UNIVERSIDADE FEDERAL FLUMINENSE

ARTHUR ALBUQUERQUE ZOPELLARO SOARES

3AS: Autenticação, Autorização e Auditoria para Smart Grids

NITERÓI

2019

UNIVERSIDADE FEDERAL FLUMINENSE

ARTHUR ALBUQUERQUE ZOPELLARO SOARES

3AS: Autenticação, Autorização e Auditoria para Smart Grids

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Computação. Área de concentração: Sistemas de Computação.

Orientadoras:
Débora Christina Muchaluat Saade
Natalia Castro Fernandes
Yona Lopes

NITERÓI

2019

Ficha catalográfica - SDC/BEE
Gerada com informações fornecidas pelo autor

S676 Soares, Arthur Albuquerque Zopellaro
3AS : autenticação, autorização e auditoria para Smart Grids / Arthur Albuquerque Zopellaro Soares ; Débora Christina Muchaluat Saade, orientadora ; Natalia Castro Fernandes, orientadora ; Yona Lopes, orientadora. Niterói, 2019.
79 f.

Dissertação (mestrado)-Universidade Federal Fluminense, Niterói, 2019.

DOI:
http://dx.doi.org/10.22409/PGC.2019.m.12803771780

1. Rede elétrica inteligente. 2. Rede definida por software. 3. Segurança da informação. 4. Auditoria de sistemas. 5. Produção intelectual. I. Saade, Débora Christina Muchaluat, orientadora. II. Fernandes, Natalia Castro, orientadora. III. Lopes, Yona, orientadora. IV. Universidade Federal Fluminense. Instituto de Computação. V. Título.

CDD -

Bibliotecária responsável: Rosiane Pedro do Nascimento - CRB7/6237

ARTHUR ALBUQUERQUE ZOPELLARO SOARES

3AS: Autenticação, Autorização e Auditoria para *Smart Grids*

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Computação. Área de concentração: Sistemas de Computação.

Aprovada em agosto de 2019.

BANCA EXAMINADORA

Prof^{a}. Débora Christina Muchaluat Saade, D.Sc. – Orientadora, UFF

Prof^{a}. Natalia Castro Fernandes, D.Sc. – Orientadora, UFF

Prof^{a}. Yona Lopes, D.Sc. – Orientadora, UFF

Prof. Igor Monteiro Moraes, D.Sc. – UFF

Prof. José Ferreira de Rezende, D.Sc. – UFRJ

Niterói

2019

À Christianne, Lucas, Noah e William.

Agradecimentos

Agradeço aos meus pais William e Christianne, ao meu irmão Lucas, e ao meu cachorro Noah, por me incentivarem a seguir no que acredito e por representarem um porto seguro nos momentos em que as coisas parecem difíceis.

Agradeço a Deus pelas oportunidades que tive durante toda minha vida, e pela coragem para enfrentar novos desafios. Agradeço também pelas pessoas que colocou em minha vida, sendo cada uma peça chave para me tornar a pessoa que sou hoje.

Ao meu amigo Lauro por ter me incentivado a entrar no meio acadêmico. Hoje não me vejo trabalhando em outra área.

Agradeço especialmente às minhas orientadoras, Débora, Natalia e Yona pelos ensinamentos durante minha pesquisa e por acreditarem em meu potencial.

Agradeço aos meus amigos da UFF e do laboratório MídiaCom, pelos momentos de descontração e pelo apoio.

Agradeço à banca pelos comentários enriquecedores.

Agradeço também aos órgãos de fomento à pesquisa FAPERJ, FAPESP, CAPES e CNPq, e à empresa TAESA e ao programa de P&D ANEEL (PD-07130-0053/2018), pelos recursos financeiros recebidos.

Resumo

A rede elétrica inteligente, ou *smart grid*, surge da necessidade de melhoria da rede elétrica tradicional, possibilitando, dentre outras características, o monitoramento e controle da rede elétrica com o auxílio de redes de comunicação e tecnologia da informação, conforme a norma IEC 61850. Apesar dos benefícios apresentados pela introdução de uma rede de comunicação, novas vulnerabilidades são também incorporadas à rede elétrica inteligente. A gestão de identidade pode ser definida como um conjunto de métodos que fornecem um nível adequado de segurança para os recursos de uma organização através de políticas impostas aos usuários, com foco nos requisitos de autenticação, autorização e auditoria. Esta dissertação propõe o 3AS - Autenticação, Autorização e Auditoria para *Smart Grids*. Esta proposta provê um mecanismo de autenticação baseado em IEEE 802.1X para os protocolos de comunicação especificados pela norma IEC 61850, propõe a utilização do controle de acesso baseado em atributos, e ainda propõe um sistema integrado de auditoria, registrando eventos de autenticação, autorização e utilização de recursos da rede de comunicação. Outros trabalhos encontrados na literatura atendem apenas a cenários específicos de redes elétricas inteligentes, enquanto o 3AS preocupa-se em atender a cenários diversos de redes elétricas inteligentes, desde a introdução de veículos elétricos na rede, até o sistema de teleproteção da rede elétrica. Através da utilização do controle de acesso baseado em atributos para a autorização, as políticas de acesso granulares permitem a criação de diferentes níveis de acesso, além de identificar erros de configuração nos dispositivos inteligentes. Por fim, diferente da maioria dos trabalhos, o 3AS propõe um modelo de autenticação e autorização integrado à auditoria, permitindo o registro de eventos da rede de forma centralizada. Através de experimentos emulados, foi constatado que o mecanismo de autenticação produz uma carga de controle de 4,65 KB, 48,84% menor do que o mecanismo proposto por outro trabalho. A autenticação também foi validada através de dois modelos de autenticação diferentes: EAP-PEAP, voltado para o cenários de veículos elétricos, e produz menor carga de controle; e EAP-TLS, voltado para o cenário de teleproteção, apresentando menor atraso. O processo de autorização demonstrou-se eficiente, bloqueando a comunicação de dispositivos não-autenticados ou não-autorizados, e permitindo a comunicação após a autorização bem sucedida.

Palavras-chave: Redes Elétricas Inteligentes, Redes Definidas por *Software*, IEC 61850, Autenticação, Autorização, Auditoria.

Abstract

The smart grid arises from the need to improve the traditional grid, enabling, among other features, the monitoring and control of the grid with the aid of communication networks and information technology, according to IEC 61850. Despite the benefits presented by the introduction of a communication network, this network also incorporates new vulnerabilities into the smart grid. Identity Management defines a set of methods that provide an adequate level of security for an organization's resources through policies imposed on users, focusing on authentication, authorization, and accounting requirements. This dissertation proposes the 3AS - Authentication, Authorization, and Accounting for Smart Grids. This proposal provides an IEEE 802.1X-based authentication mechanism for the communication protocols specified by IEC 61850, proposes the use of attribute-based access control, and proposes an integrated accounting system by logging resources usage, authentication, and authorization events. Other works found in the literature only address specific smart grid scenarios, while 3AS is concerned with meeting diverse smart grid scenarios, such as the introduction of electric vehicles to the grid, and teleprotection systems for the grid. Attribute-based access control for authorization provides granular access policies and enables the use of different levels of access, while also identifying configuration errors on smart devices. Finally, unlike most works, 3AS proposes an integrated authentication and authorization model for accounting, allowing centralized logging of network events. Emulated experiments show that the authentication mechanism produces a control load of 4.65 KB, 48.84% less than the mechanism proposed by another work. Authentication has also been validated through two different authentication models: EAP-PEAP, for electric vehicle scenarios, and produces less control overhead; and EAP-TLS, for teleprotection scenarios, showing less delay. The authorization process was shown efficient by blocking communication from unauthenticated or unauthorized devices and allowing communication only after successful authorization.

Keywords: Smart Grids, Software-Defined Networks, IEC 61850, Authentication, Authorization, Accounting.

Lista de Figuras

2.1 Diagrama de sequência demonstrando os eventos para autenticação através do protocolo 802.1X [23]. 10

2.2 Exemplo de controle de acesso baseado em atributos onde o sujeito Alice tenta enviar um pacote IP para o endereço 10.0.0.1.[1] 13

2.3 Cenário de redes elétricas inteligentes com comunicação horizontal (GOOSE e SV) e vertical (MMS). 14

2.4 Arquitetura Publicador/Assinante, onde o publicador envia a mensagem para um grupo *multicast* e os assinantes daquele grupo a recebem. 15

2.5 Exemplo de arquivo SCL de um IED que publica GOOSE para o endereço 01:0C:CD:**01**:00:01 (GSE) e SV para o endereço 01:0C:CD:**04**:00:01 (SMV). 15

2.6 Um cliente, sistema supervisório, requisitando o serviço MMS de identificação para um servidor, IED, através de uma conexão TCP. 16

2.7 Arquitetura da rede definida por *software* dividida em plano de dados, plano de controle e plano de aplicação. 19

2.8 Arquitetura ARES. 20

4.1 Componentes da arquitetura do 3AS. 29

4.2 Processo de autenticação aceito através do nó de autenticação do 3AS. . . 31

4.3 Processo de autenticação negada através do nó de autenticação do 3AS. . . 32

4.4 Processo de autorização aceita através do controle de acesso do 3AS. 33

4.5 Processo de autorização negada através do controle de acesso do 3AS. . . . 34

4.6 Processo de autorização de instalação de fluxos para controle de acesso reativo. 37

4.7 Processo de autorização de instalação de fluxos para controle de acesso proativo. 38

4.8 Processo de desconexão de IEDs. 38

4.9 Processo de registro do estado da rede elétrica inteligente. 40

4.10 Técnica de ARP *poisoning* [24]. 41

5.1 Topologia dos experimentos contendo o SCADA-NG e Nó de Autenticação conectados a um comutador SDN e um número variável de IEDs conectados a outro comutador SDN. 44

