Implementação e Demonstração de Ataques Cibernéticos em Sistemas SCADA

Camilla E. J. F. Figueiredo, Mikaelly F. Pedrosa e Iguatemi E. Fonseca

***Resumo*— Inserido no contexto de segurança de redes em sistemas ciber-físicos, o presente artigo investiga vulnerabilidades nas comunicações entre dispositivos em um sistema SCADA e evidencia ataques ambicionando penetrá-lo e comprometer serviços fornecidos por uma *smart grid*, que podem (se bem-sucedidos) ter quaisquer fins, desde danos financeiros à letais. Para tanto, como metodologia, utilizou-se a pesquisa bibliográfica exploratória bem como a pesquisa prática experimental e implementação de ataques habituais, além da contribuição de outro ataque ausente em trabalhos anteriores, para obtenção de uma análise qualitativa. Resultante disso, a efetividade dos ataques aqui trabalhados reitera vulnerabilidades do sistema exploradas em cenários reais.**

***Palavras-Chave*— Smart Grids, SCADA, Modbus, Scapy, Segurança, Ataques Cibernéticos.**

***Abstract*— Inserted in the context of network security in cyber-physical systems, this paper investigates vulnerabilities in communication between devices in a SCADA system and highlights attacks that aim to penetrate it and compromise services provided by a smart grid, which may (if successful) have any purpose, from financial to lethal damage. Therefore, as a methodology, exploratory bibliographic research as well as experimental practical research - implementing some habitual to theses environments, besides contributing with another attack absent in previous works - to obtain a qualitative analysis. As a result, the attacks' effectiveness explored here reiterates system vulnerabilities exploited in real-world scenarios.**

***Keywords*— Smart Grids, SCADA, Modbus, Scapy, Security, Cyber-attacks.**

I. Introdução

Entende-se por *smart grid*, um sistema baseado em comunicação e tecnologia da informação adequado para a geração, fornecimento e consumo de energia. Tratam-se de redes inteligentes que são incorporadas às usinas a fim de recolher e administrar dados e, com base nestas informações coletadas, controlá-las com eficácia. Para tal, as *smart grids* utilizam do fluxo bidirecional de informações, com intuito de formar um sistema automatizado, amplamente distribuído e disponível de novas funcionalidades. Estas aplicabilidades indicadas são: controle, competência operacional, resiliência da rede e uma melhor integração de tecnologias renováveis [1].

Incorporado a *smart grid*, o encargo de efetuar as coletas, supervisão e administração dos dados compete ao Sistema de Supervisão e Controle (SCADA). Os dados obtidos geralmente referem-se a valores de medidas e *status* dos diversos componentes da rede, tornando o sistema uma parte fundamental do setor elétrico, mediante a sua capacidade de cobrir grandes áreas e executar comunicações em tempo real. O SCADA é amplamente utilizado para supervisionar e monitorar continuamente infraestruturas críticas, como redes de distribuição de água, usinas de geração e distribuição de eletricidade, refinarias de petróleo, usinas nucleares e sistemas de transporte público [2].

Em contrapartida das amplas aplicabilidades e proveitos, as *smart grids* apresentam grandes riscos. Qualquer interrupção na geração de energia é capaz de interferir na estabilidade da rede e consequentemente vir a causar impactos socioeconômicos em larga escala. Além destes informes, como dados significativos são trocados entre os sistemas, o furto ou alteração destes pode ainda violar a privacidade do consumidor dos serviços. Diante destas vulnerabilidades, *smart grids* tornaram-se alvos de atacantes, obtendo a atenção e interesse do governo, da indústria e de pesquisadores [3].

Constatando as fragilidades mencionadas do sistema, alguns ataques em grandes proporcionalidades sucederam-se ao longo dos anos. Em julho de 2010, uma arma cibernética atingiu uma instalação nuclear iraniana, introduzida através de um *pendrive* - dispositivo de memória USB. O *worm* denominado Stuxnet obteve controle do sistema SCADA responsável por controlar as centrífugas de enriquecimento de urânio, estabelecendo com que girassem 40% mais rápido e, como resultado, provocando rachaduras e problemas de funcionamento. O *software* malicioso também era incumbido de capturar dados sensíveis e enviá-los diretamente aos invasores [2], [4].

