataques cibernéticos em sistemas de comunicações (24).

A seguir, definem-se os principais ataques cibernéticos conhecidos na literatura, baseados nos trabalhos de (1) e (25).

A. Acesso Externo à Rede

Em relação ao acesso externo à rede, um dos meios pelos quais este tipo de ataque pode ser efetuado é através de conexões indiretas para redes de "suporte" menos seguras. Estas redes de suporte podem estar conectadas à Internet, o que permite que invasores na Internet acessem aos ativos do sistema de controle crítico. Este invasor pode também

usar uma conexão no sistema SCADA (*Supervisory Control and Data Acquisition*) ou na rede WAN (*Wide Area Network*) de engenharia, quando estas redes não são seguras, para atacar os ativos na subestação conectada. Dentre os meios de ataque exploráveis, têm-se *modems* discados, *links* sem fio inseguros ou gabinetes de comunicação acessíveis fisicamente.

Dentre os vários meios de acesso externo à rede, o ataque conhecido como marcação de guerra (*War Dialing*) é uma técnica de identificação de *modems*, com o objetivo final de obter acesso e controle à rede atacada. Os atacantes podem também manipular os bancos de dados, como historiadores de dados de processo, processadores de comunicações ou servidores HMI (*Human Machine Interface*), com o objetivo de manipular os dados para executar ações mal-intencionadas no sistema de controle. No caso das comunicações de engenharia e do sistema SCADA (*Supervisory Control and Data Acquisition*), os pontos de acesso aos sistemas de comunicação, utilizados para configurar, controlar e monitorar dispositivos, podem ser manipulados para causar falhas em disjuntores, alterações de confirgurações dos equipamentos, limpeza de *logs*, etc. O acesso a estes sistemas de comunicação pode ser feito também através de ataques de quebra de senha, que tentam decodificar uma senha ou mensagem através de diversas tentativas, ou através de uma longa lista de palavras predefinidas, ou também através de senhas padrão, que são definidas pelo fabricante dos equipamentos e não são alteradas pelo usuário final. Por fim, os ataques de negação de serviço (*Denial of Service* - DoS) e de negação de serviço distribuído (*Distributed Denial of Service* - DDoS) impedem as informações de atingir o destinatário pretendido, através da inundação da rede com uma abundância de pedidos para que esta se torne saturada e não responda ao tráfego legítimo de informações.

B. Man-in-the-Middle

No ataque cibernético conhecido como *Man-in-the-Middle*, o invasor se coloca entre dois pontos, para assumir o controle da rede, e para que este ataque seja efetuado, o invasor precisa acessar a rede física. Estes tipos de ataques exploram a falta de autenticação, e por meio destas invasões, o atacante pode controlar a conexão, espiar os dados que passam e inserir mensagens falsas. Como exemplos para este tipo de ataque, têm-se o envio de um *status* falso de um disjuntor ou outro equipamento de proteção e o envio desta mensagem para o sistema SCADA, ou a modificação das respostas para a Interface Homem-Máquina (HMI - *Human Machine Interface*), apresentando ao operador um falso *status* do sistema.

Define-se também o ataque de acesso direto, ou *Insider*, como o ataque de pessoal autorizado que manipula deliberadamente os dispositvos para produzir uma condição não autorizada. Estes tipos de ataques são motivados por vingança ou ganhos pessoais, e são bem difíceis de serem prevenidos porque o invasor é um usuário confiável. Já os ataques de inserção de dados maliciosos, modificação de dados ou engano de dados (*Data Diddling*) consistem em alterar os dados antes de serem processados em seu destino final, e ocorrem

geralmente em ambientes de entrada de dados. No caso dos ataques de repetição ou reprodução de dados, as comunicações são espionadas, interceptadas e armazenadas, para serem reproduzidas em outro momento, quando o invasor julgar oportuno.

C. Espionagem

Os ataques de espionagem consistem numa captação silenciosa das comunicações válidas para conhecer o sistema a ser atacado.

Dentre as várias técnicas e meios de espionagem, o *Malware* é um software projetado para se infiltrar em um sistema de computador sem o consentimento informado do proprietário, é instalado através de serviços de comunicações não seguros, de mídias removíveis ou memórias USB (*Universal Serial Bus* na forma de vírus, *worms* e *trojans* e pode fazer com que o sistema pare de funcionar e permita o acesso e envi informações para usuários não autorizados.

Outra ameaça, conhecida como ameaça persistente avançada (APT - *Advanced Persistent Threat*) é um ataque que combina todos os métodos de ataques cibernéticos possíveis através de uma forma bem pensada, como um e-mail com um *link* para o que parece ser um *site*, mas, de fato, é um meio de lançamento para um ataque cibernético na infraestrutura específica. O ataque APT é planejado para alcançar rapidamente o objetivo desejado, de forma que ele não possa ser interrompido antes que o objetivo seja atingido.

Por fim, os ataques definidos como explorações de atualizações de *software* consistem em carregar código não autorizado em um dispositivo ou modificar o processo de atualização de forma a impedir o correto funcionamento dos mesmos. A exploração dessas falhas no software que monitora e controla os sistemas pode ser usado para corromper a memória, modificar os dados e executar comandos indevidos.

A seguir, são enfocados os métodos de criptografia e autenticação de dados, além das técnicas de mitigação de ataques cibernéticos (1).

2.3 Proteções de IP e Métodos de Criptografia

Muitos métodos são desenvolvidos com intenção maliciosa de espionagem, sabotagem ou acesso aos sistemas de comunicação. Esta seção apresenta definições básica de criptografia e autenticação de dados através do IPsec, X.509, *hash* de mensagens e criptografia AES (*Advanced Encryption Standard*).

2.3.1 Comunicações Seguras

Inicialmente, é necessário apresentar algumas definições básicas de criptografia de chave pública, para compreender os métodos utilizados pelos atacantes e como se defender contra tais ataques. A criptografia de chave pública requer dois códigos, definidos como

chaves, ligados matematicamente, e este par de chaves é responsável pelo segredo das mensagens em uma rede não segura. Uma chave criptografa uma mensagem de texto, enquanto a outra chave descriptografa a mensagem de texto criptografado, como mostrado na Figura 1. Como ambas as chaves não podem executar a mesma função, este método de duas chaves distintas é classificado como criptografia de chave assimétrica. A criptografia é alcançada pelo uso da chave pública, amplamente dispersa. A descriptografia, no entanto, só é alcançada através da chave privada.

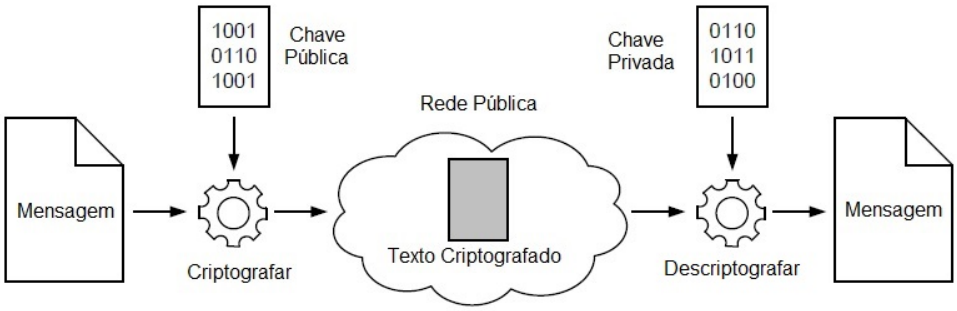

Figura 1 – Conceito de criptografia de chave pública (adaptada de (1))

A confidencialidade é alcançada através do segredo da chave privada, e se esta for comprometida, a confidencialidade pode ser prejudicada. A criptografia de chave pública e o uso de criptografia de chaves assimétricas fornecem uma segurança maior e também oferecem muitos outros benefícios. Como uma chave privada é específica para um usuário ou dispositivo, pode-se verificar sua identificação.

Uma assinatura digital é uma mensagem assinada com a chave privada do remetente e permite a verificação de identidade, integridade da mensagem e sua origem. O processamento de assinatura digital de uma mensagem é parcialmente realizado por um processo conhecido como um *hash*. O processo de *hashing* faz com que toda a mensagem seja colocada através de um processo unidirecional que não pode ser revertido. O *hash* resultante, ou a série de caracteres alfanuméricos resultantes do processo de *hashing*, é conhecido como um resumo de mensagens. O resumo da mensagem é um valor de *hash* de comprimento fixo, que independe do tamanho de dados de entrada.

Cada mensagem deve ter um resultado de *hash* exclusivo. No exemplo da Figura 2, ambas as mensagens têm valores de *hash* diferentes, embora apresentem uma pequena diferença entre as mensagens.

Se alguma parte da mensagem for adulterada ou modificada, o resumo da mensagem irá mudar, consequentemente. Uma assinatura digital será criada por *hashing* de toda a mensagem com a chave privada do remetente, como mostrado na Figura 3. Como a chave particular, específica para o remetente, é utilizada, assume-se que a mensagem associada é válida, e verifica-se também a integridade dos dados. Se o resumo da mensa-

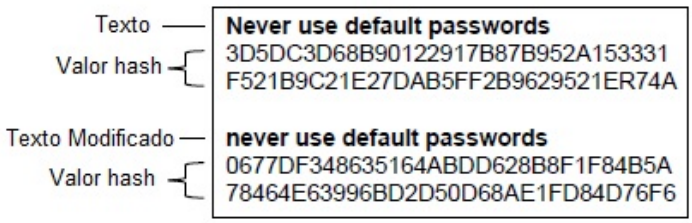

Figura 2 – Exemplo de um resumo de mensagem ou *hash* (adaptada de (1))

gem permanece inalterado do remetente para o destinatário, assume-se que a mensagem como autêntica, ou seja, esta não foi alterada ou modificada.

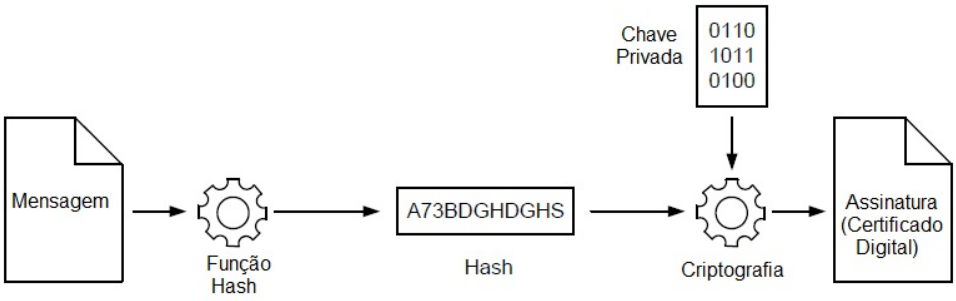

Figura 3 – Gerando uma assinatura digital (adaptada de (1))

Outro método utilizado é a criptografia de chave simétrica. A criptografia simétrica usa a mesma chave para criptografia e descriptografia. Como a mesma chave é usada para ambas as funções, a criptografia simétrica é mais rápida no processamento e maiores velocidades são alcançadas, no entanto, a segurança fica fragilizada. Se a chave estiver comprometida em uma criptografia de chave simétrica, a confidencialidade e a integridade dos dados do sistema estarão em risco.

2.3.2 IPsec

O IPsec (*Internet Protocol Security*) é uma estrutura padronizada para proteger as comunicações IP em uma rede confiável ou não confiável, fornecendo confidencialidade, integridade e autenticação. A confidencialidade é fornecida através de algoritmos de criptografia fortes, enquanto a integridade é fornecida pelo uso de validação de mensagens conhecidos como *checksums* e *hashes*.

O IPsec foi desenvolvido pela *Internet Engineering Task Force* (IETF), e ele constrói um túnel seguro de comunicações entre dois pontos finais, como mostrado na Figura 4. Isto é realizado através do uso de um protocolo que troca chaves entre os dois pontos. O IPsec funciona pelos dispositivos de envio e recepção que compartilham uma chave

pública, e após o estabelecimento deste túnel de comunicação entre os dois pontos finais, o remetente e o receptor concordam com o algoritmo de criptografia a ser usado.

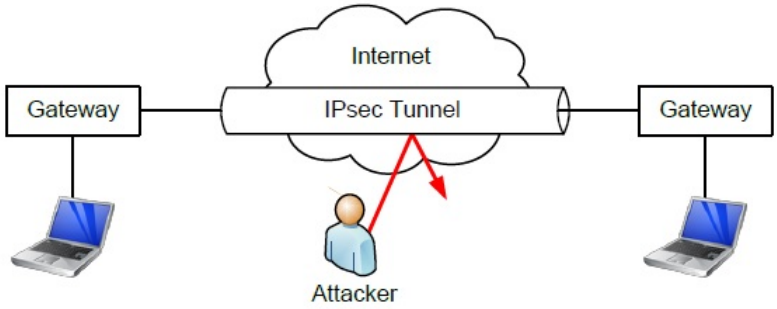

Figura 4 – Túnel seguro IPsec (adaptada de (1))

O IPsec utiliza os dois protocolos a seguir para transferência de dados, conforme mostrado na Figura 5:

• O cabeçalho de autenticação (AH - *Authentication Header*) é usado para autenticar o tráfego IP, mas não executa criptografia; esta é realizada pelo cálculo de mensagens *hash* sobre o pacote de dados.

• Encapsulamento de segurança da carga (ESP - *Encapsulating Security Payload*) fornece confidencialidade ao criptografar os dados, além de fornecer autenticação, integridade e anti-repetição, podendo ser utilizado com ou sem o protocolo AH.

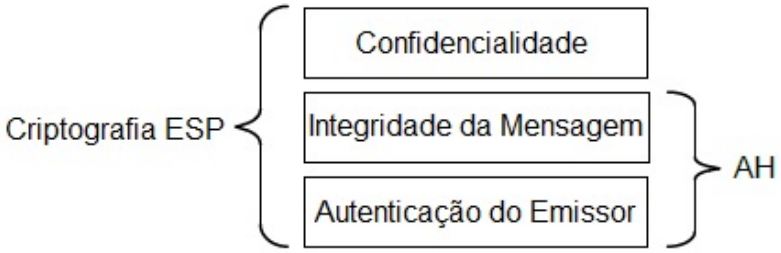

Figura 5 – ESP e AH trabalham juntos (adaptada de (1))

O IPsec pode ser implantado em uma rede SCADA para proteger as comunicações entre *gateways* que protegem dispositivos finais, como PLCs ou IEDs.

2.3.3 Criptografia AES

O AES é um algoritmo reconhecido pelos Estados Unidos e mundialmente aceito para codificar dados. O AES opera dividindo dados em blocos chamados de matrizes e operando em cada um, executando várias rodadas de codificação dos dados, substituindo dados, deslocando linhas e misturando colunas. Assim como o objetivo de qualquer criptografia, o AES fornece confidencialidade de dados, sendo o algoritmo de chave simétrico mais amplamente utilizado.

2.3.4 X.509

O X.509 é um padrão que define o contexto e o arranjo de um certificado digital, que liga uma chave pública à entidade de uma pessoa ou dispositivo, assegurando assim a validade da comunicação e impedindo a falsificação da entidade, além de fornecer confidencialidade, autenticação, não revisão e controle de acesso baseado no usuário, incluindo também um sistema de autoridades de certificação para emitir os certificados. Um certificado X.509 geralmente inclui informações sobre a entidade, como nome, organização e país e são comuns em dispositivos com uma interface web e fornecem segurança para acesso a esses dispositivos.

2.4 Técnicas de Mitigação

Em qualquer plano de segurança, o objetivo é reduzir o risco. Os diversos métodos que os atacantes utilizam para obter acesso, reunir inteligência e executar atividades malintencionadas foram discutidos anteriormente. Cada forma de ataque tem uma técnica de mitigação específica, conforme resumido na Tabela 1 (adaptada de (1)).

Tabela 1 – Tipos de Ataques e Técnicas de Mitigação

Tipos de Ataque	Técnicas de Mitigação
Ataque de Repetição	Sequenciamento de mensagens (IPsec), etiquetas de tempo
Ataque *Man-in-the-Middle*	Criptografia forte (IPsec) com PKI, AES, X.509
Ataque de Força Bruta	Política de senha forte, bloqueio de conta e atraso
Ataque de Dicionário	Política de senha forte, bloqueio de conta
Espionagem	Criptografia e autenticação fortes
DDoS	Detecção rápida, filtragem de IP (*firewall*)
Ataque de Marcação de Guerra	*Modem* comutado quando necessário, opção de retorno de chamada ativada, listagem de chamadas de entrada
Ataque de Senhas Padrão	Uso de senhas únicas, política de senha forte
Ataque de Modificação de Dados	Código de autenticação de mensagens baseado em *Hash* (HMAC), AES, X.509
Vulnerabilidades de Plataforma	Correção através de política de operações de segurança, gerenciamento de ativos e controle de mudanças
Ataque de Acesso Não Autorizado	Estado do *Firewall*, controles de acesso (*Lightweight Directory Access Protocol* [LDAP]), AES, X.509

Em um ataque de repetição, reproduz-se uma senha ou transmissão de dados interceptada. Com IPsec, incrementa-se um número de seqüência para cada pacote enviado,

o que impedirá ataques de repetição. Uma mensagem recebida com um número fora de sequência esperada será descartada.

Para ataques *man-in-the-middle*, há uma técnica semelhante. A defesa contra tais ataques é realizada através da criptografia e autenticação sólidas, utilizadas em conjunto para fornecer uma defesa adequada.

As defesas de ataques de modificações e inserções de dados falsos também dependem da autenticação. Um método de autenticação é um HMAC (*Hash Message Authentication Code*) usado dentro do IPsec, através da utilização de uma função*hash* junto com uma chave, gerando assim um código de autenticação de mensagem, e como o código de autenticação é baseado no conteúdo dos dados, se os dados forem alterados, o código de autenticação não irá corresponder de origem a destino, indicando que os dados não são autênticos. Um HMAC é usado para verificar tanto a integridade quanto a autenticidade dos dados.

No passado, o acesso aos IEDs da subestação era realizado usando *modems* em um circuito telefônico antigo (POTS - *Plain Old Telephone Service*). Esta prática está sendo descontinuada, devido à problemas de segurança. Nestes casos, a comunicação é estabelecida em uma infraestrutura que não está sob o controle da empresa, o que apresenta risco de acesso não autorizado.

O *software* de discagem de guerra (*war dialing*) é utilizado por um invasor para identificar *modems*. Embora a marcação de guerra não possa ser evitada, seu objetivo final da marcação da guerra pode ser eliminado, desconectando *modems* quando não estiverem em uso.

A defesa contra ataques a senhas, como ataques de dicionário e ataques de força bruta, requer a utilização de senhas fortes. Alguns ataques recentes em dispositivos físicos foram bem sucedidos porque as senhas nunca foram alteradas dos padrões de fábrica. Os atacantes conhecem as senhas padrão de fábrica do equipamento do fabricante, e é muito importante mudar estas senhas para torná-las fortes. Uma boa política de senha deve incluir como requisitos um número mínimo de caracteres, um ou mais símbolos especiais e caracteres em letras maiúsculas e minúsculas. Senhas como **Oaks SubStat1on Deliv3rs!** tornam difícil o ataque de dicionário e ataques de força bruta. Têm-se a substituição de alguns caracteres por números para fortalecer o segredo da senha.

Os ataques de negação de serviço e de negação de serviço distribuído requerem atenção especial, pois enquanto o ataque de negação de serviço pode ser derrotado pela filtragem e rejeição do endereço IP de origem, o ataque de negação de serviço distribuído é muito mais difícil porque o tráfego vem de muitos dispositivos e deve ser tratado por uma equipe de rede.

Outro conceito muito importante em controles de mitigação são os *firewalls*. Os

firewalls permitem ou negam o tráfego para os IEDs ou outros dispositivos, analisando os pacotes de dados recebidos e, com base em um conjunto de regras, determinam se os dados podem passar para os dispositivos ou não. Existem vários tipos de *firewalls*, incluindo um tipo conhecido como *firewall* de estado, que inspecionam pacotes de dados e acompanham o estado da conexão armazenando atributos da conexão, como endereços IP, números de porta e os números de seqüência dos pacotes.

2.5 IEC 61850 e Mensagens *Sampled Value (SV)*

2.5.1 Considerações Gerais

De acordo com (3), a integração dos sistemas elétricos de potência através das redes de comunicação permite solucionar problemas típicos das estruturas convencionais de comunicação, tais como problemas de interoperabilidade de protocolos, redes e dispositivos, problemas de manutenção, conversores de protocolos, e assim por diante.

Houve em 1995 os primeiros esforços para padronizar os aspectos de comunicação nos sistemas do setor elétrico, especificamente dentro das subestações. Assim, duas frentes iniciaram este processo, a *Electric Power Research Institute* (EPRI - EUA) e a *International Electrotechnical Commission* (IEC - França) (26). A EPRI criou especificações denominadas *Utility Communications Architecture* (UCA) e a IEC formou um grupo de trabalho para desenvolver um projeto de padronização. Após anos de desenvolvimento, em 2002 surgiu um padrão internacional para as arquiteturas de comunicação em subestações dos sistemas elétricos de potência, denominado IEC 61850.

A norma IEC 61850 é uma norma internacional que define a forma de operação entre os diferentes equipamentos presentes na automação de sistemas elétricos de potência (2). Ela modela a interconexão dos elementos de automação, através da representação em um plano lógico dos equipamentos. Esta norma possui funções que interoperam de forma distribuída, podendo estar alocadas em um ou mais IEDs conectados em rede, e isto é usado para integrar funções de medição, de controle e proteção. Fisicamente, isto possibilita a substituição dos cabos de controle por redes de comunicação, reduzindo o custo global na instalação, no comissionamento, no monitoramento, na manutenção e no diagnóstico (27).

Alguns benefícios obtidos pelo uso da norma IEC 61850 são citados em (28):

• Diminuição dos esforços de integração, uma vez que existe uma padronização dos equipamentos e interfaces de comunicação, independente do fabricante;

• Comunicação direta com sistemas EMS/DMS/SCADA eliminando dispositivos de intercomunicação (RTUs e Gateways);

• Acesso direto a todos os pontos de um sistema de potência, remota ou localmente;

• Solução distribuída que substitui os sistemas RTUs centralizados aumentando a confiabilidade do sistema;

• Livre alocação das funções nos IEDs, oferecendo maior flexibilidade;

• Solução *plug and play*, permitindo futuras expansões de planta;

• Significativa redução de custo de implementação, integração, comissionamento e manutenção.

2.5.2 Mensagens de Valores Amostrados (SV - *Sampled Values)*

Conforme foram definidas em (3), as mensagens de valores amostrados (SV- *Sampled Values*) estão inseridas nos modos de transmissão *unicast* ou *multicast* e são utilizadas para enviar dados analógicos digitalizados de corrente e / ou tensão, oriundos dos transformadores de corrente e potencial, respectivamente, para os equipamentos de proteção e controle da subestação.

A seção 9-2 da norma IEC 61850 define a forma de transmissão dos valores amostrados sobre uma rede *Ethernet* através de uma *merging unit* (MU) ou outro instrumento medidor com interface eletrônica (29).

As mensagens *Sampled Values* (SV), utilizam a camada de enlace do modelo OSI (*Open System Interconnection*) e a interface de comunicação publicador/assinante (*peer-to-peer*) e, além disso, são determinísticas. A cada período de tempo, determinado pela frequência de amostragem do sinal e pela resolução temporal necessária para a conversão analógico-digital, uma mensagem SV é colocada na rede (30). Isto poderia causar aumento no tráfego e eventual perda de pacotes e conflitos de rede e com isto, as mensagens SV ainda são um desafio para a aplicação plena da norma IEC 61850.

2.5.2.1 Requisitos de Tempo

Define-se na seção 5 da norma (2) o tempo de transferência entre dois pontos, como ilustrado na Figura 6, que é o tempo no processamento de envio e recepção das mensagens. O tempo total de transferência t é composto pela soma dos tempos ta, tb e tc. Os tempos ta e tc são os tempos de codificação e decodificação das mensagem em cada dispositivo, e o tempo tb é o tempo de propagação do quadro no meio físico utilizado.

Com base neste conceito de tempo de transferência, as mensagens são classificadas. A norma divide as mensagens em dois grupos de classes de desempenho. O primeiro grupo é para proteção e controle e cobre três classes: P1 para distribuição de vão, P2 para transmissão de vão e P3 para transmissão entre vãos com características de alto sincronismo e precisão. Entende-se por vão o nível que trata dos equipamentos de proteção,

automação e controle. Neste nível há a troca de informações entre os IEDs, o que caracteriza a comunicação horizontal. O segundo grupo é o de medição e qualidade da energia e cobre também três classes: M1 para a classe com precisão de 0,5, M2 para medidas com precisão 0,2 e M3 para medições com qualidade superior ao quadragésimo harmônico.