5.2 Topologia do primeiro cenário onde um veículo elétrico autentica-se na rede de comunicação através de usuário e senha para solicitar a recarga de sua bateria. 45

5.3 Sequência de eventos para o processo de autenticação e comunicação MMS. O mecanismo gera tráfego OpenFlow no início para instalar as regras de fluxos para permitir a autenticação IEEE 802.1X. A comunicação MMS inicia somente após o término do processo de autenticação[2]. 46

5.4 Topologia do segundo cenário onde veículos elétricos autenticam-se na rede de comunicação através de usuário e senha. O número de veículos elétricos autenticando-se ao mesmo tempo é alternado para avaliar a progressão da latência do mecanismo de autenticação. 47

5.5 Experimentos para validação da eficiência do mecanismo de autenticação. . 47

5.6 Comparação da carga de controle gerada entre a autenticação por IEEE 802.1X e *Captive Portal*. 49

5.7 Topologia do terceiro cenário onde veículos elétricos autenticam-se na rede de comunicação através de usuário e senha e dispositivos de proteção autenticam-se através de certificados. 50

5.8 Comparação entre a utilização de credencial e certificado. 50

5.9 Sequência de eventos para a autenticação por credencial (EAP-PEAP). . . 51

5.10 Sequência de eventos para a autenticação por certificado (EAP-TLS). . . . 52

5.11 Topologia do quarto cenário onde dispositivos de proteção autenticam-se na rede de comunicação através de certificados e o dispositivo 1 publica quadros GOOSE para o dispositivo 2. 53

5.12 Comparação entre o atraso gerado pela autorização proativa e autorização reativa. 53

5.13 IED2 recebe os quadros GOOSE apenas após ser devidamente autenticado e autorizado. 54

5.14 Sequência de eventos para a autorização através da API ARES e do protocolo MMS. 55

5.15 Registro de eventos gerados pelo 3AS para o experimento descrito. 56

Lista de Tabelas

2.1 Comparação entre os modelos de autenticação EAP, baseado em [23]. . . . 9

2.2 Exemplo de políticas baseadas em lista (ACL). 11

2.3 Exemplo de políticas baseadas em papéis (RBAC). Alice e Bob possuem o papel de Auditor. 11

2.4 Exemplo de políticas baseadas em atributos (ABAC). O sujeito Bob possui uma autorização especial que permite criar usuários caso esteja acessando a rede local. 12

3.1 Relação das pesquisas sobre AAA para Redes Elétricas Inteligentes. 27

Lista de Abreviaturas e Siglas

3AS Autenticação, Autorização e Auditoria para *Smart Grids* 3

AA Autenticação e Autorização 22

AAA Autenticação, Autorização e Auditoria 3

ABAC *Attribute-Based Access Control* 10

ACL *Access Control List* 10

AES *Advanced Encryption Standard* 22

API *Application Programming Interface* 18

ARES *Autonomic and Resilient communication framEwork for Smart grids* . . 2

ARP *Address Resolution Protocol* 41

EAP *Extensible Authentication Protocol* 7

EAP-MD5 EAP *Message-Digest algorithm 5* 8

EAP-PEAP *Protected* EAP 8

EAP-TLS EAP *Transport Layer Security* 8

EAP-TTLS EAP *Tunneled* TLS 8

EAPoL *Extensible Authentication Protocol over LAN* 7

GOOSE *Generic Object Oriented Substation Events* 2

IED *Intelligent Electronic Device* 1

IEC *International Electrotechnical Commission* 1

IP *Internet Protocol* 7

IPsec *IP Security* 23

LAN *Local Area Network* 7

LBAC *Lattice-Based Access Control* 23

LTE *Long-Term Evolution* 23

MAC *Medium Access Control* 9

MMS *Manufacturing Message Specification* 1

NDN *Named Data Networking* 24

OSI *Open Systems Interconnection* 16

OTP *One-Time Password* 24

OTS *One-Time Signature* 22

PDP *Policy Decision Point* 12

PEP *Policy Enforcement Point* 12

MSCHAPv2 *Microsoft's Challenge-Handshake Authentication Protocol* versão 2 8

PRP *Policy Retrieval Point* 12

RADIUS *Remote Authentication Dial In User Service* 8

RBAC *Role-Based Access Control* 10

REST *Representational State Transfer* 44

RSA *Rivest–Shamir–Adleman* 22

SASL *Simple Authentication and Security Layer* 23

SCADA *Supervisory Control and Data Acquisition* 20

SCADA-NG *Supervisory Control and Data Acquisition* de Nova Geração 21

SDN *Software-Defined Network* 2

SCL *Substation Configuration Language* 15

SV *Sampled Values* 2

TCP/IP *Transmission Control Protocol/Internet Protocol* 16

TLS *Transport Layer Security* 8

WiMAX *Worldwide Interoperability for Microwave Access* 25

XML *Extensible Markup Language* 15

XMPP *eXtensible Messaging and Presence Protocol* 23

Sumário

1 Introdução **1**

1.1 Objetivos 3

1.2 Contribuições 3

1.3 Organização do Texto 4

2 Redes Elétricas Inteligentes e Gestão de Identidade **5**

2.1 Segurança da Informação em Redes Elétricas Inteligentes 5

2.2 Gestão de Identidade 7

2.2.1 Autenticação 7

2.2.2 Autorização 10

2.2.3 Auditoria 12

2.3 Comunicação na Rede Elétrica Inteligente 13

2.3.1 Comunicação Horizontal 14

2.3.2 Comunicação Vertical 16

2.3.3 Cenários de Redes Elétricas Inteligentes 17

2.4 Redes Definidas por *Software* 18

2.4.1 ARES 19

3 Trabalhos Relacionados **22**

3.1 Autenticação 22

3.2 Autenticação e Autorização 23

3.3 Autenticação, Autorização e Auditoria 25

4 Proposta do 3AS **28**

4.1 Requisitos para implantação do 3AS 30

4.2 Módulo de Autenticação 30

4.3 Módulo de Autorização 31

4.4 Controlador SDN baseado no ARES 35

4.5 SCADA *Next Generation* 39

4.6 Modelo de Atacante 40

5 Análise do 3AS **43**

5.1 Ambiente de Testes 43

5.2 Experimentos 45

5.2.1 Autenticação: Comportamento 45

5.2.2 Autenticação: Carga de Controle e Latência 46

5.2.3 Autenticação: Comparação 48

5.2.4 Autenticação: Credenciais 49

5.2.5 Autorização: Proativa x Reativa 52

5.2.6 Autorização e Auditoria: Comportamento 54

6 Conclusão **57**

6.1 Trabalhos futuros 58

Referências **60**

Capítulo 1

Introdução

A rede elétrica inteligente, ou *smart grid*, surge da necessidade de melhoria da rede elétrica tradicional, possibilitando, dentre outras características, o monitoramento e controle da rede elétrica em tempo real [12]. Outras características compreendem desde mecanismos de qualidade de energia até a implantação de serviços autônomos para garantir a recuperação e resiliência do sistema elétrico [30]. Entretanto, novos pontos de vulnerabilidade são inseridos no sistema elétrico pela expansão da rede de comunicação [37].

Para aprimorar a escalabilidade e confiabilidade da rede elétrica inteligente, o comitê técnico 57 do *International Electrotechnical Commission* (IEC) desenvolveu a norma IEC 61850 [16] padronizando a comunicação para automação do sistema elétrico, desde a padronização para subestações, parte 6 da norma IEC 61850 [20], até a padronização para veículos elétricos, parte 90-8 da norma IEC 61850 [21]. Essa norma padroniza a modelagem dos dados de dispositivos inteligentes, além de definir os protocolos de comunicação a serem utilizados por eles. *Intelligent Electronic Device*s (IEDs) são dispositivos inteligentes com uma ou mais funcionalidades específicas, por exemplo: obtenção de medições do consumo elétrico; recarga de bateria elétrica; ou até mesmo atuação de maneira autônoma para a teleproteção da rede elétrica. Os IEDs podem ser controlados remotamente por um dispositivo ou sistema de controle e supervisão. A modelagem dos dados padronizada pela norma facilita a configuração de IEDs de diferentes fabricantes além de permitir a interoperabilidade entre eles.

A comunicação, segundo a norma IEC 61850, pode ser categorizada de duas maneiras: comunicação vertical e comunicação horizontal. A comunicação vertical descreve a comunicação entre o sistema supervisório e os IEDs através do protocolo *Manufacturing Message Specification* (MMS). O sistema supervisório é responsável por monitorar e controlar os IEDs da rede utilizando serviços, como os de leitura e escrita, providos pelo MMS.

A comunicação horizontal é caracterizada pela troca de informações entre os dispositivos da rede elétrica sem a intervenção de um sistema supervisório. São utilizados dois protocolos, o *Generic Object Oriented Substation Events* (GOOSE) e o *Sampled Values* (SV). O protocolo GOOSE é responsável pela comunicação de informações de urgência entre IEDs, enquanto o protocolo SV é responsável pelo envio de valores amostrados tanto de corrente quanto de tensão para os IEDs.