Posteriormente, em dezembro de 2015 na Ucrânia, houve uma queda de energia decorrente de um ataque cibernético, cuja a interrupção afetou mais de 225.000 pessoas. A princípio, o ataque iniciou-se através de um *malware* para o reconhecimento e monitoramento da rede elétrica, visando o planejamento das etapas do ataque. No dia em que o ataque ocorreu, o sistema SCADA foi invadido e usado pelos atacantes para abrir remotamente vários disjuntores, ocasionando o corte direto na energia de milhares de cidadãos. Agravando a situação, o sistema telefônico e a rede de comunicação foram comprometidos por um ataque de negação de serviço (*DoS - Denial of Service*), impossibilitando que os clientes pudessem informar sobre o ocorrido. Esta ação, foi uma dentre as medidas danosas cometidas pelos atacantes a fim de dificultar as medidas de restauração do sistema [5].

Diante dos problemas mencionados relacionados à segurança da *smart grid* e portanto, no SCADA, muitos esforços vêm sendo feitos por parte das indústrias e pesquisadores

Camilla Emilly Jácome Ferreira de Figueiredo e Iguatemi Eduardo da Fonseca, Programa de Pós-Graduação em Informática (PPGI), UFPB, João Pessoa-PB, e-mail: camilla.jacome@estudantes.ufpb.br, iguatemi@ci.ufpb.br; Mikaelly Felicio Pedrosa, Centro de Informática, UFPB, João Pessoa, e-mail:mikaelly.felicio@cc.ci.ufpb.br. Este trabalho foi parcialmente financiado pelo CNPq e pela CAPES.

visando uma maior proteção para o sistema. Para tal, o controle de acesso, a autenticação e a detecção de intrusões atuam como os mecanismos de segurança mais utilizados. À vista de que os sistemas SCADA operam integralmente durante a semana e 24 horas por dia, torna-se pouco viável pesquisas e experimentos em cenários reais [2].

Este artigo tem como objetivo realizar experimentos a fim de explorar as vulnerabilidades presentes nos sistemas SCADA e seus protocolos de comunicação. Para alcançar tal propósito, mediante a linguagem *Python* em conjunto com a ferramenta *Scapy* [9], foram implementados e testados três ataques cibernéticos, a saber: (i) Homem no Meio (*MitM - Man-in-the-Middle*); ii) Inundação Syn (*Syn Flood*); iii) Ataque de reflexão. Os dois primeiros discutidos em demais trabalhos através de diferentes abordagens de reprodução da que aqui empregada [2] [10] [11]. Entretanto, o terceiro ataque citado, encontra-se neste trabalho como a maior contribuição do estudo em virtude da sua ausência de implementação no contexto de sistemas SCADA.

O documento encontra-se organizado da seguinte forma: inicialmente é apresentado, na Seção II, a arquitetura do SCADA juntamente com os protocolos de comunicação empregados. Em seguida, tem-se uma revisão de segurança cibernética, com menção aos principais ataques aos quais o sistema está exposto, que serve como base para a compreensão de como estes funcionam e comprometem a defesa das *smart grids*. Na quarta seção, encontram-se as implementações dos experimentos anteriormente mencionados, bem como os resultados obtidos; e, por fim, as considerações finais e pretensões de trabalhos futuros estão presentes na última seção.