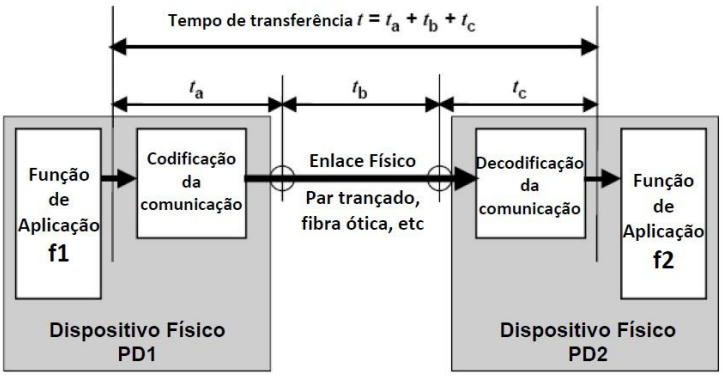

Figura 6 – Tempo de Transferência (adaptada de (2))

Além das classificações por classe, a norma define uma classificação por tipos de mensagens, como são apresentadas a seguir:

Tipo 1 - Mensagens de velocidade alta

Este tipo de mensagem tipicamente contém dados simples como exemplo comandos de *Trip* e intertravamento. O tempo de transmissão destas mensagens é dependente da classe de desempenho P1, P2 ou P3. A P1 tem tempo de transmissão de até 100 ms enquanto as classes P2 e P3 têm tempo de transmissão na ordem de 4,16 ms.

Tipo 2 - Mensagens de velocidade média

Carrega informações de estados e medições simples r.m.s.. A restrição temporal destas mensagens é de até 100 ms.

Tipo 3 - Mensagens lentas

Transmissão de registros de eventos, leituras e mudanças de ajustes, alarmes e medições não elétricas. Tempo de transmissão é de até 500 ms.

Tipo 4 - Grande Volume de dados (valores amostrados)

Esta mensagem carrega os dados amostrados dos TCs e TPs. Possui restrições temporais conforme as classes de desempenho, da mesma forma que as mensagens do tipo 1.

Tipo 5 - Funções de transferência de arquivos

Extensos arquivos de dados para registros, supervisão, ajustes e oscilografia. Restrição temporal maior ou igual a 1000 ms.

Tipo 6 - Mensagens de sincronização de tempo

Mensagens empregadas para sincronizar os relógios dos IEDs dentro do sistema de potência. Sua classe de precisão é um requisito funcional e depende do propósito do sincronismo.

Tipo 7 - Mensagens de comando com controle de acesso

Mensagem utilizada para transferir mensagens do tipo 3, com controle adicional de acesso.

2.6 Modelagem em Redes de Petri Coloridas

As Redes de Petri (RdP) são uma ferramenta matemática gráfica para a modelagem e o estudo de sistemas caracterizados como concorrentes, assíncronos, distribuídos, paralelos, não determinísticos e/ou estocásticos (31). A RdP é um grafo bipartido formada por dois conjuntos: transição e lugar, e sua representação é como mostrada na Figura 7, na qual o lugar é o círculo e a transição é o retângulo. Estes dois componentes, também definidos como nós, são interconectados por arcos dirigidos (3).

Para a modelagem e interpretação de sistemas, utilizam-se marcas ou fichas (*tokens*) atribuídas aos lugares, que representam a situação do estado do sistema, e a movimentação das marcas através dos lugares, junto com regras bem definidas, representa a dinâmica do sistema a ser modelado.

Em relação à análise de protocolos de rede, as Redes de Petri Estocásticas (SPN - *Stochastic Petri Net*) são aplicadas na análise de desempenho das redes de computador e sistemas de comunicação, pois possibilita a análise de probabilidade de estados do sistem (32). Porém, as SPNs são limitadas em modelos complexos, como modelos de dimensões industriais, por exemplo.

No caso das Redes de Petri Coloridas (CPN - *Colored Petri Nets*), que combinam as Redes de Petri (RdP) (33) com linguagem de programação, são também um superconjunto das redes de Petri ordinárias. Em CPN as fichas carregam a informação definida como a “cor" (tipificação), que pode ser tipo, tamanho, nome, registro, estado, etc. Lugares que aceitam fichas “coloridas" são coloridos também, como exemplo, lugares que suportam “cores" do tipo nome não suportam “cores" do tipo tamanho. Em relação às linguagens orientadas a objeto, diz-se que as “cores" são as classes dos objetos. As transições avaliam as fichas vindas dos seus lugares de entrada, podendo modificar a informação da ficha e carregá-la para o lugar de saída.

Nas Redes de Petri Coloridas, a temporização é uma outra propriedade usada para diferentes análises de desempenho. Em redes de Petri ordinárias tem-se que o disparo é instantâneo, no entanto, sabendo-se que sistemas reais possuem tempos envolvidos, as fichas temporizadas carregam mais uma informação, que é a estampa de tempo (*time*

stamp). A estampa de tempo é a informação de quando a ficha estará disponível, com isto pode-se garantir uma análise estocástica do sistema.

Outro característica importante que o uso das Redes de Petri Coloridas possibilita é a hierarquia de redes. Algumas partes dos modelos podem ser agrupadas em módulos (subsistemas), intitulados "transições de substituição", e podem ser reusadas múltiplas vezes em um modelo, facilitando o processo de modelagem. Elas também escondem a complexidade do comportamento do usuário permitindo melhor entendimento do processo como um todo. Para maior compreensão do sistema, pode-se olhar dentro do subsistema. Com isso, diz-se que a modelagem por meio das Redes de Petri Colorida possui maior capacidade de abstração.

A definição matemática para as CPNs é representada pela teoria de conjuntos conforme é apresentado em (34) e (35):

CPN = $\{P, T, CB, C, W^-, W^+, W^h, Pri, M_0, \theta\}$

• P é o conjunto finito de lugares;

• T é o conjunto finito de transições temporizadas e imediatas, $P \cap T = \emptyset$, $P \cup T \neq \emptyset$;

• CB é a família das classes de cores básicas: $CB = \{C_1,...,C_n\}$ com $C_i \cap C_j = \emptyset$;

• C é uma função de $P \cup T$ que associa a qualquer nó r um domínio de cor C(r) que é o produto cartesiano dos elementos de CB;

• W^-, W^+, W^h : W^-(p,t), W^+(p,t), W^h(p,t) $\in$ [C(t) $\rightarrow$ Bag(C(p))] são funções que rotulam respectivamente os arcos de entrada, saída e inibidores entre as transições t e lugares p;

• Pri é a função de prioridade definida como se segue: $\forall\ t \in T$, Pri(t) : C(t) $\rightarrow$ N. $Pri(t,c)$é a prioridade da instância $[t,\ c]$;

• M_0 é a marcação inicial que descreve o estado inicial do sistema;

• θ é a função definida no conjunto de transições T dado que θ(t) é a função de tempo do modelo.

2.6.1 *Software CPN Tools*

O *software CPN Tools* (36) simula tanto Redes de Petri ordinárias como Redes de Petri Coloridas complexas. Este software utiliza a linguagem CPN *Markup Language* (CPN ML), que é baseada na linguagem de programação ML (37). Usando CPN ML é possível definir estruturas com dados complexos, e funções para lidar com estas estruturas (3).

Dentre as facilidades que este software oferece, têm-se que enquanto o modelo é

desenvolvido, pode-se gerar códigos e suas respectivas análises de sintaxe. Com isto, torna-se possível simular e analisar as partes do modelo sintaxicamente corretos, enquanto as partes erradas ou incorretas são ignoradas. Foram desenvolvidas várias ferramentas de simulação eficientes que simulam modelos temporizados e/ou não temporizados, analisam o espaço de estados emitindo um relatório com o grafo de alcançabilidade do modelo CPN indicando os "bloqueios" e "vivacidade" da rede. Pode-se também criar blocos monitores que avaliam as condições da simulação como formação de filas, disparo de transições e outras funções que avaliam as condições de lugares e transições. A Figura 7 mostra a interface deste programa salientando algumas ferramentas disponíveis.

Na Figura 7, pode-se identificar a representação gráfica no *software CPN Tools* dos elementos básicos de uma RdP (LUGAR, ARCO e TRANSIÇÃO). Na aba *Create*, têm-se os ícones para inserir no modelo as transições, os lugares, os arcos, deletar os elementos do modelo, inserir transições de substituição, entre outras. Na aba *Sim* (*Simulation*), têm-se os ícones para simular o modelo desenvolvido, parar a simulação, simular o modelo passo a passo, simular o modelo para um número específico de passos e retornar o modelo no estado inicial. Por fim, na aba *SS* (*State Space*), gera-se o espaço de estados do modelo a ser simulado e na aba *Hier* (*Hierarchy*) definem-se as hierarquias do modelo (entradas e saídas). À esquerda, no ícone *Tool box*, têm-se as ferramentas disponíveis já citadas. No ícone *Help*, encontra-se disponíveis *online* vários tutoriais e dicas para solucionar problemas mais comuns durante o desenvolvimento dos modelos. No ícone *Options*, pode-se obter relatórios de simulação dos modelos. No ícone *History*, gera-se um histórico das simulações. Em *Declarations*, declaram-se as variáveis e funções utilizadas nos modelos. Em *Monitors*, criam-se blocos monitores que avaliam a simulação.

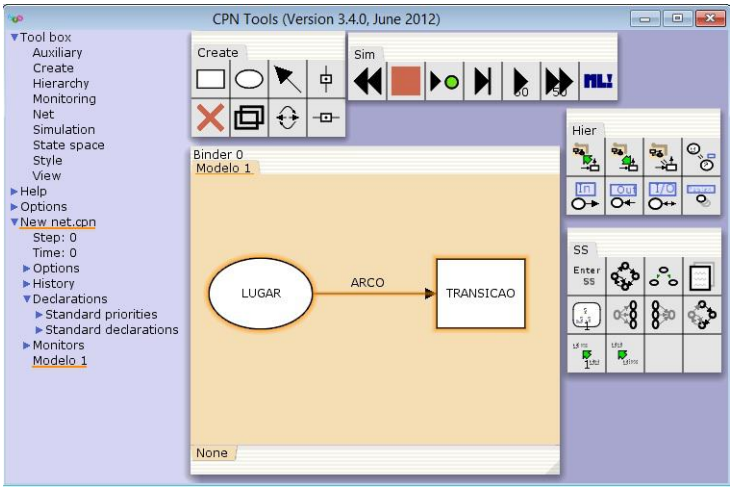

Figura 7 – Interface *software CPN Tools*

Conforme a sintaxe das CPNs, existem somente três elementos básicos na modelagem (LUGAR, ARCO e TRANSIÇÃO). A Figura 8 indica a estrutura genérica destes elementos e a estrutura no ambiente CPN Tools (3). O "LUGAR" possui a seguinte sintaxe:

nome, tipo de dado e marcações inicial e atual. Já a "TRANSIÇÃO" tem uma estrutura diferente: nome, guarda, estampa de tempo e segmento de código. O "ARCO" carrega as variáveis do sistema e tem a capacidade de aceitar trechos de código.

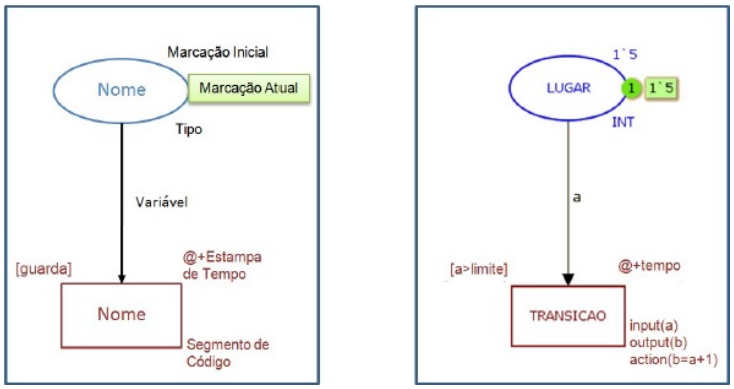

Figura 8 – Sintaxe gráfica do formalismo CPN

A semântica destes elementos é a que se segue (3):

LUGAR

• Nome: livre;

• Tipo: segue a declaração CPN ML (booleanos, inteiros, enumerações, vetores, strings, real, etc.);

• Marcação inicial: fichas que o lugar possui no estado inicial do sistema, ou seja, antes do início da simulação;

• Marcação atual: fichas que o lugar possui após certo número de passos simulados.

TRANSIÇÃO

• Nome: livre;

• Guarda: função booleana que permite ou não o disparo da transição;

• Estampa de Tempo: permite a temporização da ficha. O disparo da transição só ocorre quando a estampa de tempo for maior ou igual ao tempo de simulação;

• Segmento de código: código ML que permite a modificação de variáveis.

ARCO

• Variáveis: carrega as fichas dos lugares;

• Segmento de código: permite modificações das variáveis e outras funcionalidades da linguagem ML.

A seguir, um exemplo de transição de substituição é apresentado na Figura 9 (transição **Reverse**). Este tipo de transição será muito utilizada nos modelos desenvolvidos em Redes de Petri Coloridas, por isso, faz-se necessária uma explanação do seu

funcionamento.

Se a ficha no lugar **t** tiver um valor par (no caso, se o valor da ficha, definido como a variável **i**, for **2**), a ficha **[1,2,3,4]** no lugar **Lista** será invertida no lugar **Npar** (logo, o valor da ficha será **[4,3,2,1]**). Se a ficha no lugar **t** tiver um valor ímpar (no caso, se o valor da ficha **i** for **3**), o valor da ficha **[1,2,3,4]** no lugar **Lista** será mantido no lugar **Npar** (logo, o valor da ficha será **[1,2,3,4]**) e será enviado novamente para o lugar **Lista**.

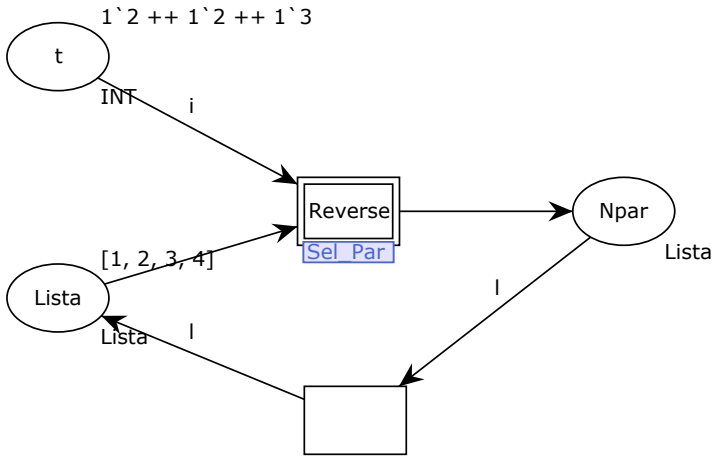

Figura 9 – Exemplo de Transição de Substituição

Na Figura 10, há o detalhamento da transição de substituição apresentada na Figura 9 (transição **Reverse**). Os lugares **Lista** e **tes**, definidos como pontos de entrada na transição **Reverse**, correspondem aos lugares **Lista** e **t**, respectivamente, da Figura 10. O lugar **Npar**, definido como ponto de saída na transição **Reverse**, corresponde ao lugar **Npar** da Figura 10. Dependendo do valor da variável **i** (se for par, a transição **Sel_par** será ativada, através da inscrição [i mod 2 =0]; se for ímpar, a transição **orig** será ativada, através da inscrição [i mod 2 <> 0]), a variável **I**, que irá assumir a ficha [1,2,3,4], manterá a sequência da ficha (se **i** for ímpar), ou irá inverter a sequência da ficha (se **i** for par).

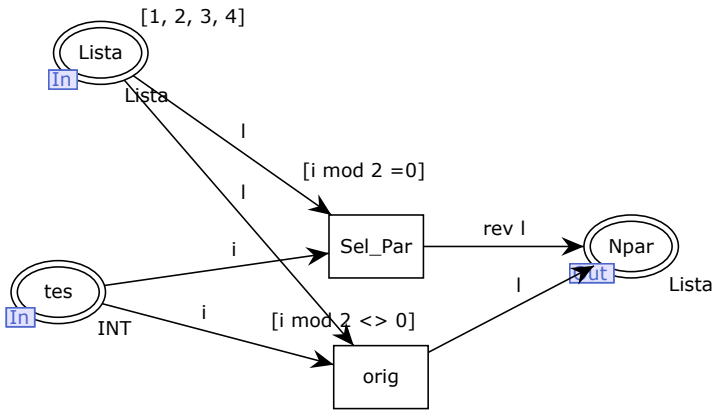

Figura 10 – Transição de Substituição **Reverse** detalhada

2.7 Modelagem de um Sistema IEC 61850 de envio de Mensagens *Sampled Values* usando Redes de Petri Coloridas

A seguir, será descrita a modelagem de um sistema IEC 61850 que envia mensagens *Sampled Values* em Redes de Petri Coloridas, apresentada em (3), que foi utilizada como base para o desenvolvimento deste trabalho. A arquitetura proposta neste trabalho utiliza onze *merging units* (MU), uma *switch* e um analisador de rede, e o modelo CPN para representar esta arquitetura física proposta pode ser visto na Figura 11. Os retângulos com linha dupla são transições de substituição e representam os dispositivos físicos correspondentes.

O modelo é composto por três tipos de transições: **MU**, **Switch** e **Analisador**, que representam respectivamente a *merging unit*, responsável pelo envio das mensagens SV; a **switch**, que realiza o chaveamento o armazenamento das mensagens; e o **Analisador**, que é utilizada para verificar os tempos de transmissão.

Cada dispositivo físico conectado ao *switch* possui uma identidade, permitindo assim a identificação da origem e do destino do pacote. Os lugares identificados no formato **Px_E** e **Px_S**, representam as portas de entrada e de saída do *switch* sendo que "x" cresce de acordo com o número de portas da *switch*.

Para o desenvolvimento destes módulos, define-se um conjunto de tipos de fichas que serão implementados. Os *color sets* e suas definições são as seguintes (3):

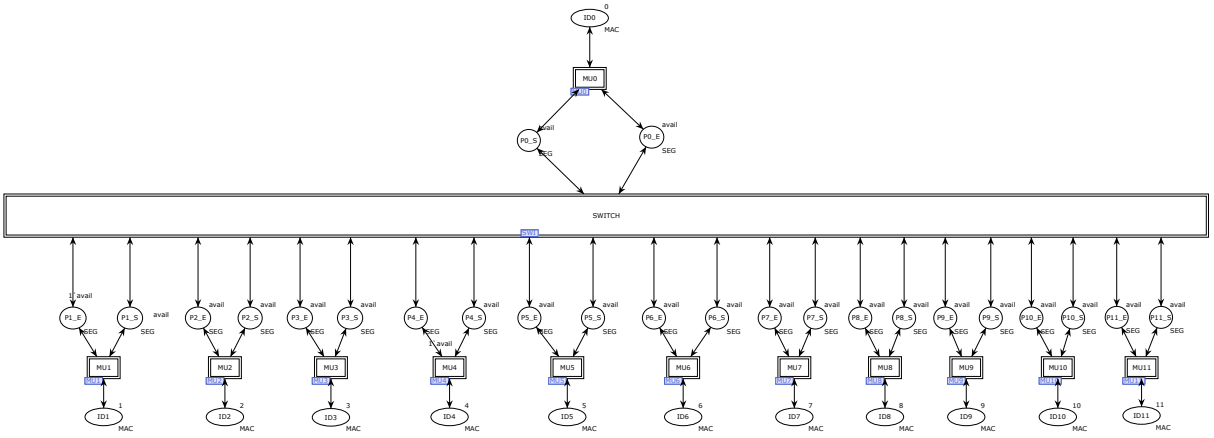

Figura 11 – Modelo da Arquitetura Proposta em (3)

```
colset MAC = int;
colset DADOS = record asdu1:INT * asdu2:INT timed;
colset TEMPO = int timed;
colset PACOTE = product MAC*MAC*DADOS*TEMPO;
colset SEG = union pac:PACOTE + avail timed;
```

Na Figura 11, o tipo **MAC** representa o endereço dos dispositivos da rede, composto por um número inteiro, enquanto que o tipo **SEG** pode carregar fichas do tipo **PACOTE** ou fichas do tipo **avail** e está conectada as portas do *switch*. As fichas do tipo **SEG** indicam quando a porta esta livre (**avail**) ou quando está a processar uma mensagem (**PACOTE**). **PACOTE** expressa o empacotamento das mensagens segundo a estrutura de destino, origem, dados, estampa de tempo. Já o tipo **DADOS** é uma classe de registro (record), composta por dois registros do tipo inteiro representando os dados que serão enviados. O **TEMPO** é tipificado com um inteiro temporizado, ou seja, suporta a estampa de tempo na simulação.

2.7.1 Modelo da *Switch*

O modelo da *switch* possui as principais características deste dispositivo. Definem-se a tabela de chaveamento, o *buffer* de pacotes, o processamento da *switch* e a interface física de comunicação (portas de entrada e sada). Para melhor entendimento deste modelo, apenas uma porta de comunicação é denida. Para a representação de outras portas, basta apenas replicar tal modelo. A figura 12 mostra as características principais de uma porta da *switch*. Este modelo tem base no trabalho desenvolvido em (38), no qual a *switch* é representada através de modelos CPN.

A figura 12 representa, em CPN, a dinâmica de um pacote dentro de um dispositivo de chaveamento real. A mensagem entra pela interface de comunicação (lugar **Porta E0**), em seguida é processada (transições **E0** e **S0**), armazenada no *buffer* (lugar **Bu0**) e em seguida é transmitida segundo a tabela de chaveamento para o respectivo destino (lugar **Swit0**). Todo este processo demanda tempo, denominado pela norma como tempo de propagação, e por tal motivo atribui-se a estampa de tempo @+tb( ) na transição **S0**.

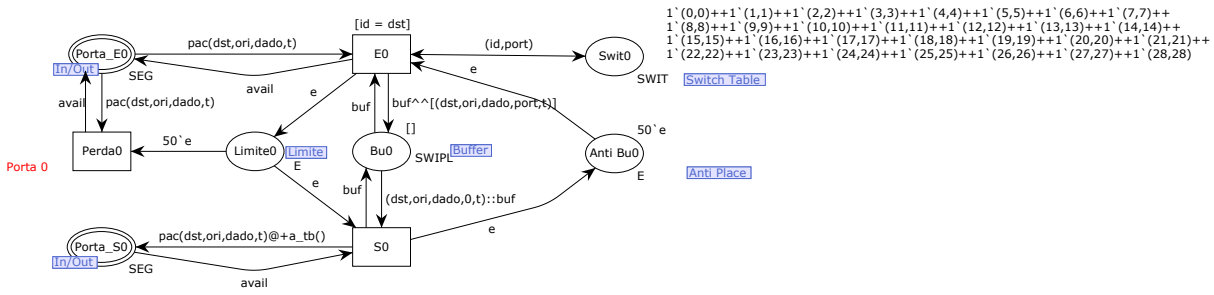

Figura 12 – Modelo da *switch* (adaptada de (3))

Para modelar estas funcionalidades, definem-se os seguintes *color sets* (3):

colset E = with e;

colset PORT = int;

colset SWIT = product INT*INT;

colset SWIP = product MAC*MAC*DADOS*PORT*TEMPO timed;

colset SWIPL = list SWIP;

O *color set* **E** é um tipo de marcação genérico para criação de fichas para limitar o *buffer*. A tipificação **PORT**, da classe inteiro, indica a numeração da porta do *switch*. As tipificações **SWIT**, **SWIP** e **SWIPL** são específicas ao modelo do *switch*, e indicam a tabela de chaveamento, os pacotes dentro do *switch* e a formação de fila respectivamente.

2.7.2 Modelo da MU (*Merging Unit*)

O modelo da figura 13 representa o dispositivo físico *merging unit* que faz a conversão dos sinais analógicos em sinais digitais e envia tais sinais no formato de mensagens *Sampled Values*. Nesta figura, os aspectos mais relevantes deste equipamento são revelados. A representação CPN da *merging unit* caracteriza o processo de amostragem, o tratamento das amostras pelos nós lógicos e a interface com a rede.