A rede elétrica inteligente geralmente tem suas funcionalidades de comunicação, como encaminhamento de pacotes, definidas durante a fase de projeto [10], o que dificulta e encarece a mudança do estado da rede em tempo real. Com a introdução de veículos elétricos[1], é necessária uma tecnologia de comunicação que permita a gerência da rede elétrica inteligente de maneira dinâmica. A rede definida por *software*, ou *Software-Defined Network* (SDN), apresenta-se como uma solução facilitadora para cenários como o da rede elétrica inteligente [11, 10, 27, 33, 46]. Neste sentido, o *Autonomic and Resilient communication framEwork for Smart grids* (ARES) [30], um arcabouço para redes elétricas inteligentes baseado em redes definidas por *software* e na norma IEC 61850, foi desenvolvido com foco na autonomia das configurações da rede de comunicação, respeitando características como resiliência da rede elétrica inteligente, qualidade de serviço dos protocolos de comunicação e cooperação entre o sistema supervisório e o controlador SDN. O controlador SDN é responsável por gerenciar os comutadores da rede de comunicação, possibilitando a reconfiguração em tempo real da rede elétrica inteligente conforme a necessidade.

O ARES aponta a necessidade da implementação de mecanismos de segurança para comunicação na rede elétrica inteligente, entretanto, eles não foram detalhados em sua primeira especificação [30]. Requisitos de segurança como autenticação, autorização, e auditoria[2] devem ser levados em consideração para nortear a confiabilidade da rede elétrica inteligente, mitigando assim vulnerabilidades e possíveis ataques ao sistema elétrico, como o controle indevido de IEDs [40], a obtenção de informações privadas [52], ou até mesmo a não-rastreabilidade de uma tentativa de ataque cibernético [50].

[1] "Em 2030 o número de veículos que podem ser abastecidos na tomada pode chegar a 125 milhões", segundo a Agência Internacional de Energia – Notícia retirada do site: g1.globo.com/jornal-nacional/noticia/2018/07/dutra-tem-postos-de-recarga-para-carros-eletricos-entre-sao-paulo-e-rio.html. Acesso em: jun. 2019

[2] O termo auditoria será utilizado nesta dissertação como sinônimo de responsabilização.

1.1 Objetivos

A gestão de identidade pode ser alcançada através da implementação de um, ou mais, mecanismos que respeitem os requisitos de autenticação, autorização e auditoria. Esta dissertação tem como objetivo realizar um estudo e uma proposta de mecanismos para redução de vulnerabilidades na comunicação de redes elétricas inteligentes. Ao integrar o sistema supervisório ao controle da rede de comunicação, é possível tratar a autenticação, autorização e auditoria, utilizando de forma eficiente os recursos de rede, além de permitir a reconfiguração em tempo real.

Esta dissertação propõe o Autenticação, Autorização e Auditoria para *Smart Grids* (3AS), estendendo o ARES com um componente de autenticação baseado na norma IEEE 802.1X [15], um controle de acesso baseado em atributos e um sistema integrado de auditoria. A proposta é avaliada através da implementação do 3AS no Ryu[3], um controlador SDN amplamente utilizado pelo meio acadêmico, e emulada em uma rede definida por *software* com comutadores virtuais.

Através do 3AS, é possível controlar de forma granular o acesso dos dispositivos à rede de comunicação, além de unificar as informações de tráfego na rede de comunicação para uma auditoria mais simples e confiável. Para isso, o 3AS visa tratar as vulnerabilidades relacionadas à Autenticação, Autorização e Auditoria (AAA):

- Bloqueando o acesso de dispositivos não identificados e/ou não autorizados à rede de comunicação;
- Permitindo o acesso apenas aos recursos necessários para cada dispositivo, considerando os protocolos de comunicação, os caminhos disponíveis e a localização dos demais dispositivos elétricos inteligentes;
- Facilitando a auditoria dos eventos da rede através de um mecanismo integrado.

1.2 Contribuições

Como principais contribuições desta dissertação, tem-se o avanço do estado da arte envolvendo segurança da informação e gestão de identidade para redes elétricas inteligentes. A proposta do 3AS é uma extensão do *framework* ARES com componentes de segurança

[3]Disponível em osrg.github.io/ryu.

para AAA. A implementação parcial em código aberto do ARES no controlador SDN Ryu além da implementação do 3AS também são contribuições do trabalho.

Outras contribuições secundárias são a criação de *scripts* para automatização de experimentos com o controlador Ryu e o emulador de redes Mininet[4], a criação de geradores de quadros GOOSE e pacotes MMS para a emulação do sistema supervisório e comunicação entre IEDs com objetivo de avaliar o 3AS.

1.3 Organização do Texto

O restante desta dissertação está estruturada em seis capítulos, sendo o Capítulo 2 a base teórica necessária para discussão da proposta apresentada neste trabalho. O principal tema desse capítulo são os conceitos de segurança da informação para redes elétricas inteligentes e a gestão de identidade, além de discorrer sobre os protocolos de comunicação e o arcabouço ARES, um arcabouço para redes elétricas inteligentes baseado em redes definidas por *software*.

O Capítulo 3 apresenta trabalhos relacionados que se propõem a estudar os problemas de segurança para redes elétricas inteligentes apontados no Capítulo 2, além de compará-los à proposta apresentada nesta dissertação. Esse capítulo se divide em duas seções: (1) gestão de identidade para redes elétricas inteligentes; e (2) gestão de identidade para redes definidas por *software*.

Em seguida, o Capítulo 4 apresenta a proposta 3AS, que oferece gestão de identidade para redes elétricas inteligentes baseadas no *framework* ARES. Através dos módulos do ARES, é possível implementar uma gerência mais dinâmica de ativos, além de possibilitar a reconfiguração da rede de comunicação em tempo real, atendendo à qualidade de serviço conforme necessário. É definida a arquitetura do 3AS e a integração de seus componentes com o ARES.

No Capítulo 5, é descrita a implementação do 3AS em um controlador amplamente utilizado e experimentos emulados são especificados com objetivo de validar a proposta. As ferramentas utilizadas para implementação e emulação são detalhadas, além de ser feita a análise dos principais resultados obtidos.

Por fim, o Capítulo 6 conclui a dissertação, revisitando os principais pontos discutidos no trabalho, destacando as principais contribuições e estabelecendo os trabalhos futuros.

[4]Disponível em bit.ly/3AS_ARES.

Capítulo 2

Redes Elétricas Inteligentes e Gestão de Identidade

A rede elétrica inteligente, ou *smart grid*, é um conceito que visa aprimorar a rede elétrica tradicional com o auxílio de redes de comunicação e tecnologia da informação. A rede de comunicação oferece diversas vantagens para a rede elétrica, como a incorporação de dispositivos inteligentes, ou *Intelligent Electronic Device* (IED), permitindo a obtenção de dados e controle desses dispositivos de maneira remota ou até autonômica. Além disso, a comunicação simplifica a construção de um mapa virtual da rede elétrica em tempo real, possibilitando a automação de subestações, a recuperação autonômica da rede elétrica após uma falta (*self-healing*), e o balanceamento de carga [12]. Outro benefício da rede elétrica inteligente é a possibilidade da comunicação bidirecional, como é o caso de veículos elétricos que podem atuar na rede de elétrica de duas maneiras diferentes: (1) recarga, quando o veículo tem sua bateria recarregada; ou (2) geração, quando o veículo fornece sua energia armazenada de volta para a rede elétrica. Sistemas complexos de proteção, como o caso dos veículos elétricos, onde o perfil da rede elétrica varia consideravelmente, são simplificados com a **teleproteção** [49], através do uso de uma rede de comunicação entre os IEDs.

2.1 Segurança da Informação em Redes Elétricas Inteligentes

Apesar dos benefícios apresentados pela introdução de uma rede de comunicação, novas vulnerabilidades são também incorporadas à rede elétrica inteligente. Assim como o

controle remoto dos IEDs facilita a manutenção da rede elétrica, atacantes[1] obtêm um novo meio de acesso indevido aos dispositivos da rede.

Para que uma rede elétrica inteligente seja considerada segura, essa deve adotar os seguintes requisitos de segurança [9, 29, 31, 37]:

- **Autenticação**, diz respeito à identificação de um dispositivo. A autenticação deve permitir que as ações de um dispositivo na rede sejam associadas a sua identidade. Em um sistema sem autenticação na rede elétrica inteligente, um atacante pode fazer com que seu veículo elétrico se passe por outro veículo para que a cobrança pelo consumo de energia seja enviada para outra pessoa.

- **Autorização**, diz respeito ao controle de acesso de dispositivos, autorizando ou não a utilização de objetos específicos. A autorização deve restringir o acesso do dispositivo aos recursos que esse está autorizado a utilizar. Em um sistema sem autorização na rede elétrica inteligente, um atacante pode enviar comandos indevidos aos IEDs de proteção para causar instabilidade no sistema elétrico.

- **Confidencialidade**, diz respeito ao sigilo das informações trafegadas na rede de comunicação. A confidencialidade deve codificar a informação de maneira que apenas os pares da comunicação consigam entender seu conteúdo. Em um sistema sem confidencialidade na rede elétrica inteligente, um atacante pode acessar as informações trafegadas na rede de comunicação para obter dados sigilosos.