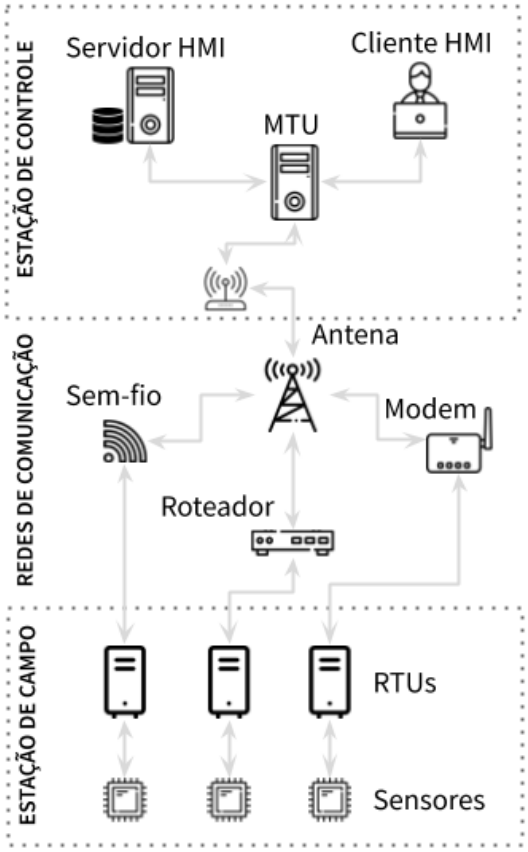

Fig. 1
ARQUITETURA TÍPICA DOS SISTEMAS SCADA.

II. ARQUITETURA DO SISTEMA E PROTOCOLOS

O sistema SCADA possui uma arquitetura constituída por dispositivos e componentes diversificados. Dentre estes distingue-se a Unidade Terminal Principal (MTU - *Master Terminal Unit*), uma unidade de controle centralizada, responsável por todo o fluxo de informações e controles no sistema. O acesso a esta unidade é realizado através da Interface Homem Máquina (HMI - *Human Machine Interface*), local em que é possível visualizar dados, configurar parâmetros e executar comandos, possibilitando o administrador da rede determinar ações e envios destes comandos de controle aos demais dispositivos. Ainda é atribuído à MTU a supervisão e controle de processos físicos, dispositivos (sensores e atuadores) e da Unidade Terminal Remota (RTU - *Remote Terminal Unit*), cuja a função é coletar dados dos dispositivos em campo, como sensores, e retornar à MTU por meio de protocolos de comunicação [2]. Na Figura 1 é demonstrada uma arquitetura SCADA característica.

O fluxo de informação entre dispositivos do sistema ocorre a partir de protocolos de interconexão de rede, que projetados com este fim, garantem eficiência, confiabilidade e precisão nas operações. Realizadas em tempo real, prover tais operações teve influência direta no projeto de protocolos: a priorização da velocidade e agilidade em detrimento de outras funcionalidades reflete a negligência para com a segurança presente nestes protocolos - como consequência, houve a retirada de algumas funcionalidades de proteção.

No âmbito explorado neste artigo - das redes industriais que fazem uso do sistema SCADA - os protocolos DNP3, Profinet e Modbus são os mais comumente encontrados. O terceiro, existente em duas variantes (Modbus RTU e Modbus TCP) será utilizado aqui por meio dos experimentos apresentados na Seção 4 na versão em que o pacote do protocolo é incorporado no segmento TCP (Modbus TCP). O Modbus TCP é uma das versões candidatas a ser utilizada em sistemas *smart grid* [6].

A. Protocolo Modbus

O protocolo Modbus é fundamentado no conceito de mestre-escravo, no qual apenas um nó mestre está conectado a um ou vários nós escravos (tendo como número máximo 247). Sua comunicação é sempre iniciada pelo mestre e os escravos respondem apenas quando solicitados. Isto é, os nós escravos nunca transmitem dados sem receber uma solicitação do nó mestre, como também nunca há transmissões entre si [6].

Além destas características, no Modbus não existem requisitos para diagnósticos relacionados ao estado do nó escravo. Caso o mestre solicite um dado com informações desconhecidas ao escravo, ele enviará como resposta uma exceção. Contudo, se a variável do processo estiver incorreta ou o dispositivo apresentar problemas de funcionamento, não há suporte no protocolo para que o escravo comunique isto, uma vez que fora projetado sem mecanismo algum de segurança.

Fig. 2
TROCA DE MENSAGENS MODBUS.

Por consequência, as mensagens podem ser interceptadas, reproduzidas ou até mesmo falsificadas, gerando um enorme prejuízo nas operações de controle ou supervisão [4].

Na Figura 2 é possível ver a comunicação dos dispositivos através do protocolo Modbus.

III. SEGURANÇA CIBERNÉTICA

Como componente principal dos sistemas de controle, o SCADA é o principal alvo dos invasores. Os ataques exploram as diversas fragilidades no sistema, sejam elas de *hardware*, *software* ou nos protocolos de comunicação. Com trocas de mensagens em larga escala acontecendo simultaneamente, o risco de um ataque cibernético explorando os protocolos de comunicações é alto. A seguir estão citados ataques relacionados a qual o sistema está sujeito, sendo alguns utilizados para os ensaios da próxima seção.