O processo de amostragem é feito a partir da leitura de um arquivo texto, denominado "*tcfile2.txt*"nesta modelagem, que contém os dados analógicos de corrente modelados que serão amostrados com valores que variam de 2 a 2000, simulando os dados de um transformador de corrente. O arquivo texto é lido através da função denida na transição **Init2**, e por meio da função **getPacketsTC( )** os dados do arquivos são transformados em fichas do tipo CPN e são enviados ao lugar **Amostras2**. As transições **Processamento2** e **EmpacotamentoSV2**, que representam os nós lógicos definidos na norma, traduzem as informações das amostras, ou fichas, e as empacota no formato *Sampled Values*. Nos lugares **LAN_E** e **LAN_S** representa-se a interface de comunicação do dispositivo. Os lugares **ORIGEM** e **DESTINO** servem para indicar à interface de comunicação a origem e o destino dos pacotes gerados pela *merging unit*. Com esta estrutura, o modelo da *merging unit* é capaz de simular dispositivos reais enviando mensagens SV.

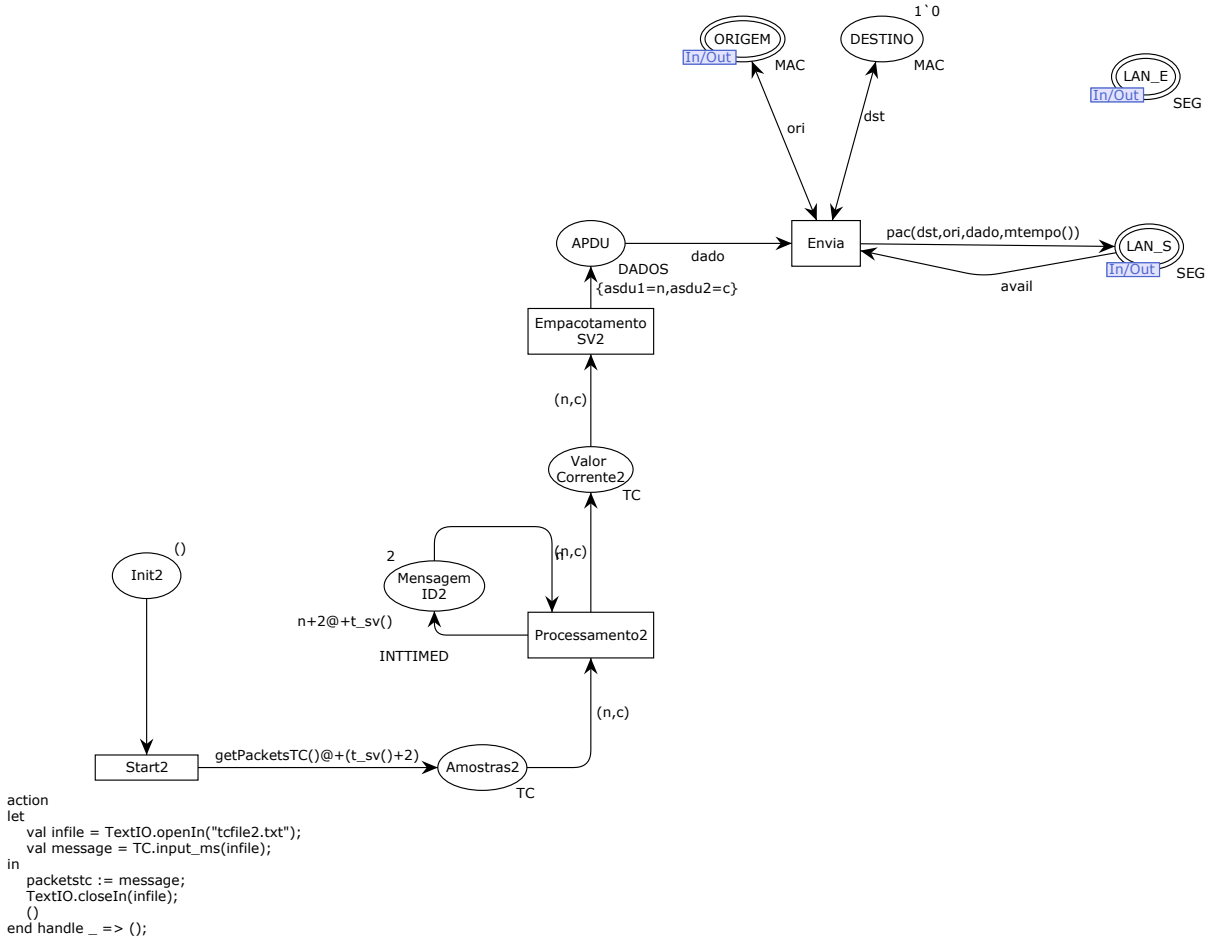

Figura 13 – Modelo da *merging unit* (MU) (adaptada de (3))

2.7.3 Modelo do Analisador

O modelo do analisador é caracterizado de forma simples conforme a Figura 14. A função deste modelo é representar o dispositivo real que verifica o tempo de latência das mensagens *Sampled Values* que trafegam na rede.

Para isso, este modelo recebe as mensagens por meio da interface de comunicação (lugar **LAN_E**) e em seguida verifica a origem do pacote (transição **Recebe** e lugar **Origem**) identificando a *merging unit* transmissora. Verificado a origem do pacote, a mensagem é enviada a transição **Buffer** onde é calculado o tempo de transferência de cada pacote SV.

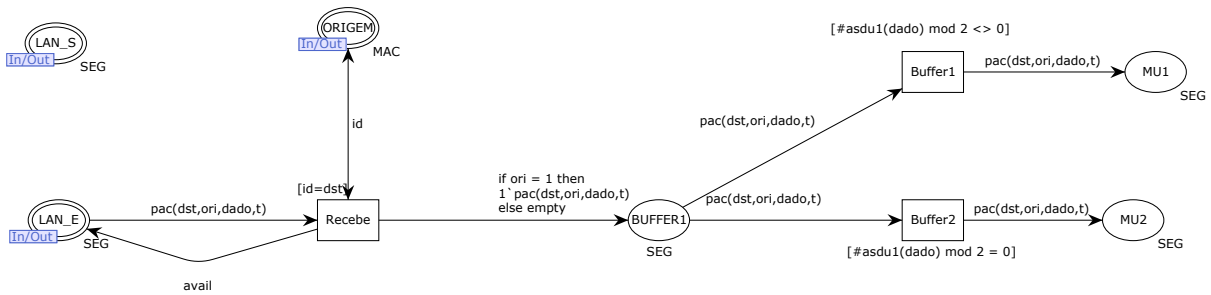

Figura 14 – Modelo do Analisador (adaptada de (3))

3 Proposta de Modelagem de um Sistema IEC 61850 com Ataque Cibernético usando Redes de Petri Coloridas

3.1 Visão Geral do Modelo

A proposta deste trabalho consiste em modelar e analisar o impacto de um ataque cibernético, modelado em Redes de Petri Coloridas, em três arquiteturas distintas, compostas por *merging units* que publicam mensagens *Sampled Values*, uma *switch* para armazenamento e envio das mensagens e um analisador de rede para verificar os pacotes recebidos, com base no trabalho desenvolvido em (3). Também será proposta uma modelagem no analisador de rede para classificar os pacotes enviados, para que seja possível identificar quais pacotes foram atacados pelo ataque cibernético modelado, ou quais pacotes não foram enviados corretamente ao seu destino final. Por fim, será proposto também um atraso de tempo em uma das arquiteturas, para avaliar o impacto do atraso de tempo na transmissão das mensagens *Sampled Values*. Este trabalho consistiu em desenvolver modificações nos modelos apresentados em (3), de tal forma que o novo modelo obtido pudesse ser interpretado como ataque cibernético, em particular de modificação de dados.

No caso da primeira arquitetura, composta por uma *merging unit* (**MU1**), uma *switch* e um analisador de rede, como pode ser visto na Figura 15, será proposto a modificação do modelo da *merging unit* **MU1**, de modo que possa ser interpretado como um ataque cibernético. Para a segunda arquitetura, será proposta a modelagem do ataque cibernético em apenas uma *merging unit* (**MU1**), a segunda *merging unit* (**MU2**) funcionará normalmente, a *switch* e o analisador de rede, como pode ser visto na Figura 16. Por fim, no caso da terceira arquitetura, será proposta a modelagem do ataque cibernético em apenas uma *merging unit* (**MU1**), a segunda *merging unit* (**MU2**) funcionará normalmente, a terceira *merging unit* (**MU3**) irá simular um problema de calibração ou de mau funcionamento do equipamento, através da leitura de dados fora da faixa de medição (valores não esperados na leitura dos dados da *merging unit*), a *switch* e o analisador de rede, como pode ser visto na Figura 17.

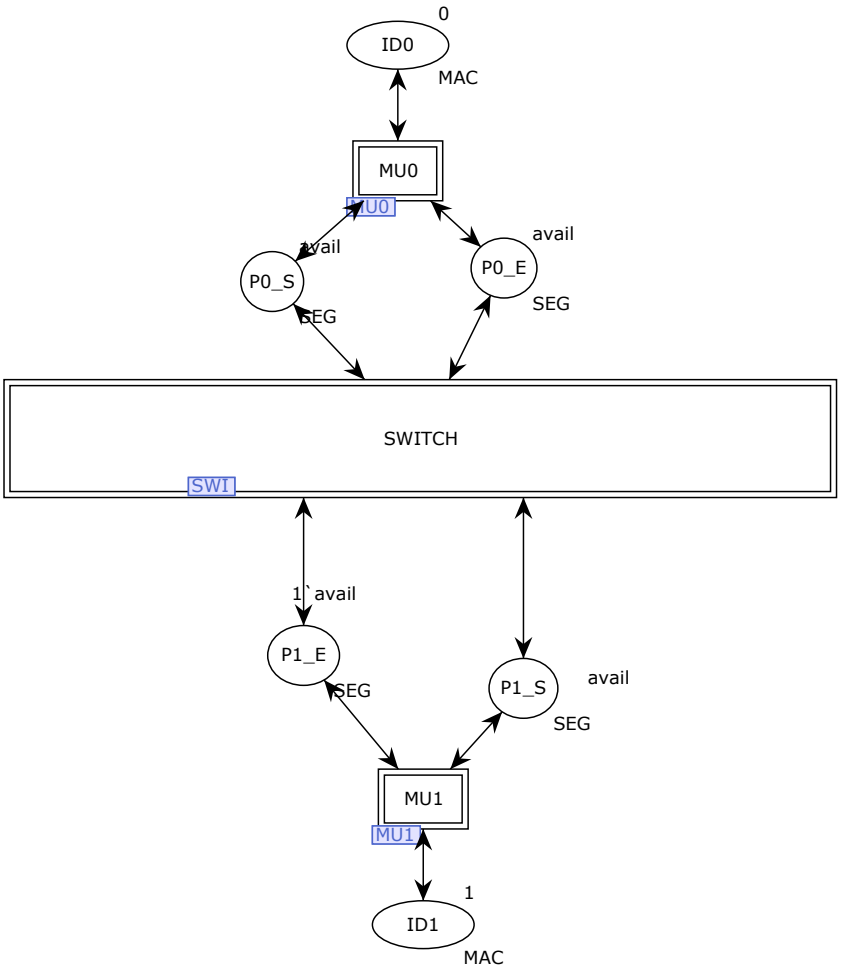

Figura 15 – Modelo da Arquitetura Proposta - 1º Cenário

Todas as *merging units* utilizadas nas três arquiteturas propostas fazem a leitura de um arquivo texto para simular a amostragem, o processamento e o empacotamento de mensagens que são valores de corrente no formato de mensagens *Sampled Values*. No caso das *merging units* **MU1** e **MU2**, o arquivo texto utilizado para leitura é denominado "*tcfile2.txt*", e este arquivo texto contém os dados analógicos de corrente modelados que serão amostrados com valores pares e crescentes, que iniciam de 2 e vão até 2000, num total de 1.000 valores que serã lidos, simulando os dados de um transformador de corrente. No entanto, para o caso da *merging unit* **MU3**, o arquivo texto utilizado para leitura é denominado "*tcfile4.txt*", e este arquivo texto contém os dados analógicos de corrente modelados que serão amostrados com valores pares e crescentes, que iniciam de 2002 e vão até 4000, num total de 1.000 valores que serã lidos, simulando os dados de um transformador de corrente. Como já foi dito anteriormente, a **MU3** irá simular um problema de calibração ou de mau funcionamento do equipamento, através da leitura de dados fora da faixa de medição (valores não esperados na leitura dos dados da *merging unit*, que no caso, seriam de 2 até 2000, como modelado no arquivo "*tcfile2.txt*"para a **MU1** e a **MU2**). Como trabalho futuro, teremos a seguinte questão a ser resolvida: há um ata-

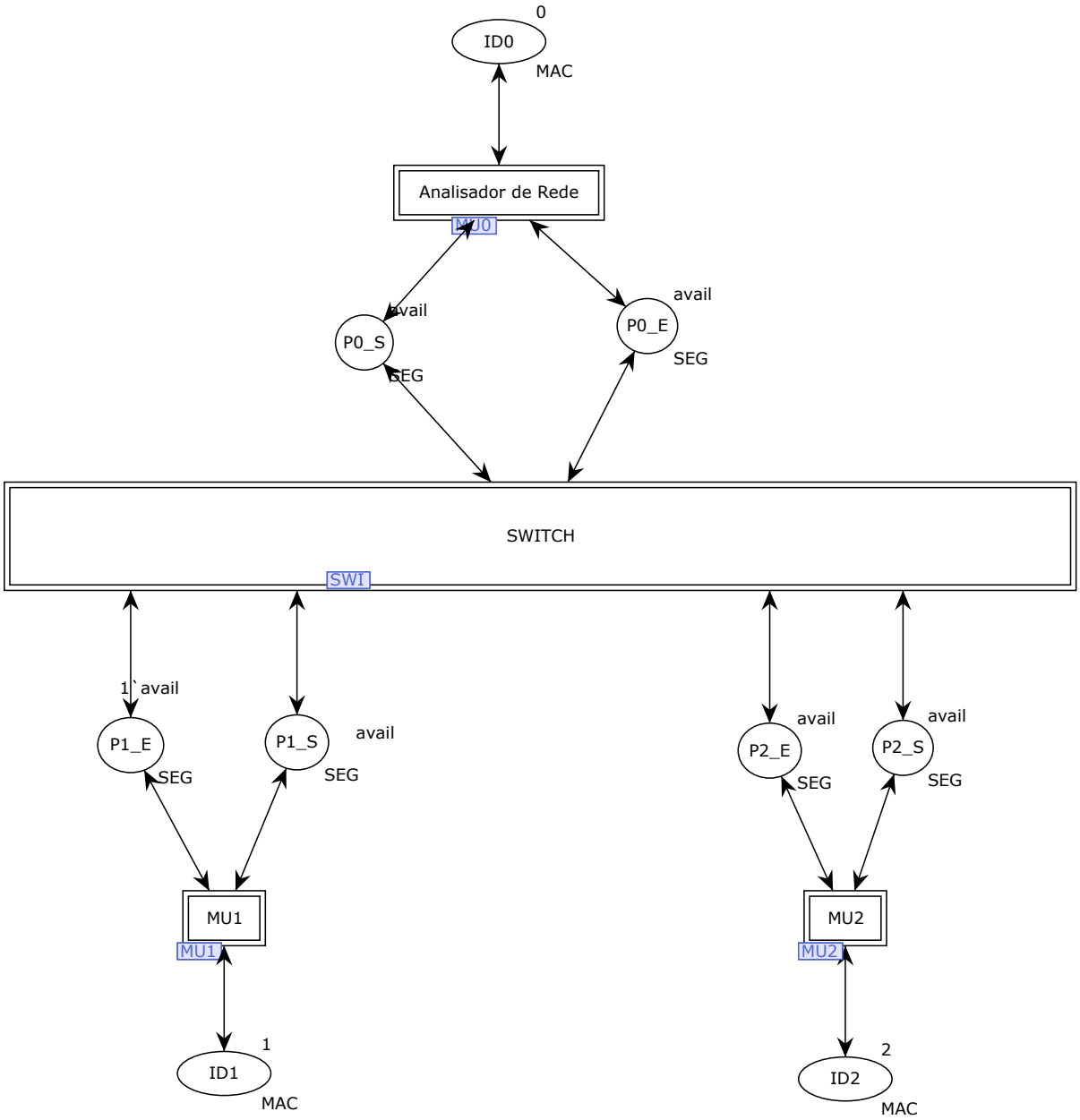

Figura 16 – Modelo da Arquitetura Proposta - 2º Cenário

que cibernético ou um problema de calibração do equipamento, no caso da **MU3**? Uma análise deverá ser feita para verificar o problema e classificar corretamente o incidente de segurança.

Na Figura 18 é apresentado um esquema que exemplifica quais arquivos de entrada de dados ("*tcfile2.txt*"ou "*tcfile4.txt*") são utilizados por cada *Merging Unit*, além de especificar em qual *Merging Unit* irá ocorrer o ataque cibernético modelado neste trabalho, em cada uma das três arquiteturas propostas.

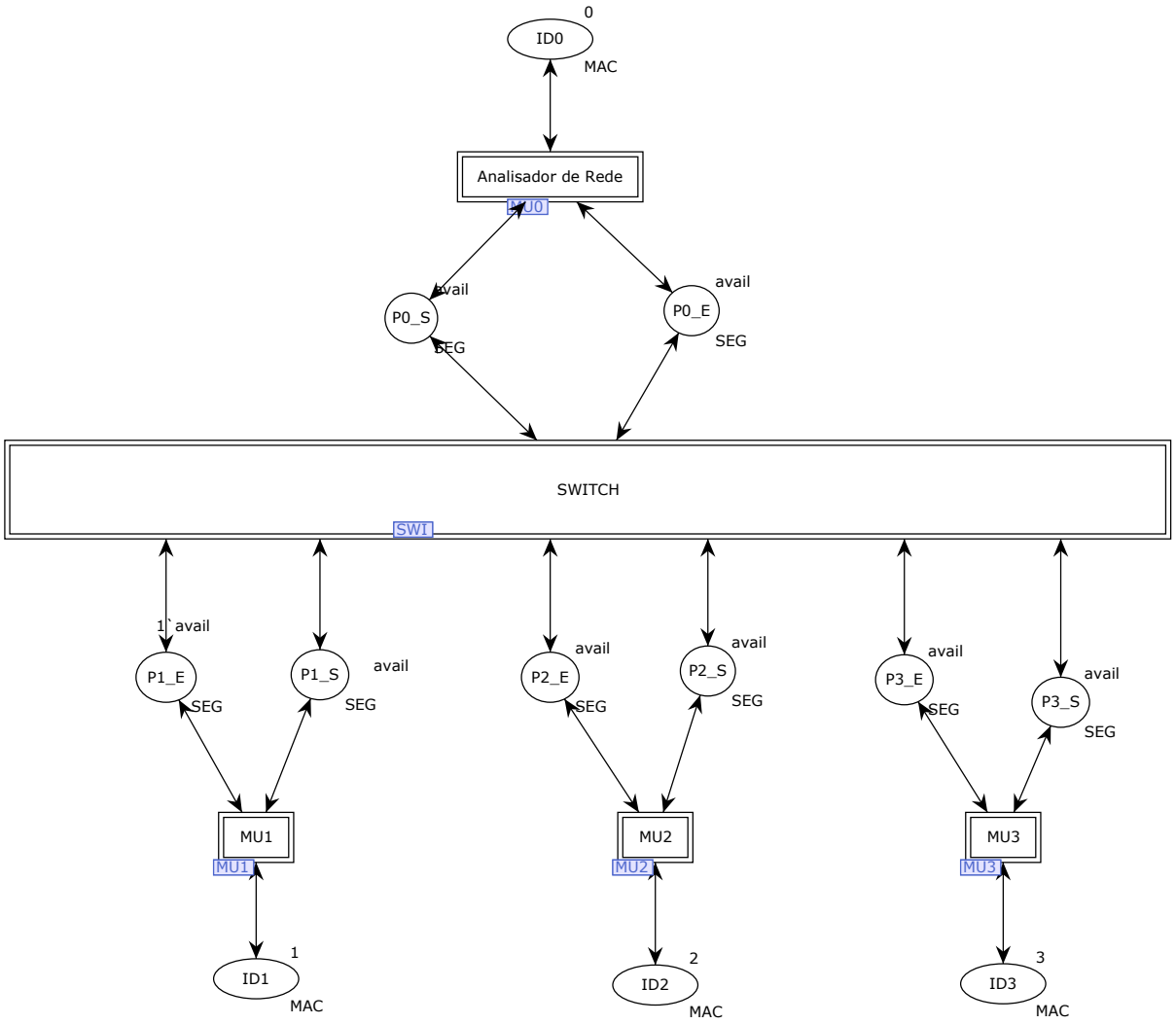

Figura 17 – Modelo da Arquitetura Proposta - 3º Cenário

Em relação ao analisador de rede, foi modelada uma classificação para os pacotes de mensagens transmitidos, para que seja possível determinar quais pacotes foram atacados pelo ataque cibernético, ou quais pacotes não foram corretamente enviados ao seu destino final.

As transições **Buffer3**, **Buffer4**, **Buffer5** e **Buffer6** irão classificar os dados, respectivamente, em dados com valores normais (lugar **MU3**), em dados nulos (lugar **MU4**), em dados com identificador de mensagem adulterado (lugar **MU5**) ou em dados fora da faixa de leitura (lugar **MU6**), dependendo do valor recebido pelo lugar **MU2**.

Se a transição **Buffer3** for disparada, a seguinte condição terá sido satisfeita, conforme a inscrição da transição: [#asdu1(dado) < 2000 andalso #asdu1(dado) = 2000 andalso #asdu1(dado) <> 0 andalso #asdu2(dado) = 5]. Para que o dado seja classificado como valor normal, teremos que seu valor deve ser menor ou igual a 2000, não deve ser igual a 0 e o identificador da mensagem deve ser igual a 5. Caso esta condição seja satisfeita, o pacote será enviado ao lugar **MU3**.

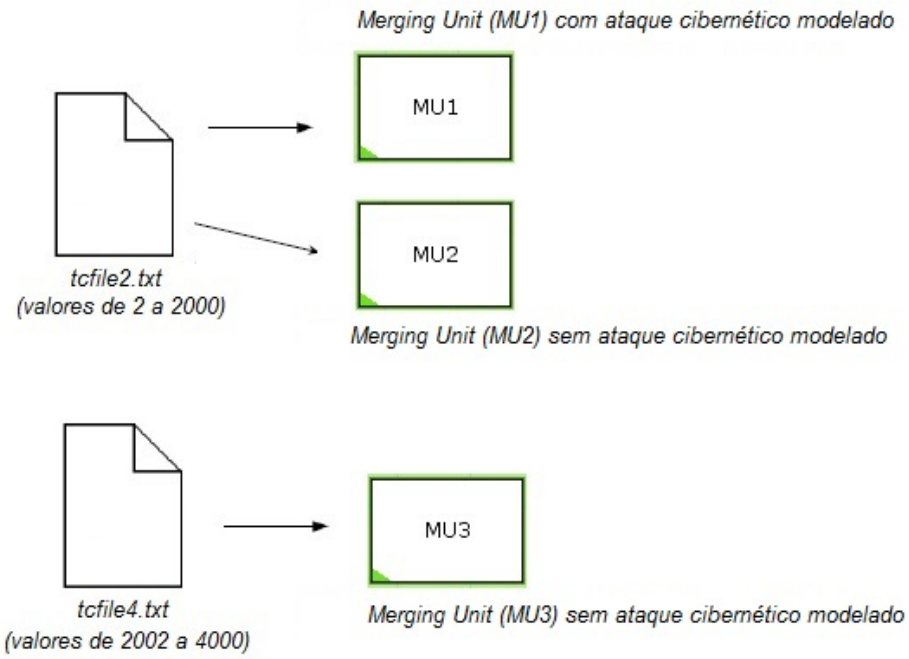

Figura 18 – *Merging Units* e seus respectivos arquivos de leitura de dados

Caso a transição **Buffer4** for disparada, a seguinte condição terá sido satisfeita, conforme a inscrição da transição: [#asdu1(dado) = 0]. Para que o dado seja classificado como valor nulo, seu valor deve ser igual a 0. Caso esta condição seja satisfeita, o pacote será enviado ao lugar **MU4**.

Se a transição **Buffer5** for disparada, a seguinte condição terá sido satisfeita, conforme a inscrição da transição: [#asdu2(dado) <> 5]. Para que o dado seja classificado como dado com identificador de mensagem adulterado, seu valor de identificador da mensagem deve ser diferente de 5. Caso esta condição seja satisfeita, o pacote será enviado ao lugar **MU5**.

Finalmente, se a transição **Buffer6** for disparada, a seguinte condição terá sido satisfeita, conforme a inscrição da transição: [#asdu1(dado) > 2000]. Para que o dado seja classificado como dado com valor fora da faixa de leitura, seu valor deve ser maior que 2000. Caso esta condição seja satisfeita, o pacote será enviado ao lugar **MU6**.