- **Integridade**, diz respeito a legitimidade da mensagem na rede de comunicação. A integridade deve garantir que a mensagem não seja adulterada durante seu ciclo de vida. Em um sistema sem integridade na rede elétrica inteligente, um atacante pode, por exemplo, alterar os dados de uma mensagem para modificar os valores de cobranças;

- **Auditoria**, diz respeito à responsabilização das ações ocorridas na rede de comunicação. A auditoria deve permitir que, através de registros, todos os eventos da rede sejam rastreáveis, auxiliando na correção de erros ou até mesmo na identificação da origem de tentativas de ataques. Em um sistema sem auditoria na rede elétrica inteligente, um atacante pode efetuar qualquer ataque sem ser rastreado;

- **Não repúdio**, diz respeito à integridade dos eventos registrados pela auditoria. O não repúdio deve garantir que um evento ocorrido não possa ser desfeito. Em um

[1] Por atacante, entende-se a entidade maliciosa que visa a obtenção ilegal de dados confidenciais e/ou a modificação do comportamento padrão de um dispositivo ou sistema.

sistema da rede elétrica inteligente sem a garantia de não repúdio, um atacante pode modificar o registro dos eventos ocorridos na rede elétrica;

- **Disponibilidade**, diz respeito à alta disponibilidade de um dispositivo ou serviço do sistema elétrico. A disponibilidade deve garantir que a rede de comunicação esteja o maior tempo possível disponível para evitar perda financeira e até mesmo danos a equipamentos. Em um sistema da rede elétrica inteligente sem alta disponibilidade, um atacante pode efetuar um simples ataque de negação de serviço e causar grande instabilidade na rede de comunicação que apoia a rede elétrica.

Um sistema que atenda a todos esses requisitos deve ser planejado em etapas. Assim, esta dissertação propõe-se a avançar o estado da arte nos quesitos de autenticação, autorização e auditoria, conforme será explicado na Seção 2.2. Portanto, os demais requisitos não fazem parte do escopo desta dissertação e serão tratados em trabalhos futuros.

2.2 Gestão de Identidade

Segundo [4], a gestão de identidade pode ser definida como um conjunto de métodos que fornecem um nível adequado de segurança para os recursos de uma organização através de políticas impostas aos usuários, focando nos requisitos de autenticação, autorização e auditoria.

2.2.1 Autenticação

O processo de autenticação é responsável por identificar um dispositivo na rede de comunicação. Um dos padrões para autenticação é o IEEE 802.1X [15] que provê um mecanismo de para controle de acesso baseado em porta. Em resumo, o processo de autenticação é associado à porta física do comutador (*switch*). O protocolo IEEE 802.1X define o encapsulamento de quadros *Extensible Authentication Protocol* (EAP), um *framework* de autenticação, para *Local Area Network* (LAN), conhecido como *Extensible Authentication Protocol over LAN* (EAPoL).

O padrão IEEE 802.1X define o processo de autenticação sobre a camada de enlace, tornando o processo de autenticação independente da atribuição de endereços *Internet Protocol* (IP). Esse padrão apresenta três elementos importantes:

1. O suplicante: a entidade, dispositivo ou usuário, que deseja se conectar à rede de comunicação;

2. O servidor de autenticação: que verifica as credenciais do suplicante e toma a decisão final sobre a confirmação, ou não, da identificação do dispositivo; e

3. autenticador: um dispositivo que atua como uma ponte entre o suplicante e o servidor de autenticação, traduzindo os quadros de autenticação enviados pelo autenticador para o protocolo utilizado pelo servidor de autenticação.

O suplicante utiliza quadros EAPoL para se autenticar na rede de comunicação. O autenticador controla o acesso dos suplicantes à rede, permitindo ou bloqueando a comunicação, além de prover um enlace entre o suplicante e o servidor de autenticação. O autenticador recebe as credenciais, ou certificados, do suplicante através dos quadros EAPoL e os envia para o servidor de autenticação decidir o resultado da autenticação do suplicante. Uma forma comum de implementar a comunicação com servidor de autenticação é através do protocolo *Remote Authentication Dial In User Service* (RADIUS) [23, 36, 51, 35]. RADIUS é um protocolo de comunicação que provê autenticação e autorização de usuários em uma rede de comunicação.

O EAPoL, por ser um *framework*, permite a autenticação através de diferentes métodos, como: EAP *Message-Digest algorithm 5* (EAP-MD5), EAP *Transport Layer Security* (EAP-TLS), EAP *Tunneled* TLS (EAP-TTLS) e *Protected* EAP (EAP-PEAP) [23]. O método EAP-MD5 utiliza uma função para gerar um texto de tamanho fixo de acordo com uma entrada fornecida pelo usuário, entretanto o EAP-MD5 é considerado inseguro, portanto não é mais utilizado [47, 23]. O método EAP-TLS utiliza uma sessão *Transport Layer Security* (TLS) para validar os certificados do cliente e do servidor produzindo uma autenticação mútua entre o suplicante e o servidor de autenticação. O método EAP-TTLS também estabelece uma sessão TLS, mas em seguida faz a troca de credenciais (usuário e senha) entre o cliente e o servidor. O EAP-TTLS também faz a autenticação mútua. Por fim, o método EAP-PEAP igualmente utiliza uma sessão TLS, em seguida faz a troca de credenciais através de um outro método EAP, por exemplo o método PEAP-*Microsoft's Challenge-Handshake Authentication Protocol* versão 2 (MSCHAPv2). A Tabela 2.1 apresenta uma breve comparação entre os métodos de autenticação EAP-MD5, EAP-TLS, EAP-TTLS e EAP-PEAP [23].

Independente do método de autenticação utilizado, o suplicante encapsula as informações em um quadro *Ethernet* do tipo `0x888E` e envia para o autenticador através do

Tabela 2.1: Comparação entre os modelos de autenticação EAP, baseado em [23].

	EAP-MD5	**EAP-TLS**	**EAP-TTLS**	**EAP-PEAP**
Autenticação do suplicante	Senha *hash*	Certificado	Certificado, Credenciais	Certificado, Credenciais
Certificado do suplicante	Não	Necessário	Opcional	Opcional
Certificado do servidor	Não	Necessário	Necessário	Necessário
Autenticação mútua	Não	Sim	Sim	Sim

endereço de destino *Medium Access Control* (MAC) *multicast* `01:80:C2:00:00:03`. Dessa forma, o suplicante não precisa ter nenhum conhecimento prévio da rede de comunicação [36]. Já o autenticador passa a conhecer o endereço MAC do suplicante após receber o primeiro quadro de autenticação, enviando os quadros para o suplicante diretamente através do seu endereço *unicast*.

A Figura 2.1 apresenta uma sequência de eventos genérica para a autenticação utilizando o protocolo 802.1X. O suplicante inicia o processo de autenticação (1) enviando um quadro EAPOL ao autenticador. Em sequência, o autenticador solicita a identificação do suplicante (2) através de um quadro EAP. Após o suplicante informar sua identidade, o autenticador encapsula o quadro EAP em um pacote RADIUS-access (3) e repassa a requisição de autenticação para o servidor de autenticação. Posteriormente, o autenticador desencapsula o pacote RADIUS-access e envia um quadro EAP (4) solicitando as credenciais do suplicante. Em seguida, o suplicante responde à solicitação (5) e envia suas credenciais. Por fim, o servidor de autenticação informa ao suplicante se sua suas credenciais foram aceitas (6) ou não (7).

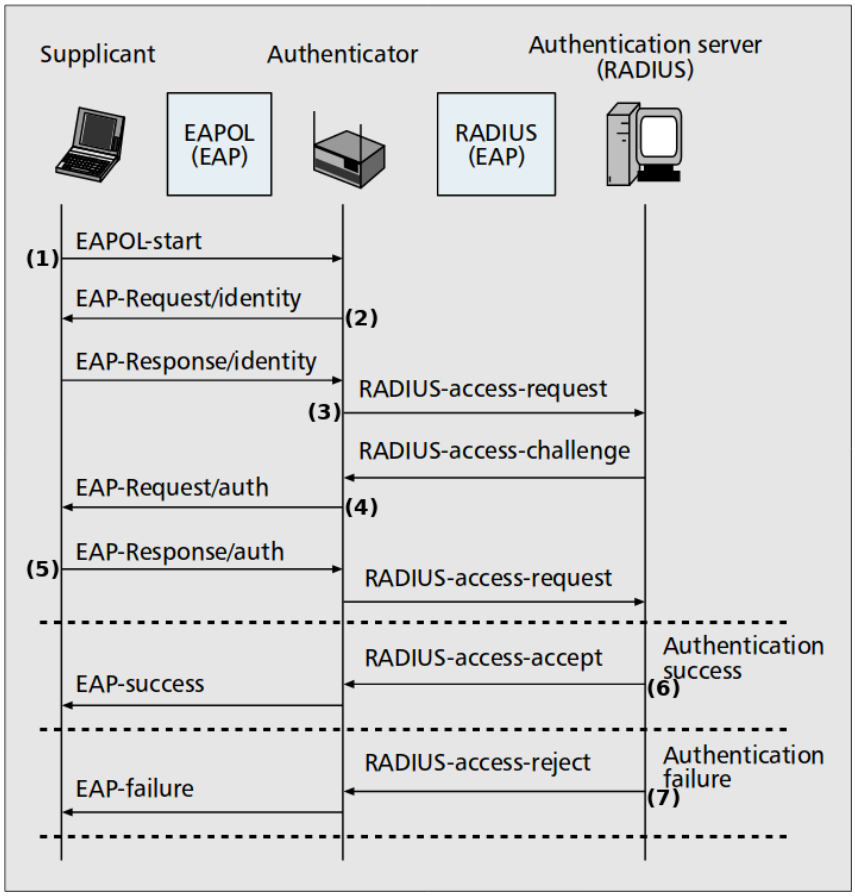


Figura 2.1: Diagrama de sequência demonstrando os eventos para autenticação através do protocolo 802.1X [23].