- **Homem no Meio (MitM - *Man-in-the-Middle*):** O ataque do homem no meio acontece quando um atacante está inserido entre dois dispositivos legítimos, "escutando" a comunicação, com a possibilidade de interceptar, alterar e modificar os dados transmitidos. O invasor está conectado aos dois dispositivos e retransmite o tráfego entre eles. Esses dispositivos legítimos parecem se comunicar diretamente quando na verdade estão se comunicando através do terceiro dispositivo atacante [3].
- **Repetição *(Replay):*** Em razão das informações do tráfego industrial serem transmitidas em texto plano, isto é, sem criptografia, um usuário malicioso pode capturar pacotes, registrar parte das informações válidas - comprometendo assim a integridade da comunicação - e repetí-los ao servidor do sistema sem ser detectado devido a validade das mensagens originais.
- **Exaustão de Recursos:** O principal objetivo deste ataque é afetar a disponibilidade do sistema incapacitando os dispositivos. Para isso, existem alguns ataques conhecidos na literatura, dentre esses destacamos:
  - **Inundação SYN *(SYN Flood)*:** O invasor inunda o sistema de destino com solicitações de conexão sem responder aos *replays*, forçando o sistema a travar. O protocolo Modbus TCP é vulnerável a esses ataques, pois opera sobre TCP [3].
  - **Reflexão *(Reflection)*:** O atacante envia uma mensagem mascarando seu próprio endereço IP (*Internet Protocol*) com o IP da vítima do ataque para *hosts* que atuarão como reflectores. Estes, por sua vez, enviam numerosas respostas ao endereço IP da vítima, sendo a carga útil dessas respostas muito superior à da solicitação. Dessa forma, quando a quantidade de tráfego de resposta for lançada, a vítima ficará submersa na inundação do ataque [7]. No contexto dos sistemas SCADA, o mestre atua como a vítima e os escravos como refletores.
- **Malware:** O SCADA é vulnerável a ser infectado por diversos softwares maliciosos - como vírus e *worms* - que possuem efeitos nocivos ao sistema. Dentre as diversas consequências, tem-se a diminuição da comunicação entre subestações e centros de controle [8]. Com o propósito de infectar um dispositivo ou sistema específico na *smart grid*, atacantes utilizam-se de *malwares* como o vírus. O *worm*, por sua vez, opera como um programa auto replicante que espalha-se através da rede, copiando-se para infectar outros dispositivos e sistemas [3].

IV. RESULTADOS EXPERIMENTAIS

A. Cenário Experimental e Métricas

Os experimentos para o presente estudo foram desenvolvidos a partir de nós virtuais, dispostos pelo *software* de virtualização *VMWare Workstation*, conectados entre si por meio do adaptador da rede configurado no modo *bridge*. Nesta condição, estão conectados diretamente pela rede física. Posto que tais dispositivos estão operantes, para implementar o protocolo Modbus TCP foi utilizada a linguagem de programação *Python* em conjunto com o *Scapy*. O *Scapy* é uma ferramenta de manipulação de pacotes, capaz de forjar ou decodificar mensagens de um grande número de protocolos, com a possibilidade de enviá-los na rede e capturá-los, corresponder solicitações e respostas, além de outras funcionalidades [9].

Correlacionadas aos experimentos, foram definidas algumas métricas em conformidade com o estudo, a saber: integridade, confiabilidade e disponibilidade do sistema. Adicionalmente, também foi examinado o consumo da largura de banda da rede utilizando a ferramenta de monitoramento de rede Bmon (*Bandwidth Monitor*), que opera como um monitor de largura de banda e estimador de taxa confiável e eficaz em tempo real. Na Figura 3 pode-se observar o cenário utilizado para a realização dos testes.