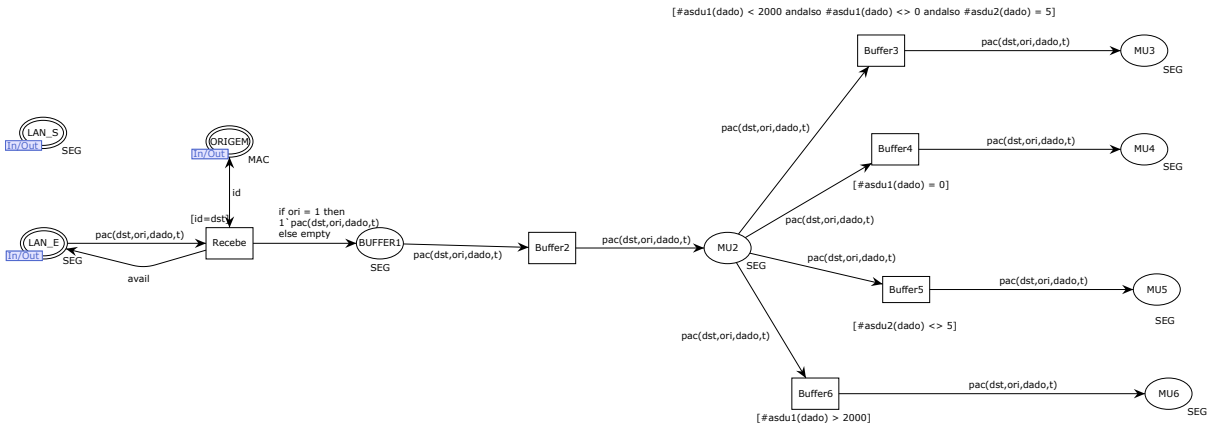

Figura 19 – Modelo do Analisador

3.2 Modelagem de um Ataque Cibernético em Redes de Petri Coloridas

Na modelagem de ataque cibernético apresentado em vermelho na Figura 20, o objetivo do ataque modelado *Data Modification* é modificar os dados a serem transmitidos antes que esses dados sejam empacotados como mensagens *Sampled Values*(SV). Neste caso, o valor dos dados analógicos vindos do transformador de corrente serão modificados (atacados) antes que sejam empacotados como mensagens (SV).

Além disso, conforme foi definido na seção 2.2, item *B* desta dissertação, a modificação de dados ocorre geralmente nos ambientes de entrada de dados, fato que se verifica, pois as *merging units* são dispositivos eletrônicos que coletam e enviam dados, o que caracteriza, de forma clara, um ambiente de entrada de dados.

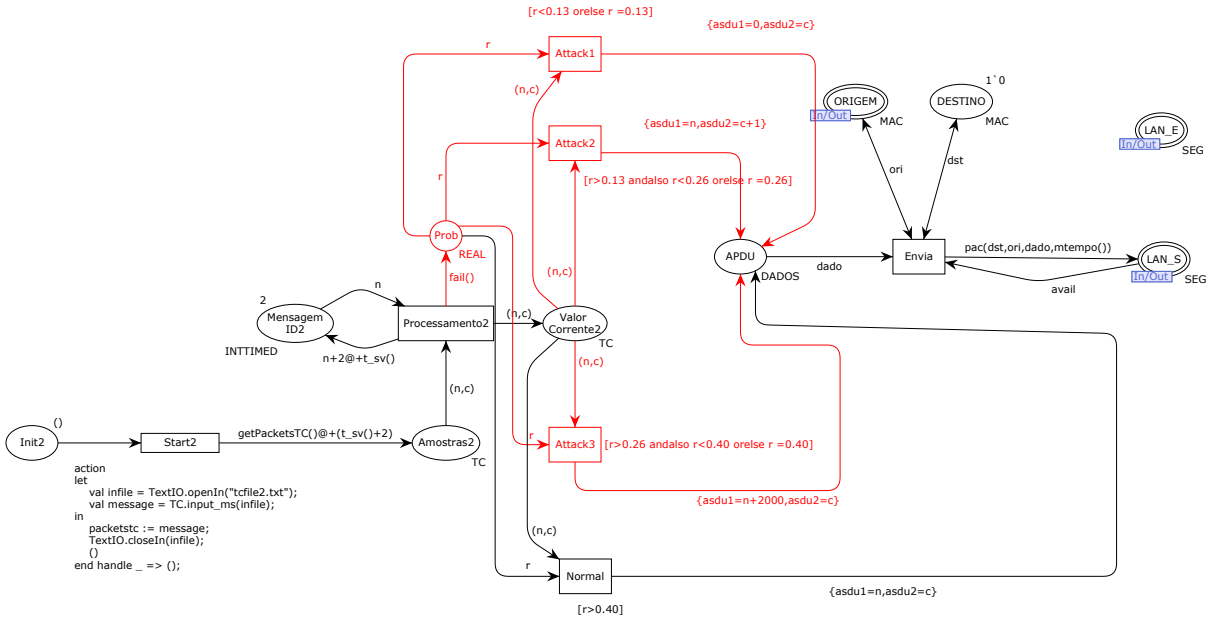

Figura 20 – Modelo de Ataque Cibernético em Redes de Petri

Para a modelagem do ataque cibernético porposto neste trabalho, na transição **Processamento2** foi criada a função *fail*(), uma distribuição uniforme que gera um valor aleatório entre 0 e 1. Assim que esse valor aleatório for gerado, esse valor vai para o lugar **Prob**. Dependendo desse valor, assumido pela variável r no modelo, a transição **Normal**, a transição **Attack1**, a transição **Attack2** ou a transição **Attack3** serão habilitadas. Para habilitar a transição **Attack1**, o valor de r gerado aleatoriamente deve ser menor ou igual a 0,13. Para habilitar a transição **Attack2**, o valor de r gerado aleatoriamente deve ser maior que 0,13 e menor ou igual a 0,26. Para habilitar a transição **Attack3**, o valor de r gerado aleatoriamente deve ser maior que 0,26 e menor ou igual a 0,40. Por fim, para habilitar a transição **Normal**, o valor de r gerado aleatoriamente deve ser maior que 0,40. Isso indica uma probabilidade de ataque cibernético de 40%. Essa probabilidade de ataque cibernético de 40% foi obtida com base em um levantamento feito em 2016 pela Kaspersky Lab ICS CERTS (39).

Para o correto funcionamento do modelo e da amostragem de sinais, após o processamento das transições **Attack1**, **Attack2**, **Attack3** ou **Normal**, foi necessário redefinir as variáveis n e c para *asdu1* e *asdu2*, respectivamente. Essa redefinição serve para garantir o correto empacotamento dos dados no lugar **APDU** como mensagens *Sampled Value*.

Se a transição **Normal** estiver habilitada, o processamento das mensagens ocorre normalmente. A inscrição do arco **{asdu1=n,asdu2=c}** da transição **Normal** apenas redefine as variáveis n e c para *asdu1* e *asdu2*, mas não faz nenhuma outra alteração, transmitindo os pacotes normalmente. Porém, se alguma das transições **Attack1**, **Attack2** ou **Attack3** estiver habilitada, o valor dos dados analógicos de corrente provenientes dos transformadores de corrente serão modificados (atacados).

No caso da transição **Attack1** estar habilitada, conforme o valor de r gerado aleatoriamente, os valores serão anulados. Para o disparo desta transição, o valor de r deve ser menor ou igual a 0,13. Caso ocorra essa situação, a transição **Attack1** irá pegar o pacote no lugar **Valor Corrente2** e através da inscrição em seu arco de disparo **{asdu1=0,asdu2=c}**, o valor da corrente será anulado (**asdu1=0**) e será mantido o número identificador da mensagem (**asdu2=c**).

Para o caso da transição **Attack2** estar habilitada, conforme o valor de r gerado aleatoriamente, será alterado o identificador das mensagens. Para o disparo desta transição, o valor de r deve ser maior que 0,13 e menor ou igual a 0,26. Caso ocorra essa situação, a transição **Attack2** irá pegar o pacote no lugar **Valor Corrente2** e através da inscrição em seu arco de disparo **{asdu1=n,asdu2=c+1}**, o número identificador da mensagem será alterado (**asdu2=c+1**) e o valor da corrente será mantido (**asdu1=n**).

No caso da transição **Attack3** estar habilitada, conforme o valor de r gerado aleatoriamente, os valores serão alterados para outros valores fora das faixas das medi-

ções elétricas esperadas. Para o disparo desta transição, o valor de r deve ser maior que 0,26 e menor ou igual a 0,40. Caso ocorra essa situação, a transição **Attack3** irá pegar o pacote no lugar **Valor Corrente2** e através da inscrição em seu arco de disparo **{asdu1=n+2000,asdu2=c}**, os valores serão alterados para outros valores fora das faixas das medições elétricas esperadas (**asdu1=n+2000**), neste caso as medidas dos valores de corrente vão apresentar um *offset* de 2000 dos valores originais e será mantido o número identificador da mensagem (**asdu2=c**).

Após o disparo das transições **Normal**, **Attack1**, **Attack2** ou **Attack3** e o correto empacotamento dos dados no lugar **APDU** como mensagens *Sampled Value*,em que as variáveis **asdu1** e **asdu2** são unidas através da variável *dado*, O padrão em que a mensagem será enviada é definido pelo *color set* **SEG**, após o disparo da transição **Envia**, carregando o destino do pacote (lugar **DESTINO**), sua origem (lugar **ORIGEM**), os dados com o valor da corrente e o número identificador da mensagem (variável *dado*), e a estampa de tempo indicando o momento que a mensagem saiu do dispositivo (variável t). As portas **LAN_E** e **LAN_S** representam interfaces de entrada e saída do dispositivo e também estão conectadas aos lugares que representam as portas da *switch*.

De acordo com o arquivo "*tcfile2.txt*", que contém os dados analógicos de corrente modelados para essa simulação e que será lido pelas *merging units* **MU1** e **MU2**, os valores de corrente variam de 2 a 2000. O ataque de *Data Modification* desenvolvido nesta simulação apenas na **MU1** em cada uma das três arquiteturas propostas irá alterar (modificar) esses dados analógicos de corrente, anulando esses valores (através da transição **Attack1**), alterando o identificador das mensagens (através da transição **Attack2**) ou acrescentando um *offset* de 2000 aos valores originais (através da transição **Attack3**).

Conforme foi dito no início deste capítulo, modelou-se também um atraso de tempo para a primeira arquitetura, obtendo-se assim um quarto cenário proposto, para avaliar o impacto do atraso de tempo na transmissão das mensagens *Sampled Values*. Para a modelagem deste atraso de tempo, foi criada a função *delay_attack()*, uma distribuição normal que gera um valor aleatório com média 10 e variância 2, implementada em cada uma das transições de ataque (**Attack1**, **Attack2** e **Attack3**). Isto pode ser visto na Figura 21.

Embora essas pequenas modificações nos dados a serem transmitidos possam parecer inicialmente simples, elas se mostram bem eficazes com relação aos objetivos a serem alcançados pelo ataque cibernético, visto que dados completamente adulterados podem implicar em mau funcionamento dos sistemas de controle e proteção das subestações de energia elétrica, além de atuações indevidas de disjuntores e relés de proteção, que podem danificar seriamente as subestações.

Pode-se verificar que além de ser um ataque cibernético de *Data Modification*, definido no Capítulo 2 desta dissertação, este ataque cibernético modelado pode também ser

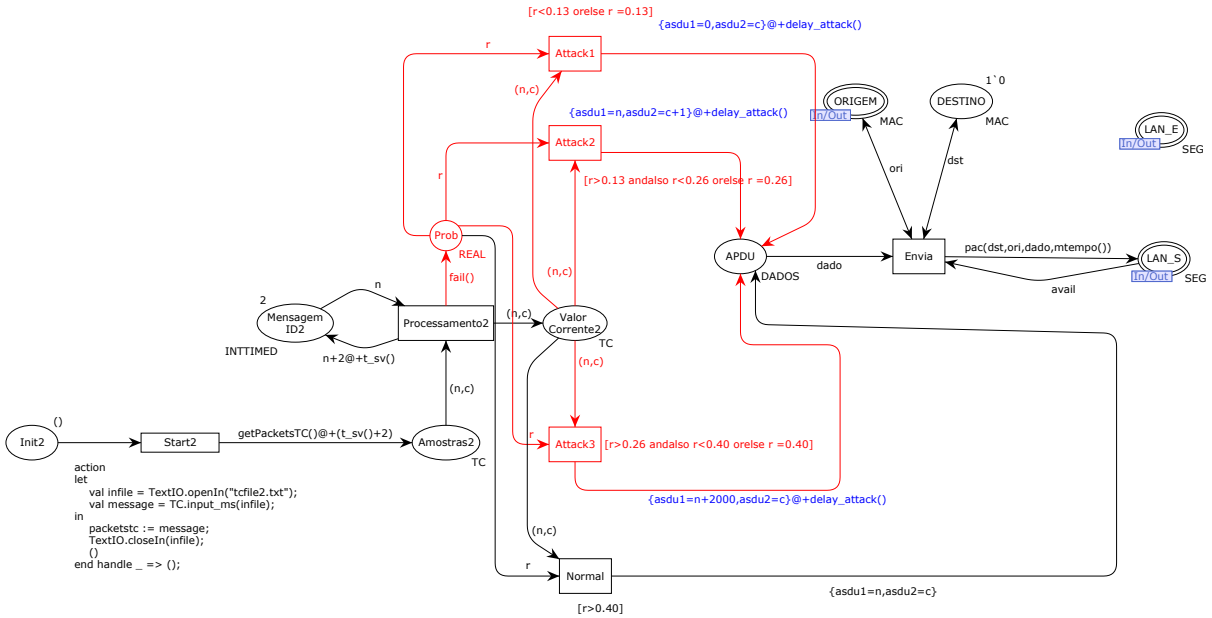

Figura 21 – Modelo de Ataque Cibernético em Redes de Petri com Atraso de Tempo

caracterizado como um ataque *Man-in-the-Middle*, pois o invasor intercepta ou subverte as comunicações e fornece dados falsos ao usuário do sistema. Outra possível classificação para esse ataque cibernético seria um ataque cibernético de um *insider* ou ataque de acesso direto, pois apenas pessoal autorizado tem acesso às *merging units* para executar esse ataque modelado e neste caso, o invasor manipula deliberadamente os dispositivos do sistema de energia para produzir uma condição não autorizada, visto que é considerado um usuário confiável.

4 Resultados e Análises dos Modelos em Redes de Petri

4.1 Análise dos Resultados gerados pela simulação

Para análise do ataque cibernético proposto neste trabalho, foram utilizadas as ferramentas de simulação disponíveis no software *CPN Tools*. Foram realizadas quatro simulações distintas para cada um dos três cenários propostos. Além destes três cenários previamente apresentados, foi simulado também em um quarto cenário a mesma arquitetura proposta no 1º cenário, porém com uma função de atraso de tempo denominada *delay_attack()*.

4.1.1 Simulações para o 1º Cenário:

Seguem-se as tabelas e os gráficos com os resultados gerados pelas simulações do modelo proposto no 1º cenário:

Tabela 2 – Transmissão de Mensagens e Dados Modificados - 1ª Simulação

Transmissão de Mensagens	**Número de Mensagens**
Normal	7
Dados Anulados	2
Alteração do Identificador das Mensagens	0
Valores Fora da Faixa de Medição	1

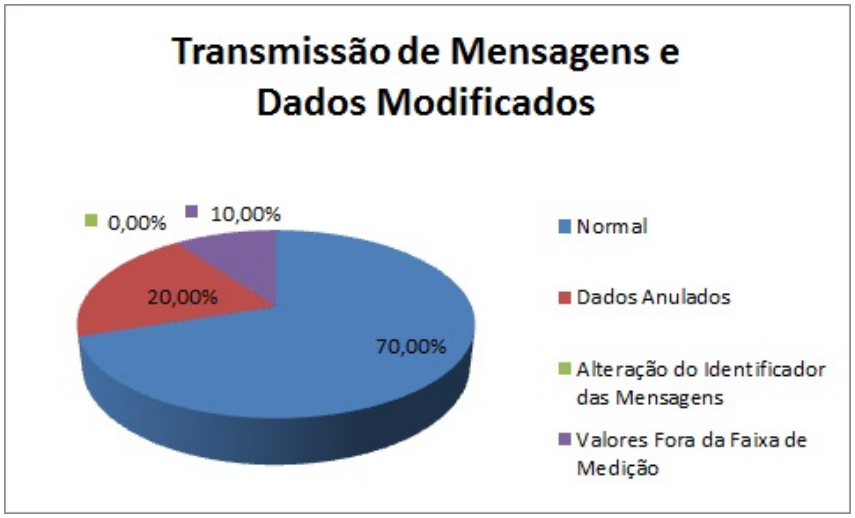

Figura 22 – 3 dados modificados em 10 dados recebidos

Tabela 3 – Transmissão de Mensagens e Dados Modificados - 2ª Simulação

Transmissão de Mensagens	**Número de Mensagens**
Normal	14
Dados Anulados	2
Alteração do Identificador das Mensagens	0
Valores Fora da Faixa de Medição	4

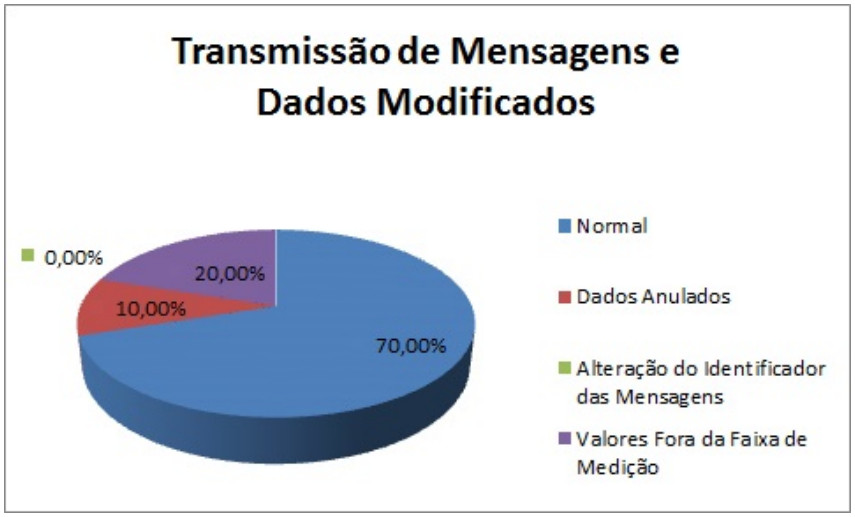

Figura 23 – 6 dados modificados em 20 dados recebidos

Tabela 4 – Transmissão de Mensagens e Dados Modificados - 3ª Simulação

Transmissão de Mensagens	**Número de Mensagens**
Normal	101
Dados Anulados	19
Alteração do Identificador das Mensagens	24
Valores Fora da Faixa de Medição	16

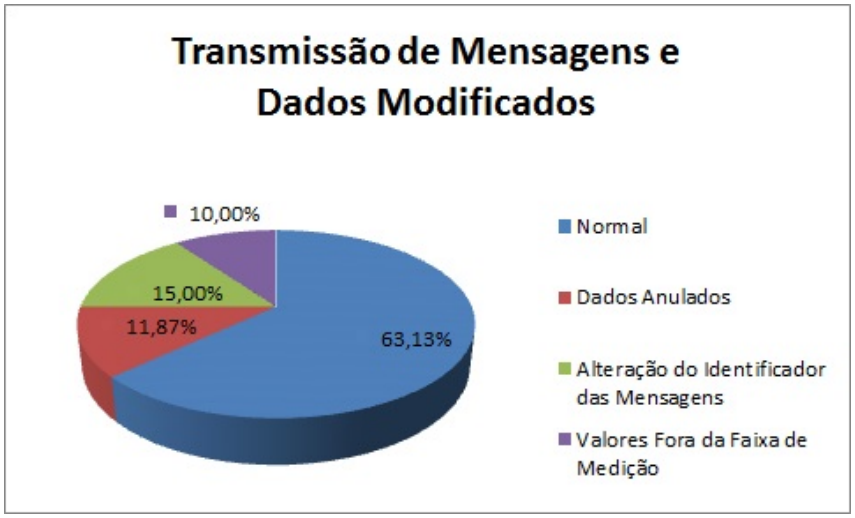

Figura 24 – 59 dados modificados em 160 dados recebidos

Tabela 5 – Transmissão de Mensagens e Dados Modificados - 4ª Simulação

Transmissão de Mensagens	**Número de Mensagens**
Normal	588
Dados Anulados	127
Alteração do Identificador das Mensagens	144
Valores Fora da Faixa de Medição	141

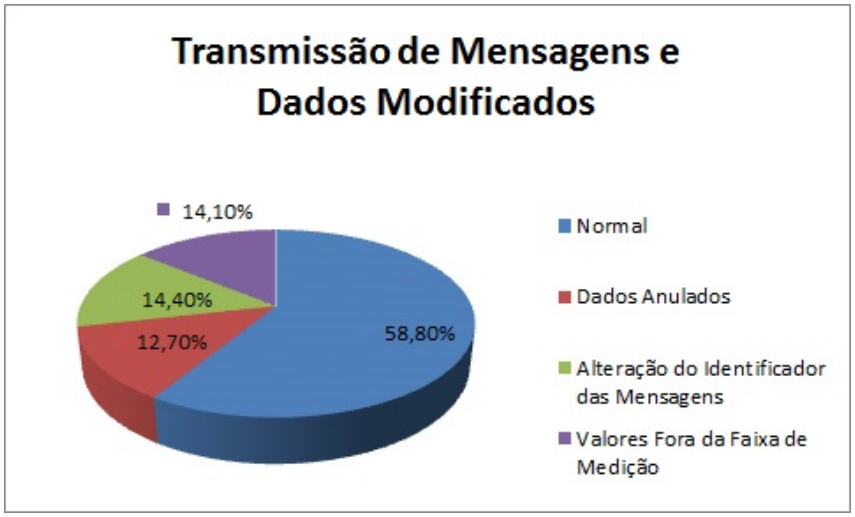

Figura 25 – 412 dados modificados em 1000 dados recebidos

Como se pode notar na Tabela 2 e na Figura 22, 7 pacotes de mensagens foram enviados corretamente ao destino final, 2 pacotes tiveram seus valores anulados (**asdu1 = 0**), não houve pacotes com identificador de mensagem adulterado de (**asdu2 = 5**) para (**asdu2 = 6**), conforme foi modelado neste trabalho e 1 pacote teve seu valor adulterado para valores fora das faixas de medições elétricas (valores de **asdu1** acima de 2000).

No caso da Tabela 3 e da Figura 23, 14 pacotes de mensagens foram enviados corretamente ao destino final, 2 pacotes tiveram seus valores anulados (**asdu1 = 0**), não houve pacotes com identificador de mensagem adulterado de (**asdu2 = 5**) para (**asdu2 = 6**), conforme foi modelado neste trabalho e 4 pacotes tiveram seus valores adulterados para valores fora das faixas de medições elétricas (valores de **asdu1** acima de 2000).

No caso da Tabela 4 e da Figura 24, 101 pacotes de mensagens foram enviados corretamente ao destino final, 19 pacotes tiveram seus valores anulados (**asdu1 = 0**), 24 pacotes tiveram o identificador de mensagens adulterado de (**asdu2 = 5**) para (**asdu2 = 6**), conforme foi modelado neste trabalho e 16 pacotes tiveram seus valores adulterados para valores fora das faixas de medições elétricas (valores de **asdu1** acima de 2000).

No caso da Tabela 5 e da Figura 25, 588 pacotes de mensagens foram enviados corretamente ao destino final, 127 pacotes tiveram seus valores anulados (**asdu1 = 0**), 144 pacotes tiveram o identificador de mensagens adulterado de (**asdu2 = 5**) para (**asdu2 = 6**), conforme foi modelado neste trabalho e 141 pacotes tiveram seus valores adulterados para valores fora das faixas de medições elétricas (valores de **asdu1** acima de 2000).

Os valores apresentados foram atacados por um ataque de modificação de dados, conforme foi proposto neste trabalho, porque o objetivo final desse tipo de ataque é mudar os dados antes de serem processados no destino final, e esse objetivo foi alcançado. No caso da última simulação, para 1000 pacotes enviados, 41,2% dos pacotes foram atacados pelos ataques cibernéticos modelados, o que está de acordo com probabilidade de ataque cibernético de 40% proposta neste modelo e obtida com base em um levantamento feito em 2016 pela Kaspersky Lab ICS CERTS (39).

Além disso, a classificação proposta no Analisador de Rede atuou corretamente, confirmando a modelagem sólida do sistema definido inicialmente nesse trabalho.