2.2.2 Autorização

O processo de autorização é iniciado após a confirmação da identidade do suplicante pelo processo de autenticação. A autorização é responsável por controlar as ações dos sujeitos, ou suplicantes, aos recursos da rede de comunicação. As ações podem ser: receber, ou enviar, mensagens com um determinado endereço IP ou MAC; os recursos podem ser alocados de acordo, por exemplo, com os protocolos de comunicação. Existem diversos modelos de controle de acesso para redes de comunicação, sendo os mais utilizados o *Access Control List* (ACL), o *Role-Based Access Control* (RBAC) e o *Attribute-Based Access Control* (ABAC) [7, 14, 45].

O controle de acesso baseado em listas, ou ACL, é um dos modelos de autorização mais simples. Uma nova política é criada para cada ação que cada identidade pode executar em cada recurso. O ACL apresenta um controle de acesso altamente granular, entretanto, não é um modelo escalável. A Tabela 2.2 apresenta um exemplo de políticas ACL onde os sujeitos Alice e Bob têm autorização apenas para ler as informações de usuários, mas

não têm acesso para criar, editar ou deletar usuários.

Tabela 2.2: Exemplo de políticas baseadas em lista (ACL).

Sujeito	**Ação**	**Recurso**	**Política**
Alice	Ler	Usuários	Permitir
Alice	Criar	Usuários	Negar
Alice	Editar	Usuários	Negar
Alice	Deletar	Usuários	Negar
Bob	Ler	Usuários	Permitir
Bob	Criar	Usuários	Negar
Bob	Editar	Usuários	Negar
Bob	Deletar	Usuários	Negar

O controle de acesso baseado em papel, ou RBAC, apresenta-se como uma evolução do ACL, onde é possível criar políticas mais genéricas que atendam a um grupo similar de sujeitos. Uma nova política é criada para cada ação que cada papel pode executar em cada recurso. O RBAC apresenta um controle de acesso menos granular e, diferente do ACL, é um modelo escalável. A Tabela 2.3 apresenta um exemplo de políticas RBAC onde o papel Auditor tem autorização apenas para ler as informações de usuários, mas não tem acesso para criar, editar ou deletar usuários. Posteriormente, esse papel pode ser associado aos sujeitos Alice e Bob.

Tabela 2.3: Exemplo de políticas baseadas em papéis (RBAC). Alice e Bob possuem o papel de Auditor.

Papel	**Ação**	**Recurso**	**Política**
Auditor	Ler	Usuários	Permitir
Auditor	Criar	Usuários	Negar
Auditor	Editar	Usuários	Negar
Auditor	Deletar	Usuários	Negar

O controle de acesso baseado em atributos, ou ABAC, apresenta-se como uma evolução do RBAC, onde é possível implementar políticas com estruturas condicionais. Uma nova política é criada para cada ação, informando através de condições, quais sujeitos e quais recursos podem ser utilizados. O ABAC também apresenta um controle de acesso altamente granular, mas diferente do ACL, é escalável; e diferente do RBAC, não é necessário criar um novo papel para atender a um situação específica. O ABAC permite a manutenção de casos especiais através da estrutura condicional de suas políticas, além de permitir regras baseadas em contexto, por exemplo, negar uma determinada ação feita de um endereço IP público, mas permitir caso seja solicitada através da rede local. A

Tabela 2.4 apresenta um exemplo de políticas ABAC onde Alice, Bob e Auditores têm autorização de leitura de usuários, mas não possuem acesso para criar, editar ou deletar usuários. Entretanto, Bob possui uma autorização especial que o permite criar usuários caso ele esteja acessando a rede local.

Tabela 2.4: Exemplo de políticas baseadas em atributos (ABAC). O sujeito Bob possui uma autorização especial que permite criar usuários caso esteja acessando a rede local.

Sujeito	**Ação**	**Recurso**	**Política**	**Contexto**
Alice ou Bob ou Auditor	Ler	Usuários	Permitir	
Alice ou Bob ou Auditor	Criar ou Editar ou Deletar	Usuários	Negar	
Bob	Criar	Usuários	Permitir	Solicitação Interna

O modelo ABAC apresenta quatro elementos importantes:

1. sujeito: a entidade que deseja requisitar o acesso a uma ação em um recurso, por exemplo um dispositivo;
2. *Policy Enforcement Point* (PEP): o módulo que garante a instituição das políticas;
3. *Policy Decision Point* (PDP): o módulo que permite, ou nega, o acesso do sujeito à ação no recurso;
4. *Policy Retrieval Point* (PRP): o módulo que possui as políticas de autorização.

A Figura 2.2 apresenta um exemplo de autorização ABAC onde o sujeito tenta enviar um pacote IP para o endereço 10.0.0.1, mas antes o PEP verifica se o sujeito tem a devida autorização.

2.2.3 Auditoria

O processo de manutenção da auditoria, ou da responsabilização, deve ocorrer constantemente em união com a autenticação, autorização e a utilização dos recursos da rede de comunicação. O registro dos eventos da rede de comunicação deve manter uma representação fiel das sequência de eventos ocorridos e associá-los aos sujeitos responsáveis. Essas informações devem ser armazenadas levando em consideração sua manutenção, uma vez que novas informações serão geradas constantemente.

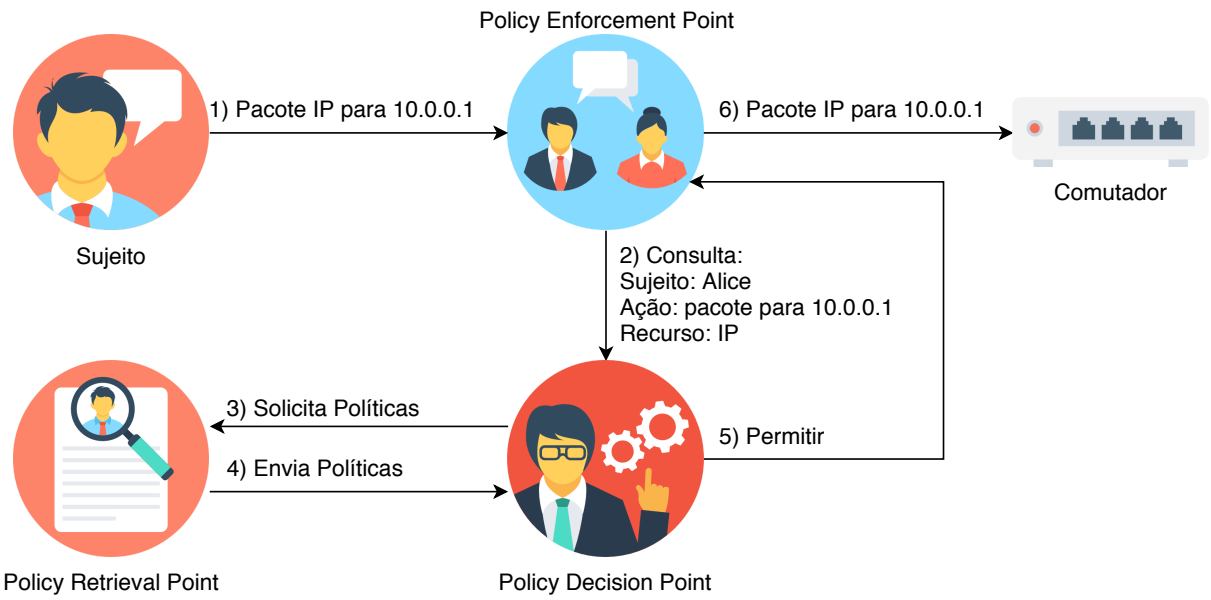


Figura 2.2: Exemplo de controle de acesso baseado em atributos onde o sujeito Alice tenta enviar um pacote IP para o endereço 10.0.0.1.[2]

Com base em [9], um registro para auditoria em redes elétricas inteligentes pode incluir: datas e horários; identidade do dispositivo, quando possível, a sua localização; registros das tentativas de acesso ao sistema aceitas e rejeitadas; registros das tentativas de acesso a outros recursos e dados aceitos e rejeitados; endereços e protocolos de rede; alarmes provocados pelo sistema de controle de acesso; e sistemas de detecção de intrusos.

2.3 Comunicação na Rede Elétrica Inteligente

A rede elétrica inteligente compreende uma complexa comunicação entre diversos dispositivos heterogêneos, apresentando padrões de comunicação com propósitos específicos. Esses dispositivos são denominados IEDs, dispositivos inteligentes capazes de obter medições da rede elétrica e atuarem de maneira autônoma em dispositivos de campo. Os IEDs podem ser controlados remotamente por um dispositivo ou sistema de controle e supervisão. Várias organizações que têm por objetivo o desenvolvimento de padrões nacionais e internacionais têm reunido esforços para se chegar a um conjunto de tecnologias, normas e padrões que definam o comportamento das redes elétricas inteligentes. Uma das principais propostas é a adoção da norma IEC 61850 [34]. A norma IEC 61850 [16], inicialmente criada para comunicação em subestações, foi estendida para englobar a automação do sistema de energia como um todo. Em 2016, foi lançada a parte 90–8 [21]

[2]Os ícones utilizados nas figuras desta dissertação são de *Vectors Market*. Disponível em flaticon.com/authors/vectors-market.

para padronização de veículos elétricos e segue sendo estendida e atualizada. A norma IEC 61850 tornou-se muito popular na área de engenharia de sistemas de potência, abordando aspectos vitais para a comunicação no sistema de energia [48]. De fato, existe um esforço para incentivar sua utilização também em *microgrids* e não somente em subestações, pavimentando o caminho para redes elétricas inteligentes ao fazer integrações entre sistemas de monitoramento, proteção, medição e controle [30].