Como constatado na Figura 3, o cenário construído é composto dos seguintes dispositivos: máquinas RTU e MTU, HMI, sensores e uma máquina atacante. O primeiro atua como dispositivo escravo, enquanto o segundo desempenha função de nó mestre. Tendo esse princípio e visto que a comunicação só pode ser iniciada pelo mestre, para o RTU apenas é lícito operar mediante solicitação da MTU, recebendo comandos e enviando mensagens de respostas de volta ao mestre. Conformemente, o atacante refere-se a um invasor infiltrado dentro da rede interna, cujo o propósito é acometer o funcionamento do sistema seja na integridade, disponibilidade ou confiabilidade. Para o caso destes experimentos em questão, o objetivo do invasor concerne em afetar a disponibilidade da rede mediante dos ataques de reflexão e de Inundação SYN. Complementarmente, o nó malicioso operou ainda como

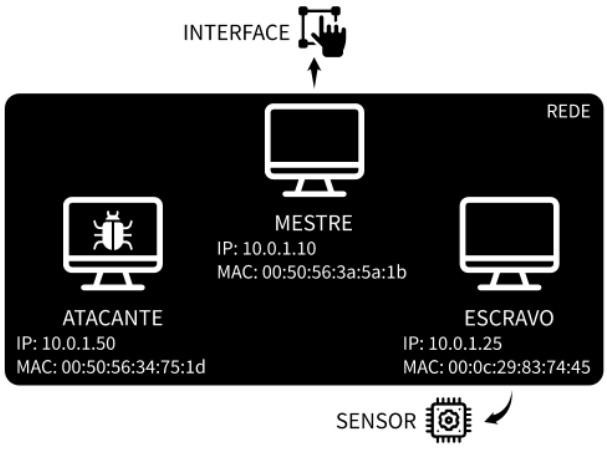

Fig. 3
CENÁRIO DOS EXPERIMENTOS.

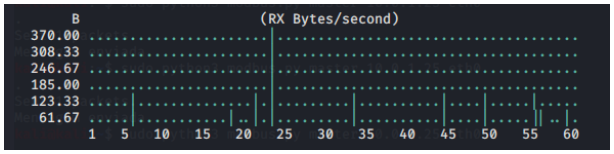

Fig. 4
GRÁFICO DO TRÁFEGO DE REDE NORMAL.

um homem do meio, executando o ataque homônimo que corrompe a integridade da mensagem e a confiabilidade do sistema.

B. Ataques Implementados e Resultados

1) ***Inundação SYN****:* Para a realização deste ataque, o *script* foi efetuado no nó invasor. Este, quando executado, tem a função de inundar a vítima com pacotes Modbus na Porta 502 - reservada unicamente ao protocolo. A cada nova mensagem remetida, o atacante substitui seu próprio endereço IP por um novo, gerado aleatoriamente, enviando inúmeras e sucessivas mensagens Modbus TCP para o alvo em questão. Após inundado, dependendo do volume de dados destinados a ele, sua capacidade de transmissão é excedida e é interrompida a comunicação deste com os demais dispositivos da rede. Quanto mais abundante o número de mensagens oriundas do invasor na rede, maior o consumo da mesma. No presente trabalho, foi realizado este ataque tanto no nó mestre quanto no escravo, resultando no aumento do consumo da largura de banda de ambos.

A Figura 4 mostra um gráfico gerado pelo Bmon, que demonstra a relação do sinal recebido em bytes pelo tempo em segundos. Neste caso, o monitoramento foi verificado na MTU, com o tráfego da rede regular e sem intermédio de ataques.

Em contrapartida, a Figura 5 exibe o gráfico resultado do monitoramento do tráfego da rede também efetuado na MTU mas, nesta ocorrência, com a interferência do ataque de Inundação SYN. Nota-se uma ampliação significativa do

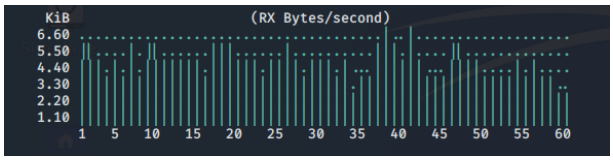

Fig. 5
GRÁFICO DO TRÁFEGO DE REDE COM ATAQUE DE INUNDAÇÃO SYN.