4.1.2 Simulações para o 1° Cenário com Atraso de Tempo

Seguem-se as tabelas (Tabela 6 e 7) com os resultados gerados pelas simulações do modelo proposto,como pode ser visto nas Figuras 26 e 27:

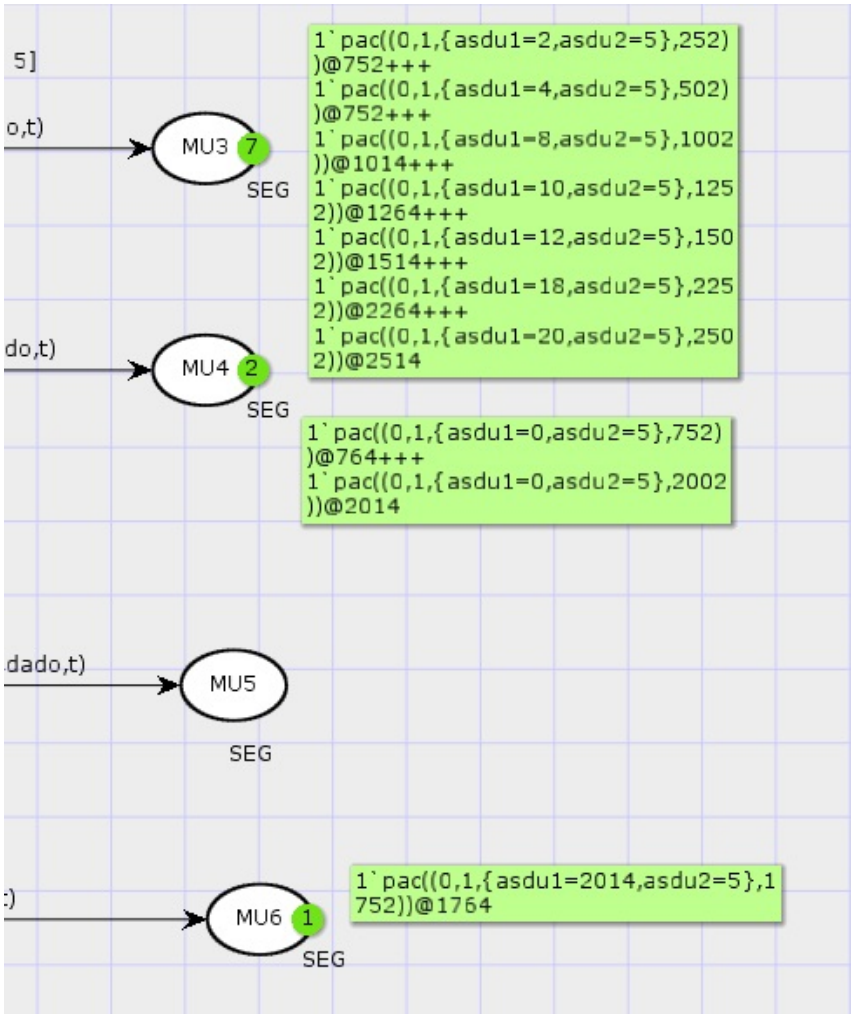

Figura 26 – Tempo de Transmissão dos Dados - 1ª Simulação

Comparando-se as Tabelas 6 e 7, obtidas com base nos dados apresentados nas Figuras 26 e 27, pode-se notar que os dados *3*, *5* e *8* tiveram um atraso de 11 microsegundos no seu tempo de transmissão. Estes atrasos de tempo estão de acordo com a função de atraso de tempo modelada, *delay_attack()*.

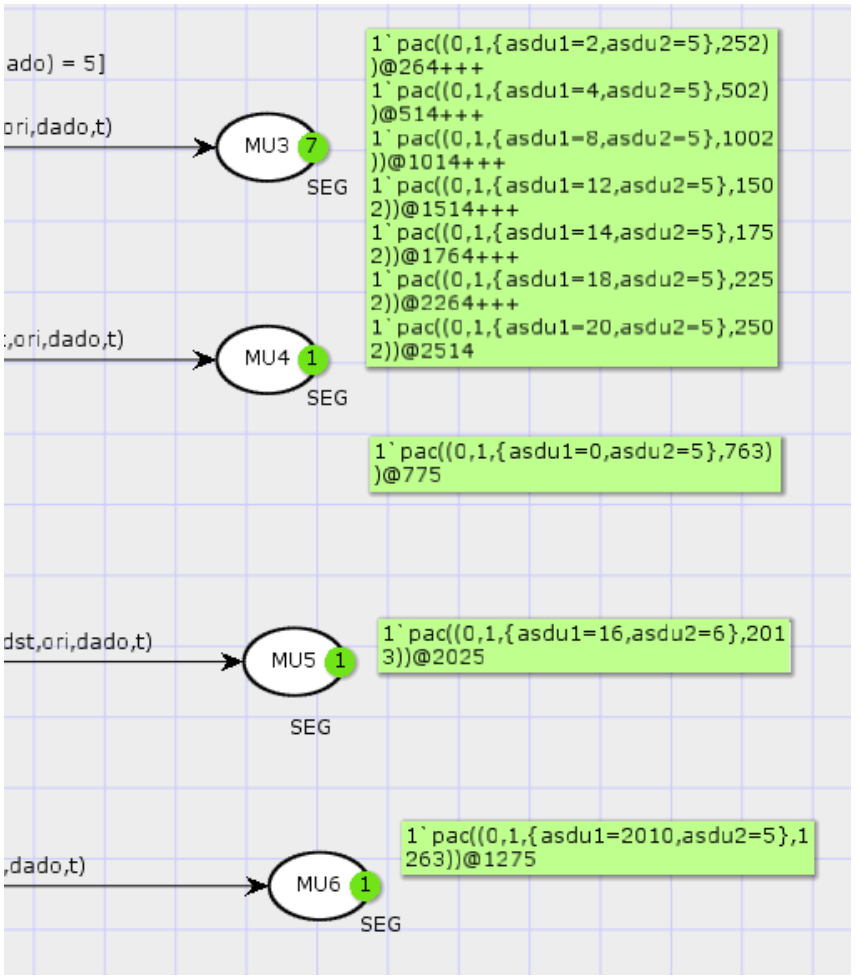

Figura 27 – Tempo de Transmissão e Dados Atrasados - 2ª Simulação com Atraso de Tempo

Sabendo-se que qualquer atraso no tempo de transmissão das mensagens *Sampled Values* pode afetar os sistemas de proteção e controle dos sistemas de potência, porque seus quadros de mensagens usam a camada 1 do modelo TCP/IP e são extremamente rápidas, estes atrasos de tempo modelados neste cenário IEC 61850 poderiam levar à problemas de operação de disjuntores e relés de proteção, e poderiam gerar sérios problemas para as subestações de energia elétrica.

Tabela 6 – Envio de Dados e Tempo de Transmissão - 1ª Simulação

Dado	**Tempo de Transmissão (microsegundos)**
1	252
2	502
3	**752**
4	1002
5	**1252**
6	1502
7	1752
8	**2002**
9	2252
10	2502

Tabela 7 – Envio de Dados e Tempo de Transmissão - 2ª Simulação com Atraso de Tempo

Dado	**Tempo de Transmissão (microsegundos)**
1	252
2	502
3	**763**
4	1002
5	**1263**
6	1502
7	1752
8	**2013**
9	2252
10	2502

4.1.3 Simulações para o 2º Cenário:

Seguem-se as tabelas e os gráficos com os resultados gerados pelas simulações do modelo proposto no 2º cenário:

Tabela 8 – Transmissão de Mensagens e Dados Modificados - 1ª Simulação

Transmissão de Mensagens	**Número de Mensagens**
Normal	16
Dados Anulados	1
Alteração do Identificador das Mensagens	1
Valores Fora da Faixa de Medição	2

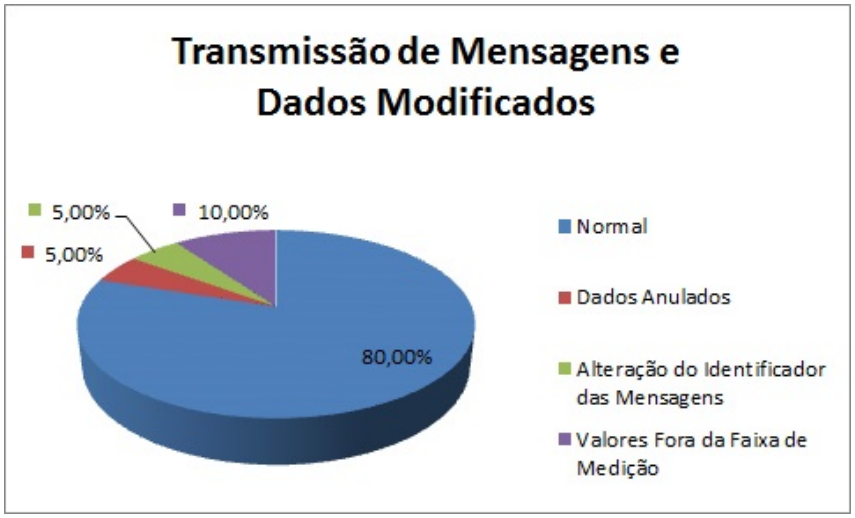

Figura 28 – 4 dados modificados em 20 dados recebidos

Tabela 9 – Transmissão de Mensagens e Dados Modificados - 2ª Simulação

Transmissão de Mensagens	**Número de Mensagens**
Normal	30
Dados Anulados	3
Alteração do Identificador das Mensagens	3
Valores Fora da Faixa de Medição	4

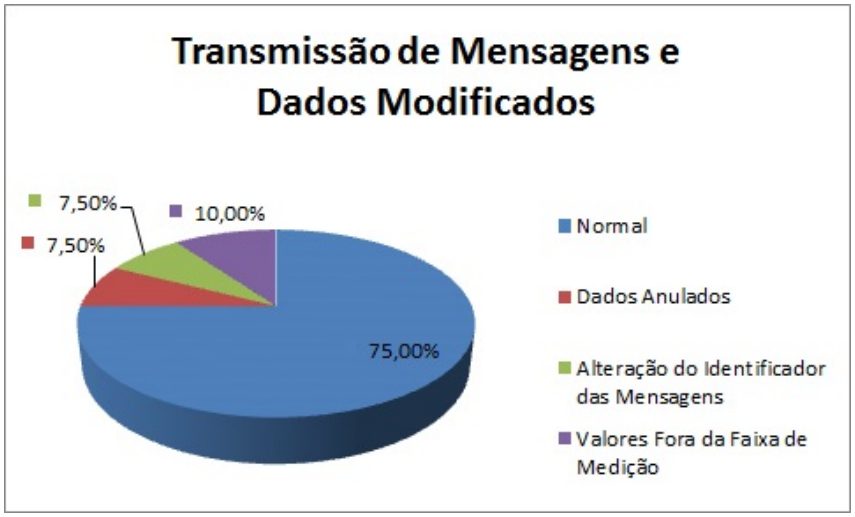

Figura 29 – 10 dados modificados em 40 dados recebidos

Tabela 10 – Transmissão de Mensagens e Dados Modificados - 3ª Simulação

Transmissão de Mensagens	**Número de Mensagens**
Normal	262
Dados Anulados	20
Alteração do Identificador das Mensagens	22
Valores Fora da Faixa de Medição	16

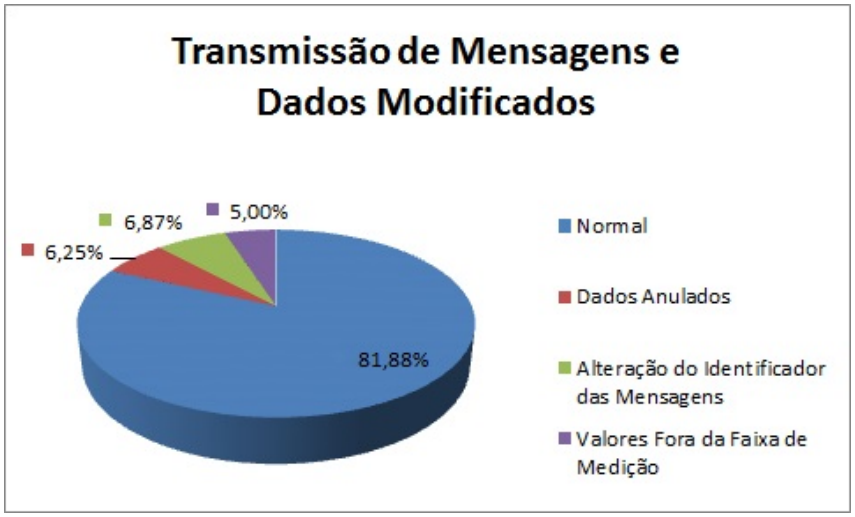

Figura 30 – 58 dados modificados em 320 dados recebidos

Tabela 11 – Transmissão de Mensagens e Dados Modificados - 4ª Simulação

Transmissão de Mensagens	**Número de Mensagens**
Normal	1588
Dados Anulados	132
Alteração do Identificador das Mensagens	143
Valores Fora da Faixa de Medição	137

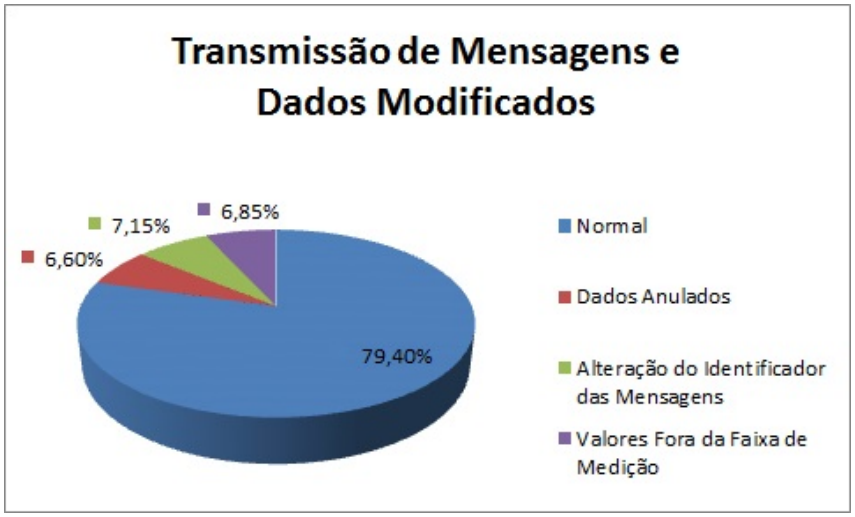

Figura 31 – 412 dados modificados em 2000 dados recebidos

Como se pode notar na Tabela 8 e na Figura 28, 16 pacotes de mensagens foram enviados corretamente ao destino final, 1 pacote teve seu valor anulado (**asdu1 = 0**), 1 pacote teve o identificador de mensagem adulterado de (**asdu2 = 5**) para (**asdu2 = 6**), conforme foi modelado neste trabalho e 2 pacotes tiveram seus valores adulterados para valores fora das faixas de medições elétricas (valores de **asdu1** acima de 2000).

No caso da Tabela 9 e da Figura 29, 30 pacotes de mensagens foram enviados corretamente ao destino final, 3 pacotes tiveram seus valores anulados (**asdu1 = 0**), 3 pacotes tiveram o identificador de mensagem adulterado de (**asdu2 = 5**) para (**asdu2 = 6**), conforme foi modelado neste trabalho e 4 pacotes tiveram seus valores adulterados para valores fora das faixas de medições elétricas (valores de **asdu1** acima de 2000).

No caso da Tabela 10 e da Figura 30, 262 pacotes de mensagens foram enviados corretamente ao destino final, 20 pacotes tiveram seus valores anulados (**asdu1 = 0**), 22 pacotes tiveram o identificador de mensagens adulterado de (**asdu2 = 5**) para (**asdu2 = 6**), conforme foi modelado neste trabalho e 16 pacotes tiveram seus valores adulterados para valores fora das faixas de medições elétricas (valores de **asdu1** acima de 2000).

No caso da Tabela 11 e da Figura 31, 1588 pacotes de mensagens foram enviados corretamente ao destino final, 132 pacotes tiveram seus valores anulados (**asdu1 = 0**), 143 pacotes tiveram o identificador de mensagens adulterado de (**asdu2 = 5**) para (**asdu2 = 6**), conforme foi modelado neste trabalho e 137 pacotes tiveram seus valores adulterados para valores fora das faixas de medições elétricas (valores de **asdu1** acima de 2000).

Os valores apresentados foram atacados por um ataque de modificação de dados, conforme foi proposto neste trabalho, porque o objetivo final desse tipo de ataque é modificar os dados antes de serem processados no destino final, e esse objetivo foi alcançado. No caso da última simulação, para 2000 pacotes enviados, 20,6% dos pacotes foram atacados pelos ataques cibernéticos modelados. Esta porcentagem obtida em relação ao número total de pacotes enviados do modelo está de acordo com probabilidade de ataque cibernético de 40% proposta neste trabalho, pois esta porcentagem de ataque cibernético foi utilizada para apenas uma *merging unit*, e como neste cenário foram utilizadas duas *merging units*, cada uma enviando 1000 pacotes, nota-se a ocorrência desta probabilidade de ataques, conforme o levantamento feito em 2016 pela Kaspersky Lab ICS CERTS (39).

Além disso, a classificação proposta no Analisador de Rede atuou corretamente, confirmando a modelagem sólida do sistema definido inicialmente nesse trabalho.

4.1.4 Simulações para o 3º Cenário:

Seguem-se as tabelas e os gráficos com os resultados gerados pelas simulações do modelo proposto no 3º cenário:

Tabela 12 – Transmissão de Mensagens e Dados Modificados - 1ª Simulação

Transmissão de Mensagens	**Número de Mensagens**
Normal	17
Dados Anulados	0
Alteração do Identificador das Mensagens	1
Valores Fora da Faixa de Medição	12

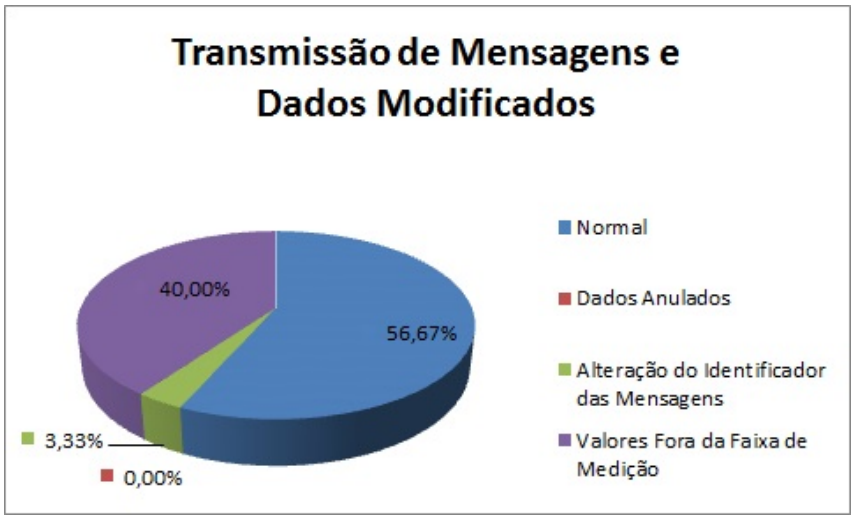

Figura 32 – 13 dados modificados em 30 dados recebidos

Tabela 13 – Transmissão de Mensagens e Dados Modificados - 2ª Simulação

Transmissão de Mensagens	**Número de Mensagens**
Normal	31
Dados Anulados	1
Alteração do Identificador das Mensagens	4
Valores Fora da Faixa de Medição	24

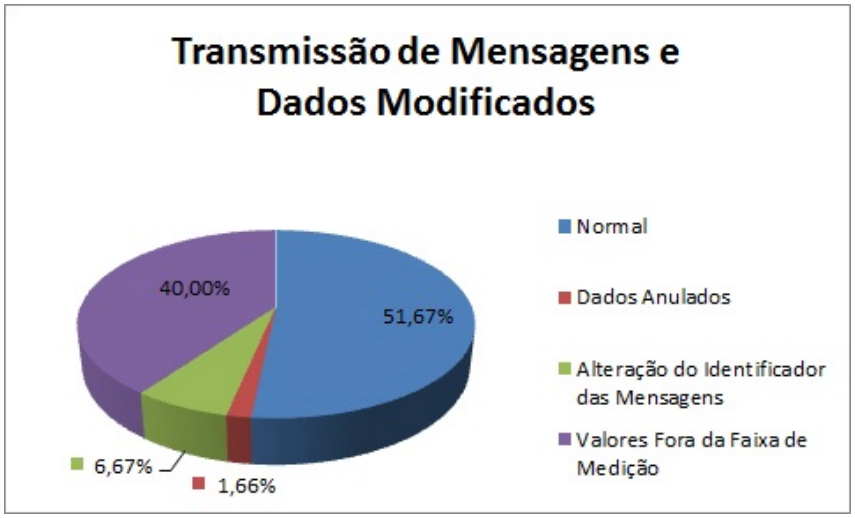

Figura 33 – 29 dados modificados em 60 dados recebidos

Tabela 14 – Transmissão de Mensagens e Dados Modificados - 3ª Simulação

Transmissão de Mensagens	**Número de Mensagens**
Normal	261
Dados Anulados	14
Alteração do Identificador das Mensagens	28
Valores Fora da Faixa de Medição	177

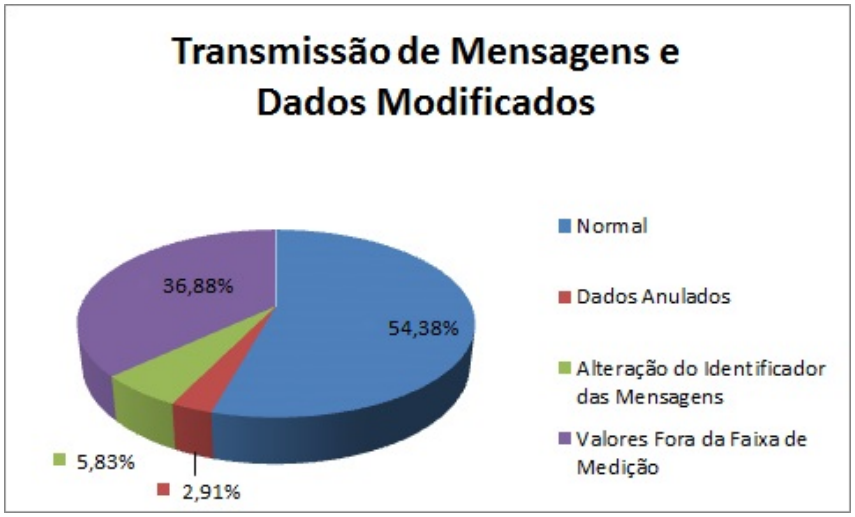

Figura 34 – 219 dados modificados em 480 dados recebidos

Tabela 15 – Transmissão de Mensagens e Dados Modificados - 4ª Simulação

Transmissão de Mensagens	**Número de Mensagens**
Normal	1635
Dados Anulados	118
Alteração do Identificador das Mensagens	127
Valores Fora da Faixa de Medição	1120

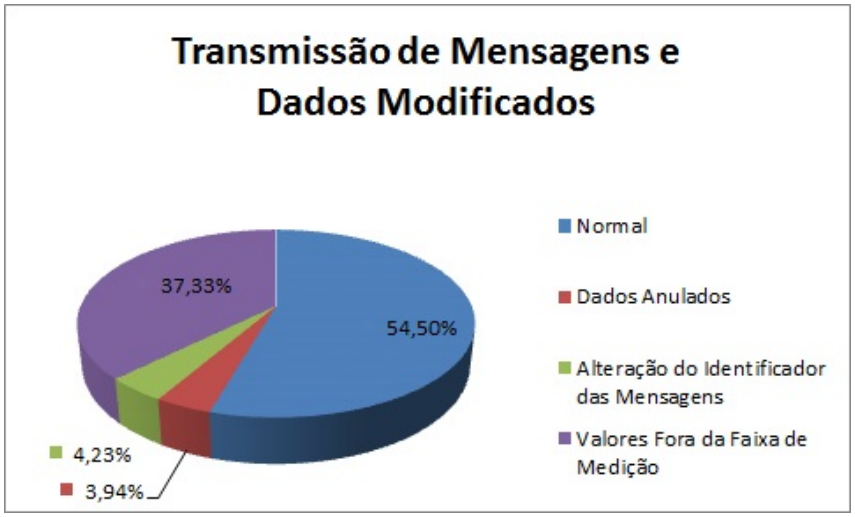

Figura 35 – 1365 dados modificados em 3000 dados recebidos

Como se pode notar na Tabela 12 e na Figura 32, 17 pacotes de mensagens foram enviados corretamente ao destino final, não houve pacotes com o valor anulado (**asdu1 = 0**), 1 pacote teve o identificador de mensagem adulterado de (**asdu2 = 5**) para (**asdu2 = 6**), conforme foi modelado neste trabalho e 12 pacotes tiveram seus valores adulterados para valores fora das faixas de medições elétricas (valores de **asdu1** acima de 2000).