A norma IEC 61850 [16] define a utilização de três protocolos de comunicação para a atender às necessidades específicas: (1) *Generic Object Oriented Substation Events* (GOOSE), para a comunicação entre IEDs; (2) *Sampled Values* (SV), para a transmissão de valores amostrados por transformadores para os IEDs; e (3) *Manufacturing Message Specification* (MMS), para a comunicação entre sistema supervisório e IED. A comunicação envolvendo os protocolos GOOSE e SV é denominada comunicação horizontal, enquanto a comunicação envolvendo o protocolo MMS é denominada comunicação vertical como pode ser visto na Figura 2.3, e será melhor explicado nas subseções a seguir.

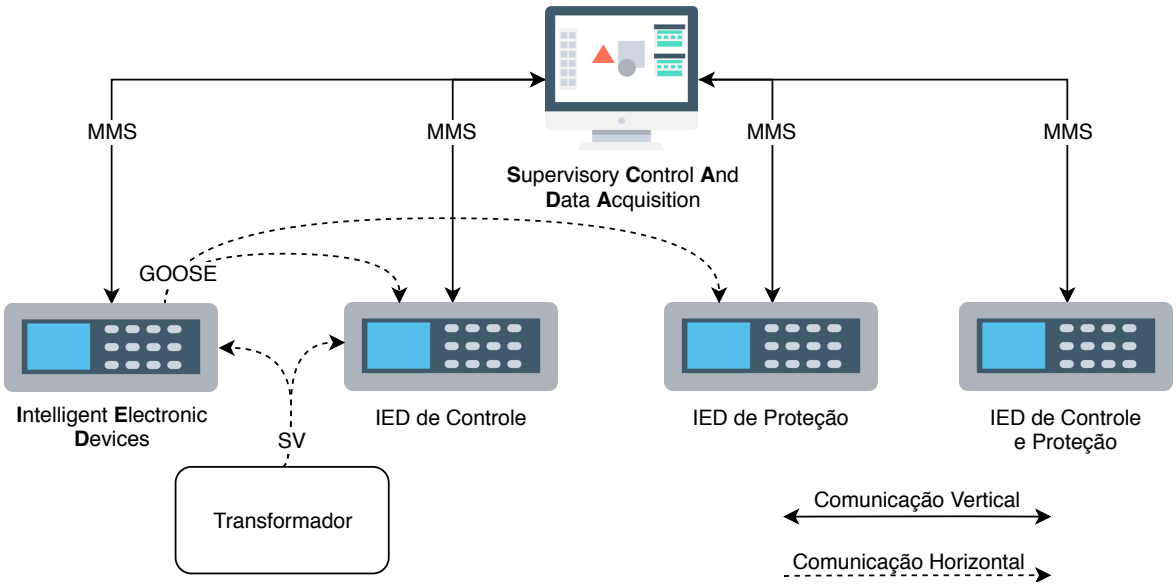


Figura 2.3: Cenário de redes elétricas inteligentes com comunicação horizontal (GOOSE e SV) e vertical (MMS).

2.3.1 Comunicação Horizontal

A comunicação horizontal especifica o envio de mensagens entre os dispositivos da rede sem a intervenção do sistema supervisório. Essa comunicação é destinada a mensagens críticas com restrições temporais tão rígidas quanto 3 milissegundos. Para evitar o atraso gerado pela camada de rede e transporte, a norma IEC 61850 define a utilização dos

protocolos GOOSE e SV diretamente sobre a camada de enlace.

O protocolo SV é utilizado para o envio de valores amostrados de tensão e corrente. Ambos os protocolos, GOOSE e SV funcionam através da arquitetura publicador/assinante como pode ser visto na Figura 2.4.

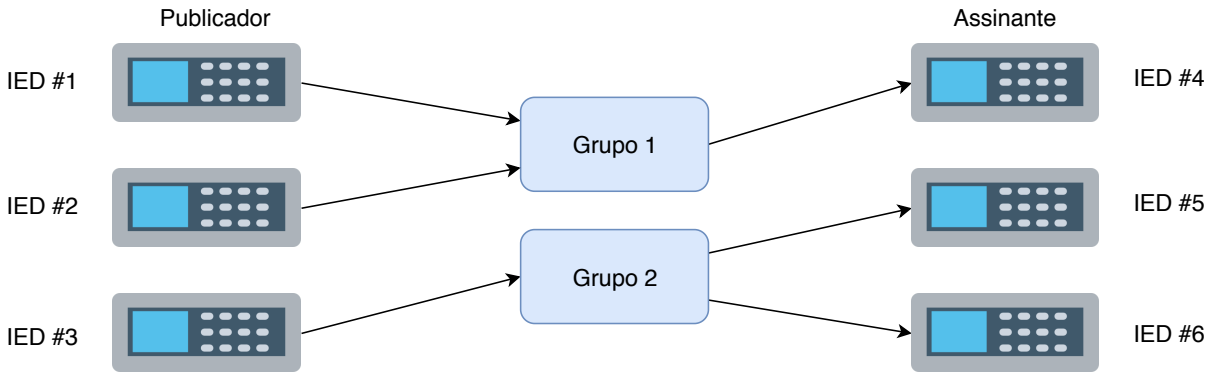


Figura 2.4: Arquitetura Publicador/Assinante, onde o publicador envia a mensagem para um grupo *multicast* e os assinantes daquele grupo a recebem.

O IED que deseja receber quadros de um determinado grupo é denominado assinante. Já o IED que deseja enviar quadros é denominado publicador. Caso o quadro seja uma mensagem GOOSE, o destino deve ser um endereço *multicast* entre os valores 01:0C:CD:**01**:00:00 e 01:0C:CD:**01**:01:FF [18]. Caso o quadro seja uma mensagem SV, o destino pode ser um endereço *unicast*, ou um endereço *multicast* entre os valores 01:0C:CD:**04**:00:00 e 01:0C:CD:**04**:01:FF [18].

A parte 6 da norma IEC 61850 [20] define a linguagem *Substation Configuration Language* (SCL) para configuração dos IEDs. O SCL é baseado em *Extensible Markup Language* (XML) e permite descrever os atributos do IED, seus valores, e até mesmo informações de comunicação. A Figura 2.5 apresenta um exemplo de um IED que foi modelado para publicar quadros GOOSE e SV.

```
<GSE ldInst="GenericIO" cbName="gcbAnalogValues">
    <Address>
        <P type="MAC-Address">01-0C-CD-01-00-01</P>
        <P type="APPID">1000</P>
        <P type="VLAN-ID">1</P>
        <P type="VLAN-PRIORITY">4</P>
    </Address>
</GSE>
<SMV ldInst="GenericIO" cbName="Volt">
    <Address>
        <P type="MAC-Address">01-0C-CD-04-00-01</P>
        <P type="APPID">4000</P>
        <P type="VLAN-ID">1</P>
        <P type="VLAN-PRIORITY">4</P>
    </Address>
</SMV>
```

Figura 2.5: Exemplo de arquivo SCL de um IED que publica GOOSE para o endereço 01:0C:CD:**01**:00:01 (GSE) e SV para o endereço 01:0C:CD:**04**:00:01 (SMV).

2.3.2 Comunicação Vertical

A comunicação vertical especifica a troca de mensagens entre o sistema supervisório e os IEDs. O sistema supervisório é responsável pela supervisão e gerência do sistema elétrico através da monitoração e controle dos IEDs. Essa comunicação se dá através do protocolo MMS [22], que é aplicada sobre o modelo *Transmission Control Protocol/Internet Protocol* (TCP/IP) ou sobre o modelo *Open Systems Interconnection* (OSI).

O MMS adota a arquitetura cliente-servidor, onde o sistema supervisório atua como cliente, requisitando serviços aos servidores IEDs conforme pode ser visto na Figura 2.6.

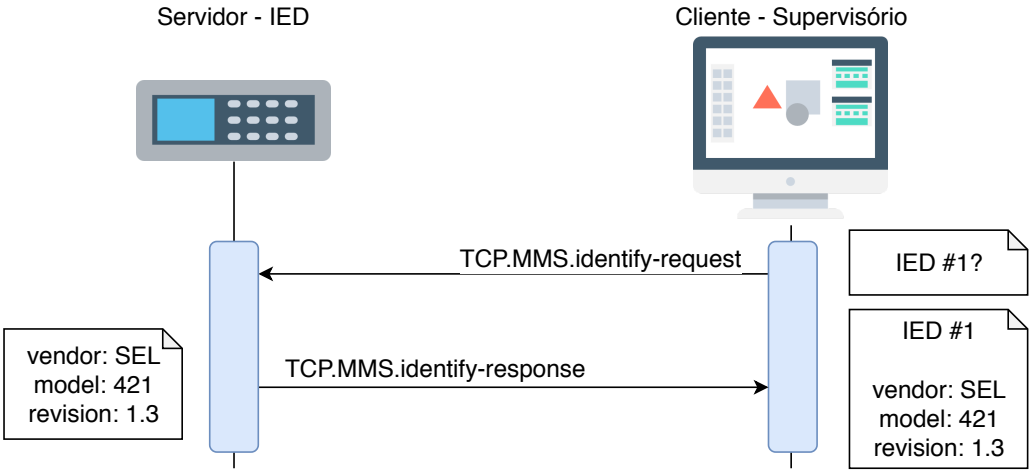


Figura 2.6: Um cliente, sistema supervisório, requisitando o serviço MMS de identificação para um servidor, IED, através de uma conexão TCP.