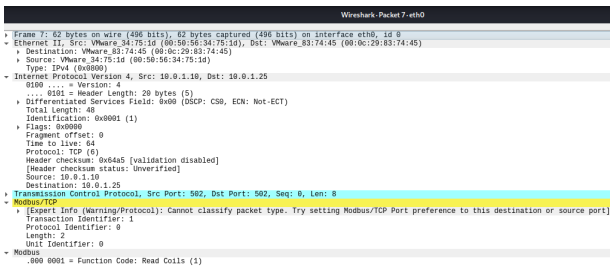

Fig. 6
CAPTURA PACOTE MODBUS ENVIADO PELO HOMEM DO MEIO.

consumo da rede. É importante acentuar que a Figura 4 indica a unidade em bytes, distinguindo-se da Figura 5 cuja unidade é quilobytes - equivalente a 1024 bytes -, evidenciando a diferença entre os dois gráficos e o êxito do ataque.

2) ***Homem no Meio****:* Na ocorrência deste ataque, o *script* efetuado pelo invasor desempenhou o homem do meio interceptando mensagens de comando e controle entre o MTU e o RTU. No cenário realizado neste experimento, o atacante deseja disfarçar-se como mestre e forjar solicitações para o escravo. Inicialmente, utiliza-se da função *sniff* do *Scapy* cuja finalidade é capturar pacotes, permitindo realizar tais capturas por meio de filtros para deter apenas determinados tipos de pacotes. Deste modo, foi feito o uso desta função com filtragem das mensagens destinadas a Porta 502 - correspondente ao protocolo Modbus TCP, como mencionado. Após a captura das mensagens anteriores, o atacante apodera-se de dados como IP de origem e de destino, e, mediante estas informações, envia uma nova mensagem Modbus TCP contendo o endereço do mestre (origem) e o do escravo (destino). Todavia, o atacante mantém o seu endereço de Controle de Acesso à Mídia (MAC - *Media Access Control*), alterando apenas o endereço IP para o do mestre, intencionando passar-se por ele.

A Figura 6 mostra uma captura de tela de um pacote capturado pelo programa *Wireshark* na MTU. É possível observar no quadro *Internet Protocol Version 4* que o campo *source* (endereço de origem) apresenta o IP do escravo e o campo *destination* (endereço de destino) compreende ao IP do mestre. De igual modo, constata-se que no quadro *Ethernet II* no *destination* está contido o MAC do dispositivo invasor e no *source* o do escravo, conjecturando a viabilidade de realizar tal ataque nos sistemas SCADA.

3) ***Ataque de Reflexão****:* A implementação desse ataque ocorre similarmente ao Homem do Meio, conforme emprega-se a função *sniff* com intuito de filtrar na rede mensagens

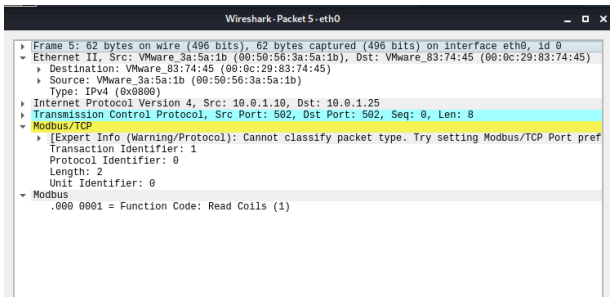

Fig. 7
CAPTURA PACOTE MODBUS DO ATAQUE DE REFLEXÃO.

destinadas também à porta 502. Com base nas capturas filtradas, o invasor obtém não apenas endereços IPs contidos no pacote, mas apropria-se ainda do MAC de origem e de destino. Subsequentemente, o atacante envia um pacote Modbus TCP para o *host* escravo, e diferente do ataque do homem do meio - que adultera apenas os campos que contém endereços IPs -, é posto no campo *source* do pacote o MAC de origem do mestre oriundo da captura. O intuito é que o escravo destine a resposta desta mensagem ao MTU. À vista disto, caso seja bem-sucedido, múltiplas mensagens provindas do atacante com destino ao escravo serão lançadas para que este replique ao mestre, ocorrendo uma inundação em ambos que prejudicará - ou mesmo esgotará - os recursos de disponibilidade da rede, além de acometer a integridade e confiabilidade do sistema.

Na captura de tela presente na Figura 7 é demonstrado que o campo *source* do quadro *Internet Protocol Version 4* exibe o IP do mestre e o campo *destination* retrata o IP do escravo. Observa-se também que no quadro *Ethernet II* o campo *source* contém o MAC do mestre e o *destination* apresenta o MAC do escravo, inferindo assim o sucesso do ataque neste cenário.