No caso da Tabela 13 e da Figura 33, 31 pacotes de mensagens foram enviados corretamente ao destino final, 1 pacote teve seu valor anulado (**asdu1 = 0**), 4 pacotes tiveram o identificador de mensagem adulterado de (**asdu2 = 5**) para (**asdu2 = 6**), conforme foi modelado neste trabalho e 24 pacotes tiveram seus valores adulterados para valores fora das faixas de medições elétricas (valores de **asdu1** acima de 2000).

No caso da Tabela 14 e da Figura 34, 261 pacotes de mensagens foram enviados corretamente ao destino final, 14 pacotes tiveram seus valores anulados (**asdu1 = 0**), 28 pacotes tiveram o identificador de mensagens adulterado de (**asdu2 = 5**) para (**asdu2 = 6**), conforme foi modelado neste trabalho e 177 pacotes tiveram seus valores adulterados para valores fora das faixas de medições elétricas (valores de **asdu1** acima de 2000).

No caso da Tabela 15 e da Figura 35, 1635 pacotes de mensagens foram enviados corretamente ao destino final, 118 pacotes tiveram seus valores anulados (**asdu1 = 0**), 127 pacotes tiveram o identificador de mensagens adulterado de (**asdu2 = 5**) para (**asdu2 = 6**), conforme foi modelado neste trabalho e 1120 pacotes tiveram seus valores adulterados para valores fora das faixas de medições elétricas (valores de **asdu1** acima de 2000).

Os valores apresentados foram atacados por um ataque de modificação de dados, conforme foi proposto neste trabalho, porque o objetivo final desse tipo de ataque é mudar os dados antes de serem processados no destino final, e esse objetivo foi alcançado.No caso da última simulação, para 3000 pacotes enviados, 45,5% dos pacotes tiveram seus valores modificados.

Deve-se notar que a *merging unit* 3 (**MU3**) não utilizou como arquivo de entrada de dados o "*tcfile2.txt*". Neste caso, para simular um possível mau funcionamento ou algum problema de calibração do equipamento, foi utilizado o arquivo "*tcfile4.txt*", que contém dados analógicos de corrente com valores que variam de 2002 a 4000. Assim, todos os dados provenientes da *merging unit* 3 estarão fora da faixa de medição (33,33% do total dos dados). Por fim, como apenas a **MU1** apresenta a probabilidade de ataque cibernético de 40% proposta neste trabalho, apenas 12,17% dos dados globais desta arquitetura foram atacados pelo ataque cibernético modelado nesta dissertação.

Além disso, a classificação proposta no Analisador de Rede atuou corretamente, confirmando a modelagem sólida do sistema definido inicialmente nesse trabalho.

Também nota-se que além de poder ser classificado como um ataque cibernético de *Data Modification* ou ataque de *Inserção de Dados Maliciosos*, definido na seção 2.2, item

J desta dissertação, este ataque cibernético modelado pode também ser definido como um ataque *man-in-the-middle*, definido na seção 2.2, item *B* desta dissertação, pois o invasor intercepta ou subverte as comunicações e fornece dados falsos ao usuário do sistema. Outra possível classificação para esse ataque cibernético seria um ataque de um *insider* ou ataque de acesso direto, definido na seção 2.2, item *H* desta dissertação, pois apenas pessoal autorizado tem acesso às *merging units* para executar essa ação e neste caso, o invasor manipula deliberadamente os dispositivos do sistema de energia para produzir uma condição não autorizada, visto que é considerado um usuário confiável.

Os resultados apresentados estão em conformidade com o que era esperado e modelado neste cenário. Sabendo que qualquer modificação de dados das mensagens *Sampled Value* pode afetar a proteção e os sistemas de controle de energia, porque seus quadros de mensagens usam a camada1 do modelo TCP / IP e são extremamente rápidos, esses modelos de modificação de dados neste cenário simples IEC 61850 poderiam levar a uma operação incorreta de disjuntores e relés, e poderiam gerar sérios problemas nas subestações de energia, porque dados falsos estão sendo inseridos no sistema.

4.2 Proposta de Mitigação dos Ataques Cibernéticos

Baseado na discussão apresentada na seção 2.4, que trata sobre as principais técnicas de mitigação conhecidas em relação aos ataques cibernéticos, têm-se as seguintes técnicas de mitigação para cada um dos tipos de ataque cibernético propostos neste trabalho:

4.2.1 Caso *Data Modification*:

Considerando-se o caso do ataque cibernético de *Data Modification*, o uso de autenticação de dados e criptografia em conjunto pode fornecer uma defesa adequada nesse tipo de ataque. De acordo com (1), o risco de modificação de dados é mitigado em protocolos Ethernet com criptografia. Além disso, a Tabela 1 - Tipos de Ataques e Técnicas de Mitigação propõe o algoritmo de código de autenticação de mensagens baseado em hash (HMAC) como técnica de mitigação para esse tipo de ataque.

No entanto, no caso do ambiente IEC 61850, conhecendo-se o tempo crítico na transmissão de mensagens *Sampled Value* (SV), conforme já foi citado no item 2.5.2.1 desta dissertação, é praticamente inviável inserir um processamento de criptografia para autenticar as mensagens a serem transmitidas, visto que o tempo de processamento dessa criptografia impedirá o correto envio das mensagens *Sampled Value* (SV). De acordo com (40), os tempos de processamento de dois algoritmos HMAC, como o HMAC-MD5 e o HMAC-SHA-1, estão na ordem de 90 ms e 148 ms, enquanto que os tempos de transmissão

das mensagens *Sampled Value* estão na ordem de 3 milissegundos (mensagens de alta velocidade), conforme especifica a sessão 2.5.2.1.

Assim, a melhor solução para mitigar este ataque cibernético seria através do controle de acesso ao meio e da utilização de *firewalls*, desde que isto não impacte na transmissão das mensagens *Sampled Value*.

4.2.2 Caso *Man-in-the-Middle*:

Considerando-se tanto o caso do ataque cibernético *Man-in-the-Middle* quanto o caso do ataque cibernético *Insider*, Acesso Direto ou Acesso Não Autorizado, o uso de autenticação de dados e criptografia em conjunto pode fornecer uma defesa adequada nesse tipo de ataque cibernético, assim como no caso do ataque de *Data Modification*. Conforme a Tabela 1, a técnica de mitigação para estes tipos de ataques cibernéticos é a utilização de criptografia forte através do protocolo de segurança da Internet(IPsec) com PKI, que fornece um método de criptografia e autenticação, além do controle de acesso e da verificação do estado do *firewall* (1).

Para estes casos também, conhecendo-se o tempo crítico na transmissão de mensagens *Sampled Value* (SV), é praticamente inviável inserir um processamento de criptografia para autenticar as mensagens a serem transmitidas, visto que o tempo de processamento dessa criptografia impedirá o correto envio das mensagens *Sampled Value* (SV), assim como já foi explicado na subseção anterior.De acordo com (41), os tempos de processamento de alguns algoritmos, como o AES, estão na ordem de segundos, enquanto que os tempos de transmissão das mensagens *Sampled Value* estão na ordem de milissegundos, conforme especifica a sessão 2.5.2.1.

Assim, a melhor solução para mitigar estes ataques cibernéticos também seria através do controle de acesso ao meio e da utilização e verificação do estado dos *firewalls*, desde que isto não impacte na transmissão das mensagens *Sampled Value*.

Para o caso específico do ataque do *Insider*, Acesso Direto ou Acesso Não Autorizado, em que o invasor é um usuário confiável (25), é fundamental um controle de acesso ao meio.

5 Conclusão

5.1 Conclusões Gerais

De acordo com o que é apresentado nesta dissertação, conclui-se que a modelagem em Redes de Petri Coloridas é perfeitamente aplicável à modelagem de ataques cibernéticos de um cenário IEC 61850. A metodologia apresentada pode suportar alguns detalhes importantes no processo de projeto de proteção das arquiteturas IEC 61850.

Os resultados gerados com simulações comprovam que o modelo respondeu corretamente de acordo com as funções criadas para produzir o ataque cibernético. Além disso, sabendo que qualquer modificação de dados das mensagens *Sampled Values* pode afetar a proteção e os sistemas de energia de controle, esse ataque cibernético de modificação de dados modelado neste cenário simples da IEC 61850 pode gerar sérios problemas nas subestações de energia, pois dados falsos estão sendo inseridos no sistema.

Nota-se também a correta classificação dos dados recebidos pelo Analisador de Rede. Essa modelagem pode ser útil para atuar em tempo real nos dispositvos de medição e controle em subestações, alertando os operadores sobre medições incorretas e possíveis invasões nos sistemas de comunicação do sistema elétrico.

Observa-se também que através do desenvolvimento de modelos automatizados de ameaças, como o proposto neste trabalho, pode-se identificar os passos mais prováveis para a execução de um ataque cibernético nestas situações. Com isso, pode-se interromper uma ameaça ou a evolução de um ataque em potencial, propondo uma metodologia de segurança para o sistema.

Por fim, percebe-se que as técnicas de mitigação propostas neste trabalho, com base na literatura consultada, podem não ser tão eficazes. No caso dos ataques de *Data Modification* e *Man-in-the-Middle*, foi proposto o uso de autenticação de dados e criptografia em conjunto, para fornecer uma defesa adequada nesses tipos de ataques cibernéticos. No entanto, de acordo com o que foi consultado em (41), os tempos de criptografia saõ bem maiores que os tempos críticos para a transmissão de mensagens *Sampled Value*.

De acordo com (30), a cada período de tempo, determinado pela frequência de amostragem do sinal e pela resolução temporal necessária para a conversão analógico-digital, uma mensagem SV é colocada na rede. Com isso, tem-se um aumento no tráfego e eventual perda de pacotes e conflitos de rede. Por tais motivos, as mensagens SV ainda são um desafio para a aplicação plena da norma IEC 61850 (3).

Assim, fica impossibilitada a aplicação de criptografia e autenticação na trans-

missão de mensagens *Sampled Value*. Para qualquer um dos casos de ataque, quer seja *Data Modification*, *Man-in-the-Middle* ou *Insider*, a melhor opção de proteção é através do controle de acesso ao meio.

5.2 Trabalhos Futuros

Os trabalhos futuros que podem ser desenvolvidos com base nesta dissertação incluem a modelagem de novos ataques cibernéticos que podem se tornar potenciais ameaças às redes de comunicação industriais e das subestações. Logo, através do projeto de novos modelos automatizados de ameaças, que podem ser mais aprimorados e sofisticados tanto em ambientes industriais quanto em subestações de energia elétrica, pode-se identificar os passos mais prováveis para a execução de um ataque cibernético nestas situações. Com isso, pode-se evitar futuros problemas possíveis com a segurança do sistema. Além disso, sugerem-se algumas novas contribuições:

- Conexão entre os formalismos CPN e as Cadeias de Markov para avaliações probabilísticas de estados de ataques cibernéticos;

- Proposta de uma metodologia para diferenciar ataques cibernéticos, incidentes de segurança e problemas de mau funcionamento dos equipamentos;

- Estudo das funcionalidades de proteção de sistema elétrico de potência verificando a influência do tempo de comunicação envolvido;

- Estudo de mecanismos de detecção de intrusão em sistemas de comunicação do sistema elétrico.

Referências

1 BARTMAN, T.; CARSON, K. Securing critical industrial systems with sel solutions. 10, 17, 20, 22, 23, 24, 25, 26, 65, 66

2 CODE, P. *Communication networks and systems in substations–Part 5: Communication requirements for functions and device models*. 2003. 10, 28, 29, 30

3 MACHADO, P. H. F. Metodologia de modelagem cpn aplicada a análise de desempenho de sistemas de comunicação baseados na norma iec 61850. 2015. 10, 28, 29, 31, 32, 33, 34, 36, 37, 39, 40, 41, 67

4 IEC 61850-1, Communication networks and systems in substations – Part 1: Introduction and overview. [S.l.], 2010. 16

5 CLEVELAND, F. M. Cyber security issues for advanced metering infrasttructure (ami). In: IEEE. *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*. [S.l.], 2008. p. 1–5. 16

6 COHEN, F. The smarter grid. *IEEE Security & Privacy*, IEEE, v. 8, n. 1, 2010. 16

7 KHURANA, H. et al. Smart-grid security issues. *IEEE Security & Privacy*, IEEE, v. 8, n. 1, 2010. 16

8 MCDANIEL, P.; MCLAUGHLIN, S. Security and privacy challenges in the smart grid. *IEEE Security & Privacy*, IEEE, v. 7, n. 3, 2009. 16

9 SMART Grid Interoperability Panel—Cyber Security Working Group Smart Grid Cyber Security Strategy and Requirements NIST, Gaithersburg, MD, Tech. Rep. draft NISTIR 76j. [S.l.], 2010. 16

10 CHEN, T. M. Survey of cyber security issues in smart grids. *Cyber Security, Situation Management, and Impact Assessment II; and Visual Analytics for Homeland Defense and Security II (part of SPIE DSS 2010)*, p. 77090D–1, 2010. 16

11 CHEN, T. M.; SANCHEZ-AARNOUTSE, J. C.; BUFORD, J. Petri net modeling of cyber-physical attacks on smart grid. *IEEE Transactions on Smart Grid*, IEEE, v. 2, n. 4, p. 741–749, 2011. 16, 17

12 DAVID, R.; ALLA, H. *Discrete, continuous, and hybrid Petri nets*. [S.l.]: Springer Science & Business Media, 2010. 16

13 JENSEN, K.; KRISTENSEN, L. M. *Coloured Petri nets: modelling and validation of concurrent systems*. [S.l.]: Springer Science & Business Media, 2009. 16

14 LIU, X. et al. A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. *IEEE Transactions on Smart Grid*, IEEE, v. 6, n. 5, p. 2435–2443, 2015. 16, 17

15 MCDERMOTT, J. P. Attack net penetration testing. In: ACM. *Proceedings of the 2000 workshop on New security paradigms*. [S.l.], 2001. p. 15–21. 16

16 DALTON, G. et al. Analyzing attack trees using generalized stochastic petri nets. In: *Information Assurance Workshop*. [S.l.: s.n.], 2006. p. 116–123. 16

17 WU, R.; LI, W.; HUANG, H. An attack modeling based on hierarchical colored petri nets. In: IEEE. *Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on*. [S.l.], 2008. p. 918–921. 17

18 SCHNEIDER, K.; LIU, C.-C.; PAUL, J.-P. Assessment of interactions between power and telecommunications infrastructures. *IEEE Transactions on Power Systems*, IEEE, v. 21, n. 3, p. 1123–1130, 2006. 17

19 GURSESLI, O.; DESROCHERS, A. A. Modeling infrastructure interdependencies using petri nets. In: IEEE. *Systems, Man and Cybernetics, 2003. IEEE International Conference on*. [S.l.], 2003. v. 2, p. 1506–1512. 17

20 LAPRIE, J.-C.; KANOUN, K.; KAÂNICHE, M. Modelling interdependencies between the electricity and information infrastructures. *Computer Safety, Reliability, and Security*, Springer, p. 54–67, 2007. 17

21 CALDERARO, V. et al. Failure identification in smart grids based on petri net modeling. *IEEE Transactions on Industrial Electronics*, IEEE, v. 58, n. 10, p. 4613–4623, 2011. 17

22 DAHL, O. M.; WOLTHUSEN, S. D. Modeling and execution of complex attack scenarios using interval timed colored petri nets. In: IEEE. *Information Assurance, 2006. IWIA 2006. Fourth IEEE International Workshop on*. [S.l.], 2006. p. 12–pp. 17

23 RAYMOND, E. S. *The new hacker's dictionary*. [S.l.]: Mit Press, 1996. 20

24 U.S. Department of Homeland Security Control Systems Security Program. [S.l.]. 20

25 SCHWEITZER, E. O. et al. How would we know? In: IEEE. *Protective Relay Engineers, 2011 64th Annual Conference for*. [S.l.], 2011. p. 310–321. 20, 66

26 CANALES, I. et al. Interuca project: Uca interoperability for distributed control within electrical substations. *Cigré 2004*, n. B5-204, p. 1–8, 2004. 28

27 PEREIRA, A. C. et al. Sistemas de proteção e automação de subestações de distribuição e industriais usando a norma iec 61850. *XIII ERIAC. Puerto Iguazú*, 2009. 28

28 TAN, J.-C.; GREEN, V.; CIUFO, J. Testing iec 61850 based multi-vendor substation automation systems for interoperability. In: IEEE. *Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES*. [S.l.], 2009. p. 1–5. 28

29 IEC61850, I. *9-2 Communication networks and systems in substations, part 9-2: Specific Communication Service Mapping (SCSM)-sampled values over ISO*. [S.l.]: Sl]: IEC, 2003. 29

30 INGRAM, D. M. et al. Performance analysis of iec 61850 sampled value process bus networks. *IEEE Transactions on industrial informatics*, IEEE, v. 9, n. 3, p. 1445–1454, 2013. 29, 67

31 MURATA, T. Petri nets: Properties, analysis and applications. *Proceedings of the IEEE*, IEEE, v. 77, n. 4, p. 541–580, 1989. 31

32 NORRIS, J. R. *Markov chains*. [S.l.]: Cambridge university press, 1998. 31

33 PETRI, C. A. Kommunikation mit automaten. 1962. 31

34 GHARBI, N.; DUTHEILLET, C.; IOUALALEN, M. Colored stochastic petri nets for modelling and analysis of multiclass retrial systems. *Mathematical and Computer Modelling*, Elsevier, v. 49, n. 7, p. 1436–1448, 2009. 32

35 CHIOLA, G. et al. Stochastic well-formed colored nets and symmetric modeling applications. *IEEE Transactions on Computers*, IEEE, v. 42, n. 11, p. 1343–1360, 1993. 32

36 CPN Tools. [S.l.]. 32

37 ULLMAN, J. D. *Elements of ML programming*. [S.l.]: Prentice-Hall, Inc., 1994. 32

38 ZAITSEV, D. A.; SHMELEVA, T. R. Switched ethernet response time evaluation via colored petri net model. In: *Proc. of International Middle Eastern Multiconference on Simulation and Modelling*. [S.l.: s.n.], 2006. p. 68–77. 37

39 COMPUTERWORLD. [S.l.]. 47, 53, 60

40 XIAOYONG, T. et al. A novel security-driven scheduling algorithm for precedence-constrained tasks in heterogeneous distributed systems. *IEEE Transactions on Computers*, IEEE, v. 60, n. 7, p. 1017–1029, 2011. 65

41 MAHAJAN, P.; SACHDEVA, A. A study of encryption algorithms aes, des and rsa for security. *Global Journal of Computer Science and Technology*, 2013. 66, 67

Apêndices

APÊNDICE A – Artigos Publicados na ICSAI 2017 (2017 4th International Conference on Systems and Informatics)

Modeling of a Cyber-Attack in an IEC 61850 Scenario Using Stochastic Colored Petri Nets

Milton Rafael da Silva, Pedro Henrique Ferreira Machado, Luiz Edival de Souza and Carlos Waldecir de Souza
Institute of Systems Engineering and Information Technology
Federal University of Itajuba
Itajubá, Minas Gerais, Brazil
miltonrafa@yahoo.com.br; machado.pferreira@gmail.com; edival@unifei.edu.br; cw.souza@yahoo.com.br

***Abstract* - Some performance parameters in IEC 61850 related to the time in processing communication are defined, and these parameters are really important and critical in the automation of power systems. Related to the security analysis of the communication networks, a really powerful tool is the Stochastic Colored Petri Net (SCPN), because it models asynchronous and concurrent processes, and it is useful to analyze delays in timed systems. So, based in this context and knowing that time is really critical in transmitting messages in the IEC 61850 context; it is modeled in an IEC 61850 scenario a cyber-attack using SCPN that aims to delay the transmission of the messages, what is really critical for the operation of the system. The results corresponded to the modeled cyber-attack, showing the efficacy of the proposed modeling method.**

***Keywords* – IEC 61850; Smart Grid; Stochastic Colored Petri Nets; Security Analysis; Modeling of Cyber-Attack.**

I. INTRODUCTION

In the intelligent transmission and power distribution networks based on interactive communication between all parts of the power conversion chain, known as Smart Grids, there are communication networks that allow the transfer of data between their components. Data exchanges, network topology, decentralized control, security, are inherent characteristics to the communication systems and are also an important part of the smart grids in the electric power sector.

In order that the information is exchanged in a correct, reliable and efficient way, standardization in data communication is needed. So there's the IEC 61850 standard. Referenced in [1], IEC 61850 proposes standards for the services and data formats exchanged on a network of electrical system equipment.

Security has been recognized as a critical matter with important implications in the smart grids scenario [2]–[7]. Also, cyber-attacks may attempt to access remotely the systems through the neighborhood area networks (NANs) or home area networks (HANs) in order to control the equipment or destroy them [8]. With the infrastructure of Internet and telecommunications, coordinating simultaneous attacks is really easy for distributed groups to do it [8].

In the scenario of cyber-attacks modeling, Petri nets became important tools for describing many different types of processes [9], [10], [11]. The importance of Petri nets in cyber-attack modeling was first described perhaps by McDermott [12]. It was noted that Petri nets identify actions during an attack [8]. Dalton *et al. used* stochastic Petri nets for cyber-attack modeling [13]. Stochastic Petri nets are timed and transitions happen after random times. Transition delays were defined as exponentially distributed what transformed the stochastic Petri net into an equivalent continuous-time Markov Chain. That transformation became true because of the analysis for Markov chains, but the exponential transition delays was not correctly justified [8].

Colored Petri nets have become interesting for cyber-attacks because they can express more details than the ordinary Petri nets. In the ordinary Petri nets, all marks (tokens) are not distinguishable from one another. In colored Petri nets, tokens carry data values (characteristics) represented by color, which allows different attackers and different actions in the model [8]. Wu *et al. used* colored Petri nets for describing a hierarchical cyber-attack modeling [14]. At a high level of a model description and its programming, a modeled cyber-attack is a colored Petri net where some transitions have hidden details, which can be viewed in details in a subpage that is another colored Petri net [8].

Related to the electrical system, Chen *et al.* [8] proposed a new methodology to create a wide Petri net from simple Petri nets in order to model some cyber-physical attacks on the smart grid [11]. Also, Petri nets have been used to present interdependencies between the electrical and communications systems [15]–[17]. Besides, Calderaro *et al.* [18] presented a describing method using Petri nets in order to identify and localize failures in the smart grid. Dahl and Wolthusen used timed colored Petri nets with the aim to create timed attacks carried out by multiple attackers against possibly different targets [8], [19].

It is noted in these Petri net models that places represent all possible states of the modeled systems and transitions changes the modeled states. What it means is that interdependencies are created with the electrical and communication devices in a unique Petri net [8].

So, in this work, based in all previous works and in a simple IEC 61850 scenario, it is proposed to model and analyze a cyber-attack in a simple architecture with one merging unit publishing Sampled Value messages, a switch for packet switching and storage, and a network analyzer to check packet latency due to the occurred cyber-attack. This cyber-attack aims to delay the transmission of the Sampled Value messages and assess the impact of it in the electrical power system communications systems.

II. STOCHASTIC COLORED PETRI NET (SCPN)

978-1-5386-1107-4/17/$31.00 ©2017 IEEE

The Petri net (PN), discussed in [20], is a graphical mathematical tool for studying systems characterized as asynchronous, competitors, distributed, non-deterministic, parallel and/or stochastic. Briefly, the PN is a bipartite graph (graphs that don't contain odd cycles) with graphical interpretation formed by two components: transition and place. Representation is as follows in Figure 1, in which spaces are the circles and thin rectangles are transitions. These two components, also called nodes, are connected by directed arcs.

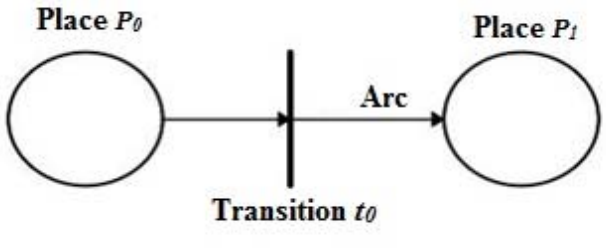

Figure 1. Basic Elements of a PN

For modeling and better interpretation of systems, it is used marks (tokens) assigned to the places that allow to represent the state situation. The movement of the marks through well-defined rules represents the system dynamics.