Os serviços básicos para entendimento do protocolo MMS são:

- `MMS.Identify`: é o serviço que permite ao sistema supervisório identificar as características do IED. Através desse serviço, o IED informa seu fabricante, modelo e versão;
- `MMS.Gets`: são os serviços que permitem ao IED se descrever para o sistema supervisório. Através desses serviços, o IED lista todos seus atributos. Ressalta-se que são passados os atributos contidos nos IEDs e não os seus valores;
- `MMS.Read`: é o serviço que permite ao sistema supervisório ler os valores dos atributos do IED (que já podem ter sido passados pelo serviço `MMS.Get`). Através desse serviço, o IED informa o valor do atributo solicitado;
- `MMS.Write`: é o serviço que permite ao sistema supervisório enviar um comando para IED. Através desse serviço, o sistema supervisório solicita a mudança do valor

de um atributo do IED, resultando na mudança de comportamento do mesmo;

- `MMS.Report`: é o serviço que permite ao IED informar de forma não solicitada uma mudança de valor dos seus atributos para o sistema supervisório. Através desse serviço, o IED informa o novo valor de seu atributo, sem a necessidade do sistema supervisório solicitar o novo valor através do `MMS.Read`.

Através dos serviços MMS, é possível obter todas as informações do IED. Por exemplo, o sistema supervisório poderia utilizar o serviço `MMS.Read` para descobrir qual o endereço *multicast* em que o IED da Figura 2.5 está enviando mensagens.

2.3.3 Cenários de Redes Elétricas Inteligentes

A rede elétrica inteligente engloba diversos cenários diferentes com características e requisitos distintos. Dois cenários notáveis, que recebem o foco desta dissertação, são o cenário de teleproteção de linhas de transmissão e o cenário de veículos elétricos, comentados a seguir.

O sistema elétrico de uma subestação possui sistemas e equipamentos de custo elevado. Com isso, uma falha que possa danificar o sistema ou os equipamentos representa uma perda financeira significativa [37]. A interrupção no fornecimento de energia também implica ações legais contra as empresas transmissoras com multas da ordem de milhões[3]. Por tanto, faz-se necessário um sistema de proteção e controle que permita que falhas sejam restabelecidas em tempo hábil e que não se propaguem afetando outras áreas ou equipamentos. Linhas de transmissão são extensas e por isso muito suscetíveis a falhas. O sistema de proteção das linhas de transmissão, denominado sistema de teleproteção, tem esquemas de proteção que são auxiliados por uma rede de comunicação. Com isso, os dispositivos localizados nas extremidades das linhas de transmissão, chamados IEDs, permitem uma reação mais eficiente para atuação em caso de falha. Esse cenário possui restrições temporais 3 milissegundos para mensagens críticas, como o caso da comunicação horizontal entre IEDs.

Outra área de impacto é o aumento da utilização de veículos elétricos. A introdução de veículos elétricos na rede elétrica levanta novas preocupações devido, dentre outras

[3] "Devido ao descumprimento da liminar que determinava o fornecimento de 100% da energia elétrica no município Manacapuru (a 70 quilômetros de Manaus), a Força-tarefa do Consumidor, instalada na Assembleia Legislativa do Estado do Amazonas (Aleam), vai solicitar à Justiça a execução de multa à Amazonas Energia, no valor de R$ 1 milhão por dia-- Notícia retirada do site: https://amazonas1.com.br/amazonas/forca-tarefa-cobra-da-justica-multa-de-r-1-milhao-por-dia-a-amazonas-energia. Acesso em: set. 2019

características, à mobilidade dos veículos. Enquanto no cenário de teleproteção, todos os IEDs são previamente conhecidos e mapeados na rede de comunicação [12], o cenário de veículos elétricos é mais dinâmico, com a conexão e desconexão de veículos ao sistema elétrico a qualquer momento. Para tal, é necessário um sistema supervisório que consiga se comunicar com esses novos dispositivos – também considerados IEDs– sem conhecimento prévio de sua posição na rede de comunicação. Por exemplo, um motorista pode querer recarregar a bateria de seu veículo no período da manhã em seu trabalho, e mais tarde recarregar o mesmo veículo em casa. Como esse cenário faz uso do sistema supervisório, os requisitos temporais são menos críticos, permitindo latência de até 1 segundo, por outro lado, a mobilidade dos veículos no sistema elétrico traz novos desafios não encontrados no cenário de teleproteção.

Cada um desses cenários possui perfis de usuários diferentes. Enquanto no cenário de teleproteção, os usuários são os próprios IEDs, no cenário de veículos elétricos, os usuários podem ser os próprios motoristas. Sendo assim, os IEDs de teleproteção operam autonomicamente e precisam de certificados para a autenticação, os veículos elétricos operam sob a supervisão do motorista, por tanto, sua autenticação pode ser feita através da tupla usuário e senha.

2.4 Redes Definidas por *Software*

A rede definida por *software*, ou *Software-Defined Network* (SDN), é um paradigma de rede de comunicação que centraliza a inteligência da rede em um controlador. Conforme pode ser visto na Figura 2.7, a arquitetura da rede definida por *software* é caracterizada por:

1. **Plano de Dados**, representado pelos comutadores SDN. Os comutadores são responsáveis por comutar quadros, ou pacotes, respeitando as regras de fluxos[4] instaladas em sua tabela de fluxos. Caso o comutador não possua uma regra para um determinado pacote, esse comutador informa ao controlador SDN através da *Application Programming Interface* (API) *southbound*, por exemplo, através do protocolo OpenFlow [38];

2. **Plano de Controle**, representado pelo controlador SDN. O controlador possui uma visão global da rede e é responsável por instalar, deletar ou modificar os fluxos de

[4]Esta dissertação utiliza o termo regra de fluxo e fluxo de maneira análoga.

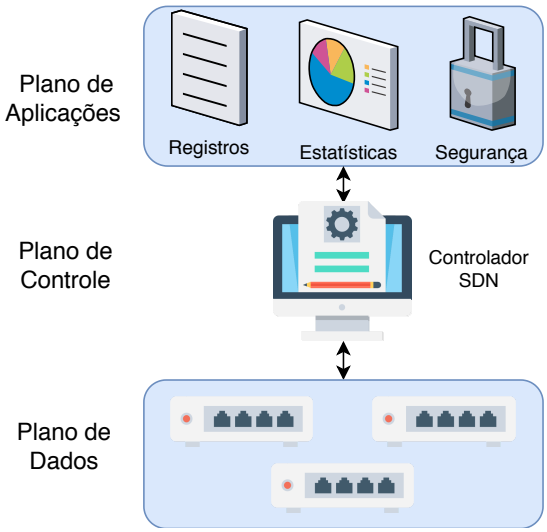


Figura 2.7: Arquitetura da rede definida por *software* dividida em plano de dados, plano de controle e plano de aplicação.

cada comutador. Ao receber uma nova solicitação de um comutador, o controlador deve decidir o que deve ser feito com pacotes daquele tipo e informar ao comutador através da API *southbound*; e

3. **Plano de Aplicação**, representado por aplicações de propósitos específicos, como um sistema de registro de auditoria ou até mesmo um sistema de segurança. O controlador pode ser auxiliado por essas aplicações para a tomada de decisão, comunicando-se através da API *northbound*, como por exemplo, uma API RESTful.

Muitos trabalhos apontam SDN como uma ótima solução de comunicação para as redes elétricas inteligentes [11], seja para uma melhor resiliência [10], escalabilidade [27], encaminhamento [33], ou até mesmo segurança [46]. Em cenários dinâmicos, como o de veículos elétricos, a rede de comunicação tradicional enfrenta uma grande complexidade enquanto na SDN, o dinamismo exigido pelos IEDs é facilmente atendido [31, 46].

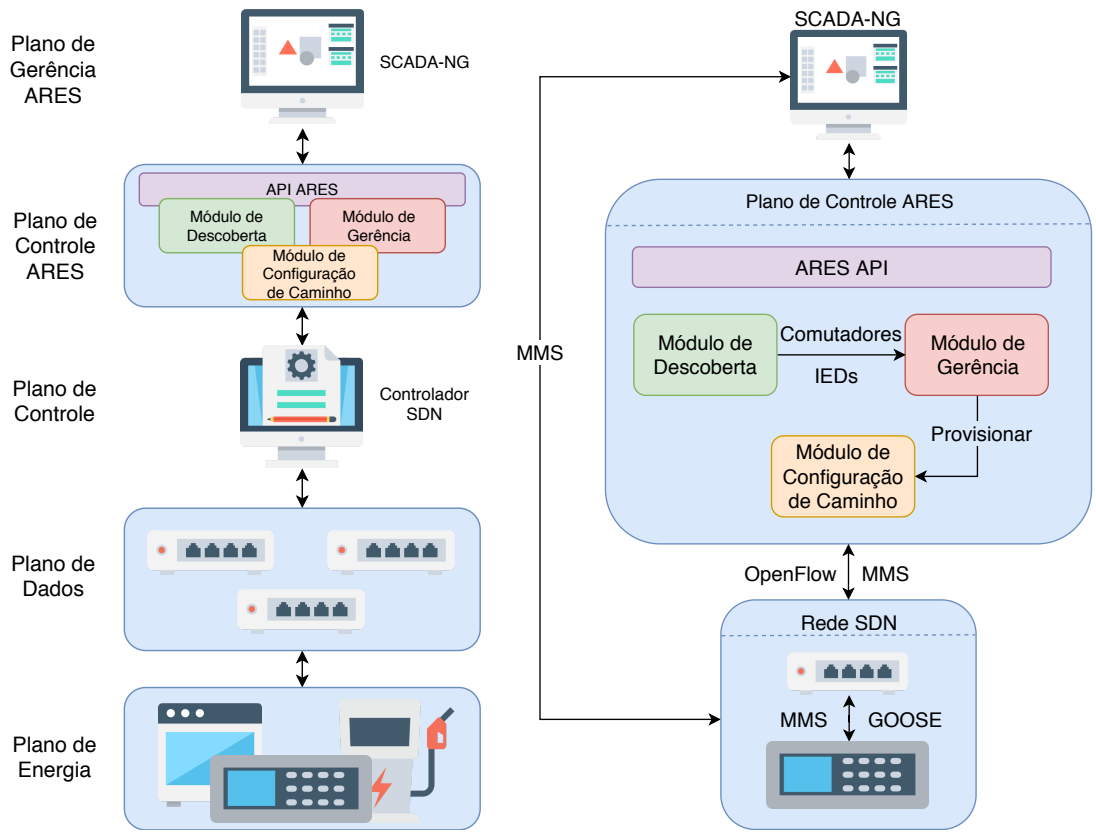
2.4.1 ARES

O *Autonomic and Resilient communication framEwork for Smart grids* (ARES) é um arcabouço para a redes elétricas inteligentes baseado em SDN e na norma IEC 61850. Segundo [30], esse arcabouço permite que os serviços de controle configurem dinamicamente a rede de comunicação em tempo real, criando uma ponte entre o sistema supervisório e o controlador SDN.