V. CONCLUSÕES

A *smart grid* oferta inúmeros benefícios para a indústria, assim decorrentemente, para a sociedade atual, e para esse fim, é essencial garantir a proteção de seus componentes vitais. De acordo com as vulnerabilidades dissertadas e dos testes efetuados através da implementação autoral do protocolo Modbus TCP e dos ataques realizados, é notório o quão os sistemas SCADA estão expostos a diversos problemas de cibersegurança. Mediante os resultados obtidos pelos experimentos, infere-se que ataques cibernéticos deliberadamente visando a sabotagem - como do homem do meio, o de Inundação SYN e o ataque de reflexão - permitem a influência e comprometimento de operações outrora seguras e confiáveis do SCADA. Tais experimentos demonstram como os invasores podem prejudicar e/ou interromper o sistema, ocasionando diversos insupríveis danos.

Considerando a significativa importância da segurança cibernética em *smart grids*, visamos progredir os estudos nesta área em questão a fim de explorar demais fraquezas eminentes no SCADA e em seus protocolos de comunicação, bem como possíveis soluções para mitigação de tais vulnerabilidades.

REFERÊNCIAS

[1] C. Sun, A. Hahn e C. Liu, *"Cyber security of a power grid: State-of-the-art"*, *International Journal of Electrical Power & Energy Systems*, v. 99, pp. 45-56, Julho 2018.

[2] A. Tesfahun e L. Bhaskari, *"A SCADA testbed for investigating cyber security vulnerabilities in critical infrastructures"*, *Automatic Control and Computer Sciences*, v. 50, pp 54-62, Abril 2016.

[3] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi e H. E. Ghazi, *"Cyber-security in smart grid: Survey and challenges"*, *Computers & Electrical Engineering*, v. 67, pp. 469-482, Abril 2018.

[4] Z. Drias, A. Serhrouchni e O. Vogel, *"Analysis of Cyber Security for Industrial Control Systems"*, *International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pp. 1-8, Agosto 2015.

[5] X. Huang, Z. Qin e H. Liu, *"A Survey on Power Grid Cyber Security: From Component-Wise Vulnerability Assessment to System-Wide Impact Analysis"*, *IEEE Access*, v. 6, pp. 69023-69035, 2018

[6] *MODBUS Protocol Specification*, Disponível em: <http://www.modbus.org/specs.php>, Acesso em: 20 de Abril, 2020.

[7] C. Liu, G. Xiong, J. Liu e G. Gou, *"Detect The Reflection Amplification Attack Based On Udp Protocol"*, *10th International Conference on Communications and Networking in China (ChinaCom)*, pp. 260-265, Agosto 2015.

[8] Y. Yang et al., *"Man-in-the-middle Attack Test-bed Investigating Cyber-security Vulnerabilities In Smart Grid Scada Systems"*, *International Conference on Sustainable Power Generation and Supply (SUPERGEN)*, pp. 1-8, 2012.

[9] *Scapy's documentation*, Disponível em: <https://scapy.readthedocs.io/>, Acesso em: 20 de Abril, 2020.

[10] Z. Ahmad e M. H. Durad, *"Development of SCADA Simulator using Omnet++"*, *16th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, pp. 676-680, Janeiro 2019.

[11] A. Lu e H. Yang, *"False data injection attacks against state estimation in the presence of sensor failures"*, *Information Sciences 508*, pp. 92-104, 2020.

[12] C. Roberts et al., *"Learning Behavior of Distribution System Discrete Control Devices for Cyber-Physical Security"*, *IEEE Transactions on Smart Grid 11.1*, pp. 749-761, 2020.

[13] F. Sicard, E. Zamai e J. Flaus, *"An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems"*, *Reliability Engineering System Safety 188*, pp. 584–603, 2019.

[14] P. I. Radoglou-Grammatikis e P. G. Sarigiannidis, *"Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems"*, *IEEE Access 7*, pp. 46595–46620, 2019.

[15] E. Irmak e İ. Erkek, *"An overview of cyber-attack vectors on SCADA systems"*, *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pp. 1-5, Maio 2018.