In the field of network protocol analysis, the Stochastic Petri Net (SPN), variants of PN, are constantly applied in the performance analysis in the computer networks and communication systems, since SPN is isomorphic and enables, together with the Markov chains [21], the state probability analysis of the system. However, even with these important characteristics, the SPNs are limited in complex models and in models with industrial dimensions.

The Stochastic Colored Petri Nets (CSPN) has higher abstraction capacity. This allows each place to have various types of marks and transitions that represent various types of functions, thereby reducing the number of nodes. A key point for the application of this type of Petri nets in the communication systems is precisely the connection with programming languages, as an example the Meta Language (ML) used in CPN Tools [22] software.

Formally, the definition for the SCPN is represented as follows and can be verified in [23] and [24]:

$SCPN = \{P, T, CB, C, W^-, W^+, W^h, Pri, M_0, \theta\}$

• P is the finite set of places;
• T is the finite set of timed and immediate transitions, $P \cap T = \emptyset$, $P \cup T \neq \emptyset$;
• CB is the family of basic color classes: $CB=\{C_1,...,C_n\}$ with $C_i \cap C_j = \emptyset$;
• C is a $P \cup T$ function that associates to any r node a color domain $C(r)$ that is the Cartesian product of the CB elements;
• W^-, W^+, W^h: $W^-(p, t)$, $W^+(p, t)$, $W^h(p, t) \in [C(t) \rightarrow Bag(C(p))]$ are functions that label respectively the entrance, output and inhibitors arches between t transitions and p places;
• Pri is the priority function defined as follows: $\forall t \in T$, $Pri(t) : C(t) \rightarrow N.Pri(t)(c)$ is the priority of the instance$[t,c]$.
• M_0 is the initial marking that describes the initial state of the system;
• θ is the defined function in the set of transitions T given that $\theta(t)$ is the time function of the model.

III. IEC 61850 – GENERAL OVERVIEW

The IEC 61850 is an international standard that defines the communication and services form between different equipment present in the automation of power electrical systems [25]. It establishes the following objectives: Interoperability between manufacturers, free configuration (modeling), and long-term stability.

The most significant benefits of implementing this standard are the independence of future technology, ease of long-term maintenance, reduced wiring, and free specification and exchange of data at high speed.

A. Sampled Values

This type of message has the proposal of transmission of sampled values of measurement, according to [26], inserted into types of *unicast* or *multicast* messages. Commonly, this message is used to send analog data coming from the current and voltage meters (Current Transformers and Voltage Transformers).The IED (Intelligent Electronic Device) that implements the messages *Sampled Values* (SV) needs hardware that supports huge volume of Analog-to-Digital conversions that must be processed quickly and safe. This is only possible with the use of more resistant components, more reliable and more expensive. This is the burden that SV messages produce in the IEDs that implement them.

The sampled values are used by control and protection system. The frames of SV messages uses layer1 of the TCP / IP model and are extremely fast.

B. Time Requirements

In section 5 of the standard [25] the transfer time between two points is defined as shown in Figure 2 [27]. In other words, the transfer time is the time spent from the moment the transmitting device puts the message at the top of its transmission stack until the instant the receiving device extracts the data from its receiving stack. The transfer time t between two physical devices is composed by the sum of times t_a, t_b and t_c. The times t_a and t_c correspond to the coding and decoding times of the message frames in each device, transmitter and receiver respectively. The time t_b is the propagation time of the frame in the physical medium used.

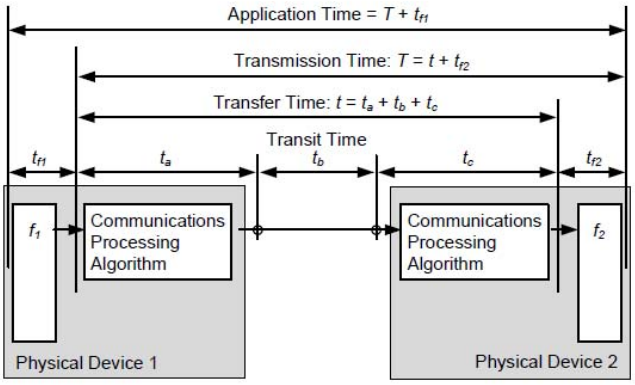

Figure 2. Transfer Time

If there's any delay in the transfer time or in any of its components (t_a , t_b and t_c), it may affect the protection and the control power systems, in the case of SV messages, because its frames of messages uses layer1 of the TCP / IP model and are extremely fast. This could lead to misoperation of circuit breakers and relays, and could generate serious problems in power substations.

IV. SCPN MODELING OF AN IEC 61850 SYSTEM – *SAMPLED VALUE* (SV) MESSAGES AND CYBER-ATTACK

The following SCPN models seek to represent the main characteristics of the devices presented in the proposed architecture. So the proposed methodology concerns about analyze the performance of this network architecture using modeling only, when it is working normally or when it is attacked. According to the presented theoretical basis, it is started then the development of a SCPN modeling of the standard IEC 61850 together with a cyber-attack. For this, two guidelines are defined. The first one deals with the part of system concepts involving the definitions of the standard IEC 61850. The second one, structures the way how it should be elaborate the models in SCPN, together with the modeled cyber-attack. In Figure 3 it can be seen the proposed architecture.

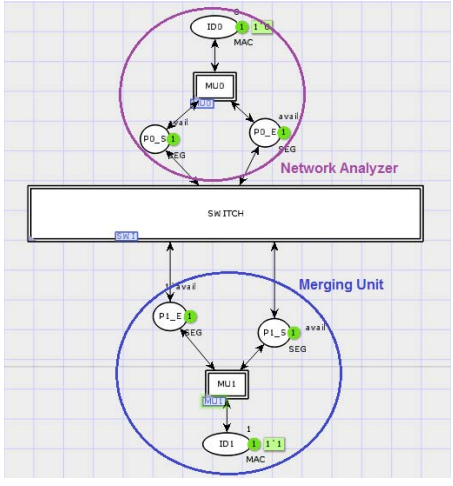

Figure 3. Proposed Architecture

A. *Switch Model*

The switch model has the main features of this device. The switching tables, packet buffer, switch processing and physical communication interfaces (input and output ports) are all defined. To better understand this model, only one communication port is defined. For the representation of other ports, a simply replication of such model is done. Figure 4 shows the main characteristics of this device. The switch model is based on the work developed in [28], in which this equipment is represented in CPN models.

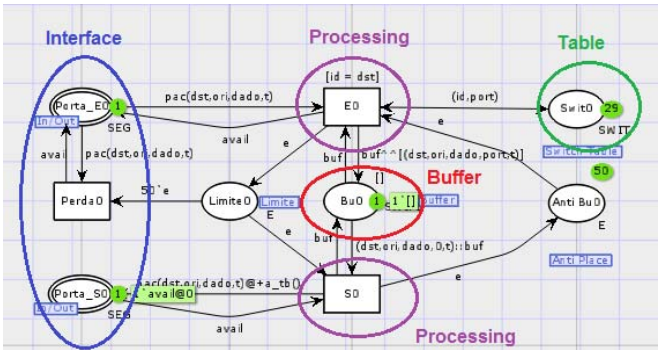

Figure 4. CPN Model of the Switch

Regarding the model representation, Figure 4 indicates the dynamics of a SV packet within a real switching device. The message enters via the communication interface (place **Porta_E0**), then it is processed (transitions **E0** and **S0**), stored in the buffer (place **Bu0**) and then is transmitted according to the switching table to the respective destination (place **Swit0**). This whole process takes time, called by the norm as propagation time, and for this reason it is attributed to the time stamp @ + tb () in the transition **S0**.

B. *Merging Unit Model*

The model of Figure 5 represents the physical *merging unit* device that converts the analog signals into digital signals, and sends such signals in the format of *Sampled Value* messages.

The CPN representation of the *merging unit* characterizes the signal sampling, the processing of the samples by the logical nodes and the interfacing with the network.

The sampling process is done by reading a text file containing the current transformer samples, which simulates the data of a real transformer. The text file is read through the function defined in the **Inicio** transition, and through the **getPacketsTC** () function. After that, the file data is transformed into CPN tokens. **TCTR** and **MMXU** transitions, which represent the logical nodes defined in the IEC 61850 standard, translate the information from the samples (tokens) and pack them into the *Sampled Value* format. The right part of the model represents the communication interface of the device (**LAN_S** and **LAN_E** places). The **Origem** and **Destino** places indicate the communication interface of the source and destination of the packages (**Origem** and **Destino** places)

generated by the *merging unit*. With this structure, the *merging unit* model is able to simulate real devices sending SV messages.

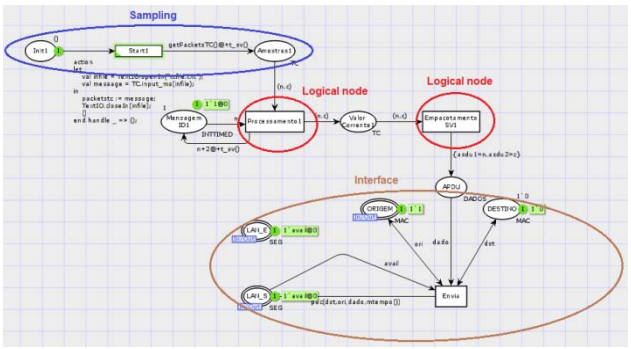

Figure 5. CPN Model of the Merging Unit

C. *Analyzer Model*

The analyzer model is characterized in a simple way according to Figure 6. The function of this model is to represent the device that verifies the latency time of the *Sampled Value* messages that is transferred in the network.

To do this, the model receives the messages through the communication interface (**LAN_E** place) and then verifies the origin of the packet (**Recebe** transition and **Origem** place) identifying the *merging unit* transmitter. After this, the message is sent to the **Buffer** transition where the transfer time of each SV packet is calculated.

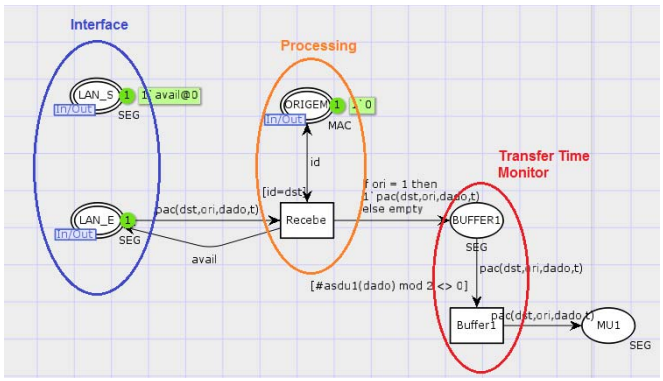

Figure 6. CPN Model of the Analyzer

D. *Cyber Attack Model*

In the cyber-attack model presented in color red in Figure 7, it was created the function *fail(),* a uniform distribution that generates a random value between 0 and 1. As soon as this random value is generated, that value goes to the place *Prob.* Depending on this value, the transition *Normal* or the transition *Attack* are enabled. To enable the *Normal* transition, this random generated value must be greater than 0.1. To enable the *Attack* transition, this random generated value must be smaller than or equal to 0.1. This indicates a cyber-attack probability of 10%. If the *Normal* transition is enabled, the message flow is normal. If the *Attack* transition is enabled, the message flow is delayed according to the function *delay_attack(),* a normal distribution that generates a random value with mean 10 and variance 2.

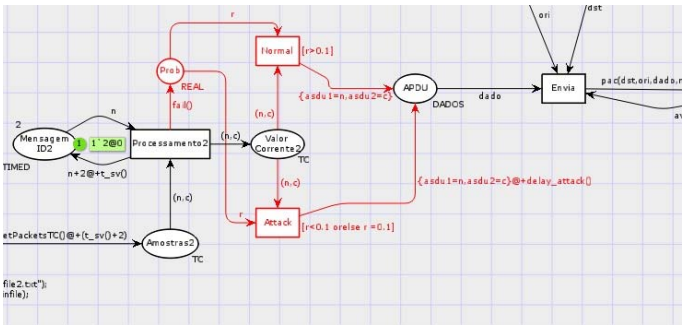

Figure 7. Cyber-attack Model

V. RESULTS AND DISCUSSION

For cyber-attack analysis, it is used the simulation tools available in the *CPN Tools software*. Times and stochastic presented here are illustrative. Evidenced earlier in the description of the model, it is defined some stochastic. They are *fail()* and *delay_attack(),* which represent the probability of cyber-attack. These parameters allow creating in the model the non-determinism of the process.

It follows some results generated from model simulations.

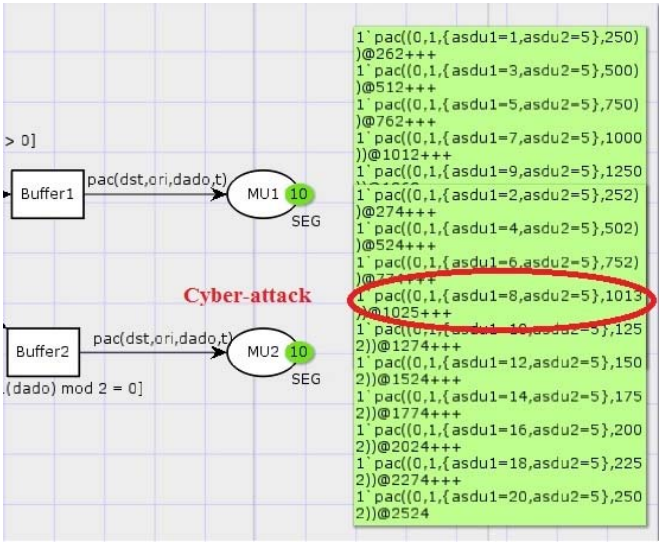

Figure 8. 1 Cyber-attack for 10 received packets

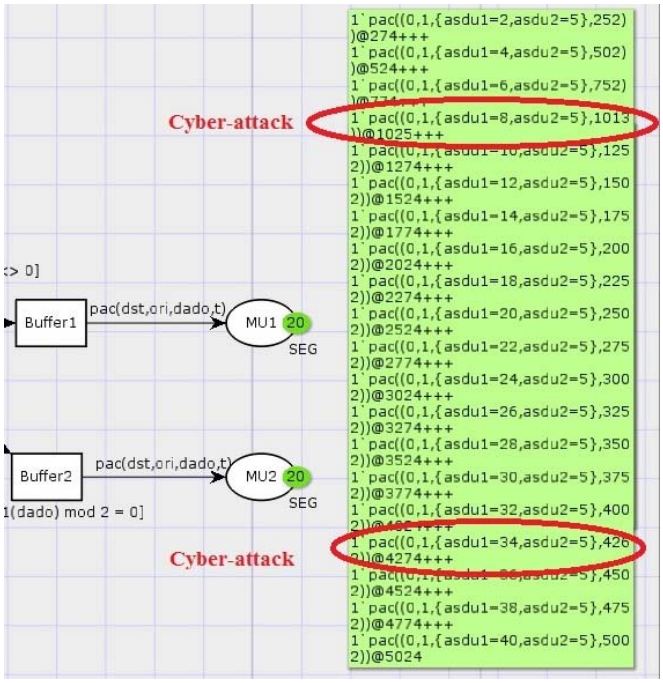

Figure 9. 2 Cyber-attacks for 20 received packets

According to the functions *fail()* and *delay_attack()*, there's a cyber-attack probability of 10%. It can be seen in the results generated by the *CPN Tools software* that, in fact, for a simulation with 10 sent packets (Figure 8) and for a simulation with 20 sent packets (Figure 9), 10% of the packets were *attacked* (1 and 2 packets were attacked, respectively). These attacks can be verified in the time delay of the attacked packets, since according to the cyber-attack model implemented in this work, an attacked packet will be delayed according to the function *delay_attack()*. In the first attacked packet, in both simulations (Figures 8 and 9), the time values should be 1002 and 1024, but the time values are 1013 and 1025. In the second simulation (Figure 9), with 20 sent packets, the second attacked packet should have a time value of 4252, but the time value it has is 4262. So, presented results are in according to what was expected and modeled in this scenario.

Knowing that any delay in the transfer time of the SV messages may affect the protection and the control power systems, because its frames of messages uses layer1 of the TCP / IP model and are extremely fast, these modeled delays in this simple IEC 61850 scenario could lead to misoperation of circuit breakers and relays, and could generate serious problems in power substations.

VI.CONCLUSION

According to what is presented in this article, it is concluded that the SCPN modeling is perfectly applicable to the modeling of cyber-attacks of an IEC 61850 scenario. The presented methodology is simple, but can support some important details in the design of protection process of IEC 61850 architectures.

The results generated with simulations prove that the model responded correctly according to the functions created to produce the cyber-attack. Also, knowing that any delay in the transfer time of the SV messages may affect the protection and the control power systems, these modeled delays in this simple IEC 61850 scenario could generate serious problems in power substations.

Future projects include the modeling of new cyber-attacks that can become potential threats to substation networks. Also, those cyber-attacks can be improved and sophisticated, avoiding future possible problems with the security of the system.

VII. ACKNOWLEDGEMENTS

We would like to dedicate this work to my God, *Yahweh* (יהוה), for giving us strength to overcome difficulties. Our sincere thanks to the Federal University of Itajuba (UNIFEI). Also, we gratefully acknowledge CNPq (National Council for Scientific and Technological Development – Brazil) for funding this work.

VIII. REFERENCES

[1] IEC 61850-1, *Communication networks and systems in substations – Part 1: Introduction and overview,* Ed. 2.0., 2010.
[2] F. Cleveland, "Cyber security issues for advanced metering infrastructure (AMI)," in *Proc. 2008 IEEE Power Energy Soc. Gen. Meet.—Convers. Del. Electr. Energy 21st Century*, Pittsburgh, PA, Apr. 2008, pp.1–5.
[3] F. Cohen, "The smarter grid," *IEEE Security Privacy*, vol. 8, pp. 60–63, Jan. 2010.
[4] H. Khurana, M. Hadley, L. Ning, and D. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, pp. 81–85, Jan. 2010.
[5] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, pp. 75–77, Mar. 2009.
[6] Smart Grid Interoperability Panel—Cyber Security Working Group Smart Grid Cyber Security Strategy and Requirements NIST, Gaithersburg, MD, Tech. Rep. draft NISTIR 76j, 2010.
[7] T. Chen, "Survey of cyber security issues in smart grids," in *Proc. Cyber Security, Situation Management, and Impact Assessment II; and Visual Analytics for Homeland Defense and Security II (part of SPIE DSS 2010)*, Orlando, FL, Apr. 2010, p. 77090D.
[8] T. Chen, J.C.S. Aarnoutse and J. Bufford, "Petri Net Modeling of Cyber-Physical Attacks on Smart Grid", *IEEE Transactions on Smart Grid,* vol.2, no.4, pp. 741-749, Dec. 2011.
[9] R. David and H. Alla, *Discrete, Continuous, and Hybrid Petri Nets*. Berlin, Germany: Springer-Verlag, 2005, pp. j9–294.
[10] K. Jensen and L. Kristensen, *Coloured Petri Nets: Modelling and Validation of Concurrent Systems*. Berlin, Germany: Springer-Verlag, 2009, pp. 193–198.
[11] X. Liu, P. Zhu, Y. Zhang and K. Chen, "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure", *IEEE Transactions on Smart Grid,* vol. 6, no. 5, pp. 2435-2443, Sep. 2015.
[12] J. McDermott, "Attack net penetration testing," in *Proc. Workshop New Security Paradigms (NSPW),* Cork, Ireland, 2000, pp. 15–21.
[13] G. Dalton, R. Mills, J. Colombi, and R. Raines, "Analyzing attack trees using generalized stochastic Petri nets," in *Proc. IEEE Workshop Inf. Assur.,* West Point, NY, USA, 2006, pp. 116–123.
[14] R. Wu, W. Li, and H. Huang, "An attack modeling based on hierarchical colored Petri nets," in *Proc. IEEE Int. Conf. Comput. Elect. Eng. (ICCEE),* Phuket, Thailand, 2008, pp. 918–921.
[15] K. Schneider, C.-C. Liu, and J.-P. Paul, "Assessment of interactions between power and telecommunications infrastructures," *IEEE Trans. Power Syst.*, vol. 21, no. 3, pp. 1123–1130, Aug. 2006.
[16] O. Gursesli and A. Desrochers, "Modeling infrastructure interdependencies using Petri nets," in *Proc. IEEE Int. Conf. Syst.,* vol. 2. Washington, DC, USA, 2003, pp. 1506–1512.
[17] J.-C. Laprie, K. Kanoun, and M. Kaaniche, "Modelling interdependencies between the electricity and information infrastructures," in *Proc. 26th Int. Conf. Comput. Safety Rel. Security (SAFECOMP),* Nuremberg,

Germany, 2007, pp. 54–67.
[18] V. Calderaro, C. N. Hadjicostis, A. Piccolo, and P. Siano, "Failure identification in smart grids based on petri net modeling," *IEEE Trans. Ind. Electron.*, vol. 58, no. 10, pp. 4613–4623, Sep. 2011.
[19] O. Dahl and S. Wolthusen, "Modeling and execution of complex attack scenarios using interval timed colored Petri nets," in *IEEE Int. Workshop Innov. Archit. Future Gen. High-Perform. Proc. Syst.*, Kona, Hawaii, Jan. 2006, pp. 49–55.
[20] T. Murata, "Petri Nets: Properties, Analysis and Application", Proceedings of the IEEE [0018-9219] Murata, Tadao yr:1989 vol:77 iss:4 pg:541 -580.
[21] J. R. Norris, "Markov Chains", Cambridge University Press, July 1998.
[22] CPN Tools: Available at: http://cpntools.org/. Accessed in 07/30/2014.
[23] N.Ghabi, C. Dutheillet and M. Ioualalen, "Colored stochastic Petri nets for modelling and analysis of multicasts retrial systems", Mathematical and Computer Modelling 49 (2009), pp. 1436-1448.
[24] G. Chiola, D. Dutheillet, G. Franceschinis and S. Haddad, "Stochastic Well-Formed Colored nets and symmetric modeling applications", IEEE Transactions on Computers 42 (1993), pp. 1343-1360.
[25] IEC61850-5 (2010). *Communication networks and systems in substations - Part 5:Communication requirements for functions and device model*, 2.0 edn, International Electro technical Commission, France.
[26] IEC 61850-9-2, *Communication networks and systems in substations – Part 9-2:* Sampled values over ISO/IEC 8802-3,Ed. 2.0, 2010.
[27] Chelluri, S., Dolezilek, D., Dearien, J., and Kalra, A. (2014). "Understanding and Validating Ethernet Networks for Mission-Critical Protection, Automation, and Control Applications", *NTPC Limited and Schweitzer Engineering Laboratories, Inc. All rights reserved. 20140327•TP6656-01*
[28] Zaitsev, D. A. and Shmeleva, T. R. (2006). Switched Ethernet response time evaluation via colored petri net model, Proc. of International Middle Eastern Multiconference on Simulation and Modelling, pp. 68-77.

Modeling of a Data Modification Cyber-Attack in an IEC 61850 Scenario Using Stochastic Colored Petri Nets

Milton Rafael da Silva, Luiz Edival de Souza and Carlos Waldecir de Souza
Institute of Systems Engineering and Information Technology
Federal University of Itajuba
Itajubá, Minas Gerais, Brazil
miltonrafa@yahoo.com.br; edival@unifei.edu.br; cw.souza@yahoo.com.br

***Abstract* - In the IEC 61850 standard, the transmission of the sampled values message packets of measurement in processing communication are defined, and these parameters are really important and critical in the automation of power systems. Related to the security analysis of the communication networks, a really powerful tool is the Stochastic Colored Petri Net (SCPN), because it models asynchronous and concurrent processes, and it is useful to analyze delays in timed systems. So, based in this context and knowing that the correct value of sampled values measurements is really critical in transmitting messages in the IEC 61850 context; it is modeled in an IEC 61850 scenario a cyber-attack using SCPN that aims to modify the data to be transmitted before it is packed as a Sampled Value (SV) message, what is really critical for the operation of the system. The results corresponded to the modeled cyber-attack, showing the efficacy of the proposed modeling method.**

***Keywords* – IEC 61850; Smart Grid; Stochastic Colored Petri Nets; Security Analysis; Modeling of Cyber-Attack.**

I. INTRODUCTION

In the intelligent transmission and power distribution networks based on interactive communication between all parts of the power conversion chain, known as Smart Grids, there are communication networks that allow the transfer of data between their components. Data exchanges, network topology, decentralized control, security, are inherent characteristics to the communication systems and are also an important part of the smart grids in the electric power sector.

In order that the information is exchanged in a correct, reliable and efficient way, standardization in data communication is needed. So there's the IEC 61850 standard. Referenced in [1], IEC 61850 proposes standards for the services and data formats exchanged on a network of electrical system equipment.

Security has been recognized as a critical matter with important implications in the smart grids scenario [2]–[7]. Also, cyber-attacks may attempt to access remotely the systems through the neighborhood area networks (NANs) or home area networks (HANs) in order to control the equipment or destroy them [8]. With the infrastructure of Internet and telecommunications, coordinating simultaneous attacks is really easy for distributed and different groups to do it [8].

In the scenario of cyber-attacks modeling, Petri nets became important tools for describing many different types of processes [9], [10], [11]. The importance of Petri nets in cyber-attack modeling was first cited perhaps by McDermott [12]. It was noted that Petri nets are really useful in identifying actions during an attack [8]. Dalton *et al. used* stochastic Petri nets for cyber-attack modeling in their work [13]. Stochastic Petri nets have the characteristics of being timed and transitions take place after random times. Transition delays were defined as exponentially distributed what transformed the stochastic Petri net developed in that work into an equivalent continuous-time Markov Chain. That transformation became true because of the analysis for Markov chains, but the exponential transition delays was not justified [8].

Colored Petri nets have become interesting for cyber-attacks modeling because they can express more details than the ordinary Petri nets, and also all marks (tokens) are not distinguishable from one another. In colored Petri nets, tokens carry data values (characteristics) represented by color, which allows different attackers and different actions to be represented in the model [8]. Wu *et al. developed* colored Petri nets for describing a hierarchical cyber-attack modeling [14]. At a high level of a model description and its programming, a modeled cyber-attack is a colored Petri net where some transitions have hidden details, which can be viewed in details in a subpage that is another colored Petri net [8].

About the electrical system, Chen *et al.* [8] proposed a new manner to create a wide Petri net from simple Petri nets in order to model some small cyber-physical attacks on the smart grid [11]. Also, Petri nets have been used to present interdependencies between the electrical and communications systems [15]–[17]. Besides, Calderaro *et al*. [18] presented a describing method using Petri nets in order to identify and localize failures in the smart grid. Dahl and Wolthusen used timed colored Petri nets with the aim to create timed attacks carried out by many attackers against possibly different targets [8], [19].

One can note that in these Petri net models places represent all states of the modeled systems and transitions changes the modeled states. What it means is that interdependencies are created with the electrical and communication devices in a unique Petri net [8].

So, in this work, based in all previous works and in a simple IEC 61850 scenario, it is proposed to model and analyze a cyber-attack in a simple architecture with one merging unit publishing Sampled Value messages, a switch for packet switching and storage, and a network analyzer to check

978-1-5386-1107-4/17/$31.00 ©2017 IEEE

the packets sent. This cyber-attack aims to modify the transmission of the Sampled Value messages (Data Modification) and assess the impact of it in the electrical power system communications systems. Data modification, also known as data diddling or data injection, involves changing data before they are processed at their destination [20].

II. STOCHASTIC COLORED PETRI NET (SCPN)

The Petri net (PN), discussed in [21], is a graphical mathematical tool for studying systems characterized as competitors, asynchronous, distributed, parallel, non-deterministic and/or stochastic. Briefly, the PN is a bipartite graph (graphs that don't contain odd cycles) with graphical interpretation formed by two components: transition and place. Representation is as follows in Figure 1, in which spaces are the circles and thin rectangles are transitions. These two components, also called nodes, are connected by directed arcs.

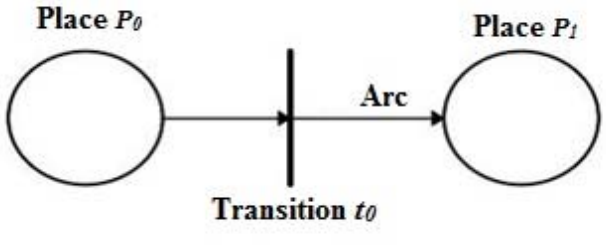

Figure 1. Basic Elements of a PN

For modeling and better interpretation of systems, it is used marks (tokens) assigned to the places that allow to represent the state situation. The movement of the marks through well-defined rules represents the system dynamics.

In the field of network protocol analysis, the Stochastic Petri Net (SPN), variants of PN, are constantly applied in the performance analysis in the computer networks and communication systems, since SPN is isomorphic and enables, together with the Markov chains [22], the state probability analysis of the system. However, even with these important characteristics, the SPNs are limited in complex models and in models with industrial dimensions.

The Stochastic Colored Petri Nets (CSPN) has higher abstraction capacity. This allows each place to have various types of marks and transitions that represent various types of functions, thereby reducing the number of nodes. A key point for the application of this type of Petri nets in the communication systems is precisely the connection with programming languages, as an example the Meta Language (ML) used in CPN Tools [23] software.

Formally, the definition for the SCPN is represented as follows and can be verified in [24] and [25]:

$SCPN = \{P, T, CB, C, W^-, W^+, W^h, Pri, M_0, \theta\}$

• P is the finite set of places;
• T is the finite set of timed and immediate transitions, $P \cap T = \emptyset$, $P \cup T \neq \emptyset$;
• CB is the family of basic color classes: $CB=\{C_1,...,C_n\}$ with $C_i \cap C_j = \emptyset$;
• C is a $P \cup T$ function that associates to any r node a color domain $C(r)$ that is the Cartesian product of the CB elements;
• W^-, W^+, W^h: $W^-(p, t)$, $W^+(p, t)$, $W^h(p, t) \in [C(t) \rightarrow Bag(C(p))]$ are functions that label respectively the entrance, output and inhibitors arches between t transitions and p places;
• Pri is the priority function defined as follows: $\forall t \in T$, $Pri(t) : C(t) \rightarrow N.Pri(t)(c)$ is the priority of the instance$[t,c]$.
• M_0 is the initial marking that describes the initial state of the system;
• θ is the defined function in the set of transitions T given that $\theta(t)$ is the time function of the model.

III. IEC 61850 – GENERAL OVERVIEW

The IEC 61850 is an international standard that defines the communication and services form between different equipment present in the automation of power electrical systems [26]. It establishes the following objectives: Interoperability between manufacturers, free configuration (modeling), and long-term stability.

The most significant benefits of implementing this standard are the independence of future technology, ease of long-term maintenance, reduced wiring, and free specification and exchange of data at high speed.

A. Sampled Values

This type of message has the proposal of transmission of sampled values of measurement, according to [27], inserted into types of *unicast* or *multicast* messages. Commonly, this message is used to send analog data coming from the current and voltage meters (Current Transformers and Voltage Transformers).The IED (Intelligent Electronic Device) that implements the messages *Sampled Values* (SV) needs hardware that supports huge volume of Analog-to-Digital conversions that must be processed quickly and safe. This is only possible with the use of more resistant components, more reliable and more expensive. This is the burden that SV messages produce in the IEDs that implement them.

The sampled values are used by control and protection system. The frames of SV messages uses layer1 of the TCP / IP model and are extremely fast.

IV. SCPN MODELING OF AN IEC 61850 SYSTEM – *SAMPLED VALUE* (SV) MESSAGES AND CYBER-ATTACK

The following SCPN models seek to represent the main characteristics of the devices presented in the proposed architecture. So the proposed methodology concerns about analyze the performance of this network architecture using modeling only, when it is working normally or when it is attacked. According to the presented theoretical basis, it is started then the development of a SCPN modeling of the standard IEC 61850 together with a cyber-attack. For this, two guidelines are defined. The first one deals with the part of system concepts involving the definitions of the standard IEC

61850. The second one, structures the way how it should be elaborate the models in SCPN, together with the modeled cyber-attack. In Figure 2 it can be seen the proposed architecture.

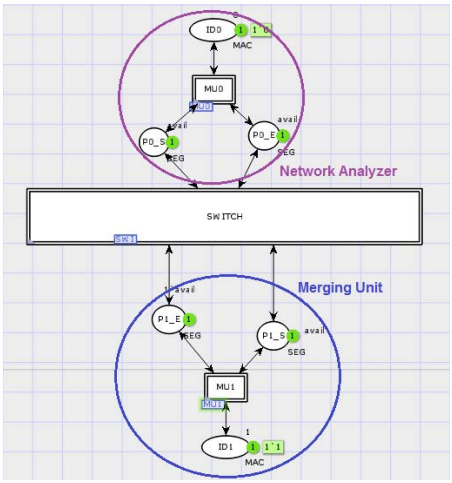

Figure 2. Proposed Architecture

A. *Switch Model*

The switch model has the main features of this device. The switching tables, packet buffer, switch processing and physical communication interfaces (input and output ports) are all defined. To better understand this model, only one communication port is defined. For the representation of other ports, a simply replication of such model is done. Figure 3 shows the main characteristics of this device. The switch model is based on the work developed in [28], in which this equipment is represented in CPN models.

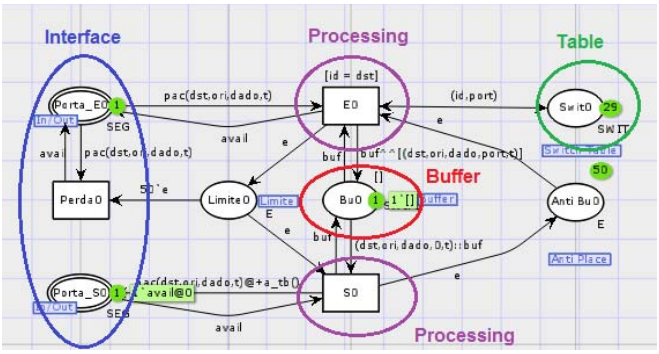

Figure 3. CPN Model of the Switch

Regarding the model representation, Figure 3 indicates the dynamics of a SV packet within a real switching device. The message enters via the communication interface (place **Porta_E0**), then it is processed (transitions **E0** and **S0**), stored in the buffer (place **Bu0**) and then is transmitted according to the switching table to the respective destination (place **Swit0**). This whole process takes time, called by the norm as propagation time, and for this reason it is attributed to the time stamp @ + tb () in the transition **S0**.

B. *Merging Unit Model*

The model of Figure 4 represents the physical *merging unit* device that converts the analog signals into digital signals, and sends such signals in the format of *Sampled Value* messages.

The CPN representation of the *merging unit* characterizes the signal sampling, the processing of the samples by the logical nodes and the interfacing with the network.

The sampling process is done by reading a text file containing the current transformer samples, which simulates the data of a real transformer. The text file is read through the function defined in the **Inicio** transition, and through the **getPacketsTC** () function. After that, the file data is transformed into CPN tokens. **TCTR** and **MMXU** transitions, which represent the logical nodes defined in the IEC 61850 standard, translate the information from the samples (tokens) and pack them into the *Sampled Value* format. The right part of the model represents the communication interface of the device (**LAN_S** and **LAN_E** places). The **Origem** and **Destino** places indicate the communication interface of the source and destination of the packages (**Origem** and **Destino** places) generated by the *merging unit*. With this structure, the *merging unit* model is able to simulate real devices sending SV messages.

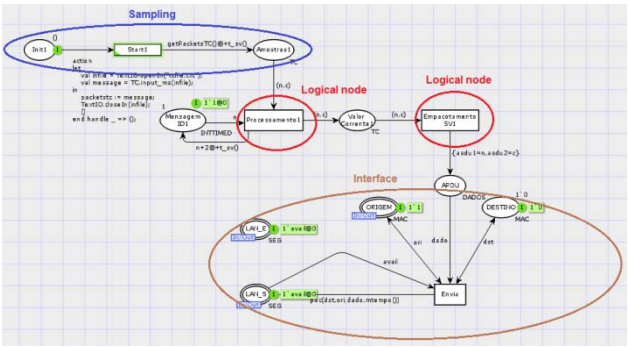

Figure 4. CPN Model of the Merging Unit

C. *Analyzer Model*

The analyzer model is characterized in a simple way according to Figure 5. The function of this model is to represent the device that verifies the latency time of the *Sampled Value* messages that is transferred in the network.

To do this, the model receives the messages through the communication interface (**LAN_E** place) and then verifies the origin of the packet (**Recebe** transition and **Origem** place) identifying the *merging unit* transmitter. After this, the message is sent to the **Buffer** transition where the transfer time of each SV packet is calculated.

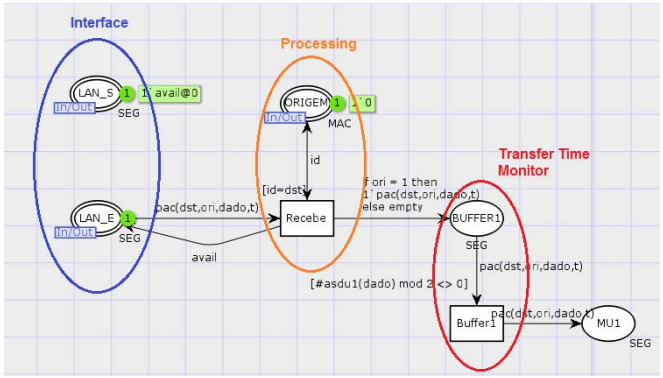

Figure 5. CPN Model of the Analyzer

D. *Cyber Attack Model*

In the cyber-attack model presented in color red in Figure 6, the aim of the modeled Data Modification attack is to modify the data to be transmitted before it is packed as a Sampled Value (SV) message. In this case, the value of analog data coming from the current and voltage transformers will be modified (attacked) before it is packed as a Sampled Value message.

For this cyber-attack model, it was created the function *fail(),* a uniform distribution that generates a random value between 0 and 1. As soon as this random value is generated, that value goes to the place *Prob.* Depending on this value, the transition *Normal* or the transition *Attack* is enabled. To enable the *Normal* transition, this random generated value must be greater than 0.4. To enable the *Attack* transition, this random generated value must be smaller than or equal to 0.4. This indicates a cyber-attack probability of 40%. If the *Normal* transition is enabled, the message flow is normal. If the *Attack* transition is enabled, the analog datum received from the current and voltage transformers will be modified, and the message flow will be delayed according to the function *delay_attack(),* a normal distribution that generates a random value with mean 10 and variance 2, in order to indicate that a cyber-attack occurred in the system.

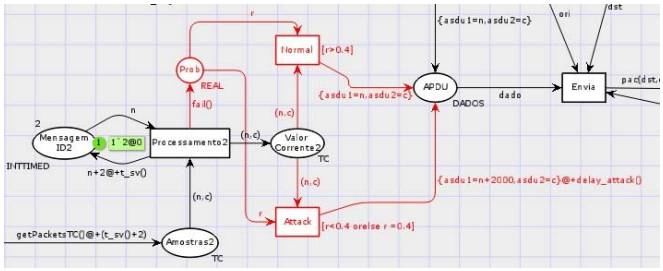

Figure 6. Cyber-attack Model

V. RESULTS AND DISCUSSION

For cyber-attack analysis, it is used the simulation tools available in the *CPN Tools software*. It follows some results generated from model simulations in Figure 7.

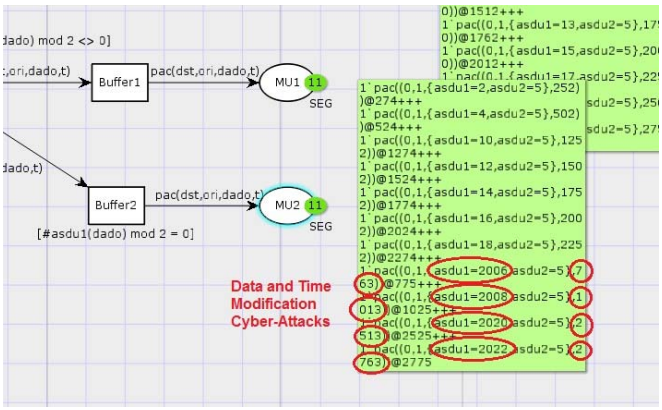

Figure 7. 4 Cyber-attacks for 11 received packets

The structure of the packets is: pac (dst,ori, dado, t). This means that the first number of the packet is the destination of the datum; the second number is the origin of the datum (0 or 1 indicates respectively Merging Unit 0 or Merging Unit 1); the third one is the value of the datum, which varies from 1 to 2000, as it was modeled in this model and the last one is the time spent for the datum to leave the origin and get to the final destination.

In this model, the read of the analog data that is coming from the current transformer comes from a txt file named *tcfile2*. In this txt file, the first eleven values of the data are: (asdu1=2); (asdu1=4); (asdu1=6); (asdu1=8); (asdu1=10); (asdu1=12); (asdu1=14); (asdu1=16); (asdu1=18); (asdu1=20); (asdu1=22). As it can be noticed in Figure 7, the first eleven received values of the data are: (asdu1=2); (asdu1=4); (asdu1=10); (asdu1=12); (asdu1=14); (asdu1=16); (asdu1=18); (asdu1=2006); (asdu1=2008); (asdu1=2020); (asdu1=2022). The missing packets (asdu1=6); (asdu1=8); (asdu1=20); and (asdu1=22) from the *tcfile2* have been attacked by the modeled Data Modification Cyber-Attack proposed in this work. The offset between these four missing packets and the last four received packets is 2000, which is in according to what was modeled in transition *Attack*, in color red in Figure 6, *n+2000*, where *n+2000* corresponds to asdu1 value. The presented values have been attacked by a Data Modification Attack, because the final objective of this kind of attack is to change data before they are processed at their destination, and this goal was achieved in this simple model. Also, in these four attacked packets in this model, it can be noticed that the time spent for the datum to leave the origin and get to the final destination was delayed, according to the function *delay_attack()* implemented in this work. The times were supposed to be 752, 1002, 2502 and 2752, but the times are 763, 1013, 2513 and 2763 in the attacked packets, so there's an offset of 13 in the time in the attacked packets.

So, presented results are in according to what was expected and modeled in this scenario. Knowing that any data modification of the SV messages may affect the protection and

the control power systems, because its frames of messages uses layer1 of the TCP / IP model and are extremely fast, these modeled data modification with time delay in this simple IEC 61850 scenario could lead to misoperation of circuit breakers and relays, and could generate serious problems in power substations, because false data are being injected in the system.

VI.CONCLUSION

According to what is presented in this article, it is concluded that the SCPN modeling is perfectly applicable to the modeling of cyber-attacks of an IEC 61850 scenario. The presented methodology is simple, but can support some important details in the design of protection process of IEC 61850 architectures.

The results generated with simulations prove that the model responded correctly according to the functions created to produce the cyber-attack. Also, knowing that any data modification of the SV messages may affect the protection and the control power systems, these modeled data modification in this simple IEC 61850 scenario could generate serious problems in power substations, because false data are being injected in the system.

Future projects include the modeling of new cyber-attacks that can become potential threats to substation networks. Also, those cyber-attacks can be improved and sophisticated, avoiding future possible problems with the security of the system.

VII. ACKNOWLEDGEMENTS

I would like to dedicate this work to my God, *Yahweh* (יהוה), for giving me strength to overcome difficulties. My sincere thanks to the Federal University of Itajuba (UNIFEI). Also, I gratefully acknowledge CNPq (National Council for Scientific and Technological Development – Brazil) for funding this work.

VIII. REFERENCES

[1] IEC 61850-1, *Communication networks and systems in substations – Part 1: Introduction and overview,* Ed. 2.0., 2010.
[2] F. Cleveland, "Cyber security issues for advanced metering infrastructure (AMI)," in *Proc. 2008 IEEE Power Energy Soc. Gen. Meet.—Convers. Del. Electr. Energy 21st Century*, Pittsburgh, PA, Apr. 2008, pp.1–5.
[3] F. Cohen, "The smarter grid," *IEEE Security Privacy*, vol. 8, pp. 60–63, Jan. 2010.
[4] H. Khurana, M. Hadley, L. Ning, and D. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, pp. 81–85, Jan. 2010.
[5] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, pp. 75–77, Mar. 2009.
[6] Smart Grid Interoperability Panel—Cyber Security Working Group Smart Grid Cyber Security Strategy and Requirements NIST, Gaithersburg, MD, Tech. Rep. draft NISTIR 76j, 2010.
[7] T. Chen, "Survey of cyber security issues in smart grids," in *Proc. Cyber Security, Situation Management, and Impact Assessment II; and Visual Analytics for Homeland Defense and Security II (part of SPIE DSS 2010)*, Orlando, FL, Apr. 2010, p. 77090D.
[8] T. Chen, J.C.S. Aarnoutse and J. Bufford, "Petri Net Modeling of Cyber-Physical Attacks on Smart Grid", *IEEE Transactions on Smart Grid,* vol.2, no.4, pp. 741-749, Dec. 2011.
[9] R. David and H. Alla, *Discrete, Continuous, and Hybrid Petri Nets*. Berlin, Germany: Springer-Verlag, 2005, pp. j9–294.
[10] K. Jensen and L. Kristensen, *Coloured Petri Nets: Modelling and Validation of Concurrent Systems*. Berlin, Germany: Springer-Verlag, 2009, pp. 193–198.
[11] X. Liu, P. Zhu, Y. Zhang and K. Chen, "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure", *IEEE Transactions on Smart Grid,* vol. 6, no. 5, pp. 2435-2443, Sep. 2015.
[12] J. McDermott, "Attack net penetration testing," in *Proc. Workshop New Security Paradigms (NSPW),* Cork, Ireland, 2000, pp. 15–21.
[13] G. Dalton, R. Mills, J. Colombi, and R. Raines, "Analyzing attack trees using generalized stochastic Petri nets," in *Proc. IEEE Workshop Inf. Assur.,* West Point, NY, USA, 2006, pp. 116–123.
[14] R. Wu, W. Li, and H. Huang, "An attack modeling based on hierarchical colored Petri nets," in *Proc. IEEE Int. Conf. Comput. Elect. Eng. (ICCEE),* Phuket, Thailand, 2008, pp. 918–921.
[15] K. Schneider, C.-C. Liu, and J.-P. Paul, "Assessment of interactions between power and telecommunications infrastructures," *IEEE Trans. Power Syst.*, vol. 21, no. 3, pp. 1123–1130, Aug. 2006.
[16] O. Gursesli and A. Desrochers, "Modeling infrastructure interdependencies using Petri nets," in *Proc. IEEE Int. Conf. Syst.,* vol. 2. Washington, DC, USA, 2003, pp. 1506–1512.
[17] J.-C. Laprie, K. Kanoun, and M. Kaaniche, "Modelling interdependencies between the electricity and information infrastructures," in *Proc. 26th Int. Conf. Comput. Safety Rel. Security (SAFECOMP),* Nuremberg, Germany, 2007, pp. 54–67.
[18] V. Calderaro, C. N. Hadjicostis, A. Piccolo, and P. Siano, "Failure identification in smart grids based on petri net modeling," *IEEE Trans. Ind. Electron.*, vol. 58, no. 10, pp. 4613–4623, Sep. 2011.
[19] O. Dahl and S. Wolthusen, "Modeling and execution of complex attack scenarios using interval timed colored Petri nets," in *IEEE Int. Workshop Innov. Archit. Future Gen. High-Perform. Proc. Syst.*, Kona, Hawaii, Jan. 2006, pp. 49–55.
[20] Tom Bartman and Kevin Carson, "*Securing Critical Industrial Systems with SEL Solutions"*, SEL (Schweitzer Engineering Laboratories, Inc.) White Paper LWP0013-01, Date Code 20150406, © 2015 by Schweitzer Engineering Laboratories, Inc. All rights reserved.
[21] T. Murata, "Petri Nets: Properties, Analisys and Application", Proceedings of the IEEE [0018-9219] Murata, Tadao yr:1989 vol:77 iss:4 pg:541 -580.
[22] J. R. Norris, "Markov Chains", Cambridge University Press, July 1998.
[23] CPN Tools: Available at: http://cpntools.org/. Accessed in 07/30/2014.
[24] N.Ghabi, C. Dutheillet and M. Ioualalen, "Colored stoschastic Petri nets for modelling and analysis of multicass retrial systems", Mathematical and Computer Modelling 49 (2009), pp. 1436-1448.
[25] G. Chiola, D. Dutheillet, G. Franceschinis and S. Haddad, "Stochastic Well-Formed Colored nets and symmetric modeling applications", IEEE Transactions on Computers 42 (1993), pp. 1343-1360.
[26] IEC61850-5 (2010). *Communication networks and systems in substations - Part 5:Communication requirements for functions and device model*, 2.0 edn, International Electrotechnical Commission, France.
[27] IEC 61850-9-2, *Communication networks and systems in substations – Part 9-2:* Sampled values over ISO/IEC 8802-3,Ed. 2.0, 2010.
[28] Zaitsev, D. A. and Shmeleva, T. R. (2006). Switched ethernet response time evaluation via colored petri net model, Proc. of International Middle Eastern Multiconference on Simulation and Modelling, pp. 68-77.