Através de seus módulos, componentes e de sua API, o ARES permite que o sistema

supervisório aloque recursos de comunicação sob demanda [30] para melhor gerenciar a rede elétrica, possibilitando a integração de sistemas dinâmicos como é o caso de veículos elétricos. As redes elétricas inteligentes geralmente têm suas funcionalidades de rede, como o encaminhamento de pacotes, definido durante a fase de projeto, o que dificulta a reconfiguração da rede em tempo real [10]. Logo, uma rede de comunicação dinâmica é essencial para as redes elétricas em um cenário onde IEDs são móveis, como os veículos elétricos, podendo se conectar à rede em pontos e horários diferentes.

A Figura 2.8(a) apresenta a arquitetura do ARES, que se divide em: (1) plano de energia, que representa os IEDs modelados em conformidade com a norma IEC 61850; (2) plano de dados SDN; (3) plano de controle; (4) plano de controle ARES, que funciona de forma similar ao plano de aplicação SDN; e (5) plano de gerência baseado no ARES, representado pelo sistema supervisório.



(a) Plano de energia, plano de dados, plano de controle, plano de controle ARES e plano de gerência baseado no ARES.

(b) Visão geral da interação entre os módulos de descoberta, de gerência e de configuração de caminho.

Figura 2.8: Arquitetura ARES.

O *Supervisory Control and Data Acquisition* (SCADA) é um sistema para monitoramento e controle amplamente implementado [12]. Como o ARES necessita de um sistema

supervisório *ARES-aware*, ou ciente do ARES, a autora propõe a criação do *Supervisory Control and Data Acquisition* de Nova Geração (SCADA-NG), um sistema supervisório capaz de se comunicar com o arcabouço ARES. O SCADA-NG é modular e permite que várias aplicações para monitoração e controle de sistemas de energia, chamadas aplicações de energia, sejam criadas baseadas nos mesmos serviços. O SCADA tradicional apenas controla a operação dos IEDs enquanto o SCADA-NG traz um conjunto de novas funcionalidades que permitem atrelar o controle da operação dos IEDs a adaptação autonômica da rede. Por exemplo, o veículo elétrico que em um momento recarrega sua bateria, em outro momento pode ser usado como fonte, precisando assim participar do esquema de proteção do sistema elétrico. A Figura 2.8(b) apresenta uma visão geral do funcionamento dos módulos ARES.

O `Módulo de Descoberta` é responsável por mapear e descobrir os comutadores SDN e IEDs conectados à rede de comunicação. O `Módulo de Gerência` é responsável por prover as informações necessárias ao `Módulo de Configuração de Caminho` e por gerenciar os eventos de rede de comunicação. O `Módulo de Configuração de Caminho` é responsável pelo cálculo dos caminhos necessários na rede de comunicação e pela instalação dos fluxos nos comutadores SDN, conforme solicitado pelo `Módulo de Gerência`.

Quando um novo IED se conecta à rede SDN, o `Módulo de Descoberta` faz a leitura de seus dados através do protocolo MMS e localiza informações referentes à comunicação, como por exemplo, o grupo GOOSE *multicast* para o qual aquele IED irá enviar mensagens, vide a Figura 2.5. Após o mapeamento, o `Módulo de Descoberta` repassa essas informações ao `Módulo de Gerência`, que decide quais fluxos devem ser provisionados e suas respectivas prioridades. Em seguida, o `Módulo de Gerência` solicita o provisionamento desses fluxos ao `Módulo de Configuração de Caminho`, que calcula um caminho principal e outro *backup*, para assegurar os requisitos temporais impostos pela norma IEC 61850 mesmo em caso de falhas na rede de comunicação, e, finalmente, instala os devidos fluxos.

Esta dissertação propõe a inclusão de funcionalidades de autenticação, autorização e auditoria para redes elétricas inteligentes através da extensão do *framework* ARES, como será discutido nos próximos capítulos.

Capítulo 3

Trabalhos Relacionados

A integridade e confidencialidade em redes elétricas inteligentes vem sendo bastante investigadas [28, 8, 2, 42, 46, 6], assim como Autenticação e Autorização (AA) para controlar o acesso de novos serviços ou dispositivos na rede elétrica [51, 39, 44, 41, 19]. Entretanto, ainda há pouca discussão sobre sistemas integrados de Autenticação, Autorização e Auditoria (AAA) [26]. Este capítulo apresenta uma revisão sobre os trabalhos relacionados à AAA para redes elétricas inteligentes, além de compará-los com o 3AS, proposto nesta dissertação.

3.1 Autenticação

Muitos dos trabalhos sobre segurança da informação em redes elétricas inteligentes têm como foco a autenticação para integridade e confidencialidade das mensagens [28, 8, 2, 42, 46, 6], mas não se atentam para a autorização ou auditoria.

Em [28], os autores propõem a autenticação através da assinatura de quadros *multicast* (GOOSE e SV) utilizando *One-Time Signature* (OTS) para garantir a integridade das mensagens. O publicador utiliza funções *hash* passando como parâmetros sua chave privada e o conteúdo do quadro *multicast* para obter um valor específico e assinar a mensagem. Já o assinante, utiliza a chave pública para verificar se o conteúdo da mensagem corresponde à assinatura do publicador. Em [42], os autores também avaliam a autenticação através da assinatura de quadros *multicast* (GOOSE, SV) para garantir a integridade das mensagens. Entretanto, os autores utilizam os protocolos *Rivest–Shamir–Adleman* (RSA) e *Advanced Encryption Standard* (AES), além de avaliar também a cifragem de toda a informação para garantir a confidencialidade. Os autores confirmam a inviabilidade do RSA, por demandar muito processamento de dispositivos com baixa capacidade de proces-

samento, mas comprovam a possibilidade de utilizar o protocolo AES, tendo desempenho suficiente para assinar e cifrar toda a mensagem.

Em [8], os autores avaliam a autenticação através do TLS para garantir a confidencialidade e integridade de pacotes MMS. Apesar de observarem a possibilidade da utilização do TLS, os autores indicam o problema de desempenho em sistemas legados, em experimentos com máquinas de 96 MHz CPU e 32 MBytes de RAM, devido à latência introduzida pelo *handshake* do TLS, levando aproximadamente 2,8 segundos. Já em [2], os autores avaliam a autenticação através do TLS e *Simple Authentication and Security Layer* (SASL) para garantir a confidencialidade e integridade de pacotes MMS enviados por veículos elétricos. O veículo elétrico primeiro se autentica através do TLS, e com o canal seguro estabelecido, o veículo autentica-se com o servidor *eXtensible Messaging and Presence Protocol* (XMPP) utilizando SASL.

Em [6], os autores avaliam a autenticação para mensagens IEC 61850 (GOOSE, SV e MMS) no contexto de troca de informações entre subestações. Os autores propõem a redundância da comunicação com fio utilizando enlaces sem-fio *Long-Term Evolution* (LTE) ou IEEE 802.11 em uma rede definida por *software*. Os autores avaliam a sobrecarga gerada pela autenticação das duas tecnologias utilizando os protocolos de autenticação padrões das mesmas: *IP Security* (IPsec) para LTE; e EAP-PSK para IEEE 802.11. Essa proposta é uma solução inteligente para garantir a resiliência da rede, pois, uma vez que o enlace físico falhe, os comutadores SDN comutam automaticamente para o enlace sem-fio autenticado previamente. De qualquer forma, essa proposta é específica para a comunicação entre os comutadores de diferentes subestações, e não entre IEDs dentro de uma única subestação.

3.2 Autenticação e Autorização

Diversos trabalhos levam em consideração o controle de acesso de usuários e IEDs para adotar políticas de segurança mais restritivas [51, 39, 44, 41, 19]. Os modelos de controle de acesso mais utilizados são *Role-Based Access Control* (RBAC) e *Attribute-Based Access Control* (ABAC), mas alguns trabalhos priorizam a utilização de outros modelos, como o *Access Control List* (ACL) e *Lattice-Based Access Control* (LBAC).

O FlowIdentity [51] propõe a autenticação para redes definidas por *software* através do IEEE 802.1X e utiliza o modelo RBAC para autorização. É proposto que o controlador SDN atue também como autenticador. Inicialmente, o controlador SDN permite tráfego

de pacotes de autenticação. Após o dispositivo ser autenticado, a autorização é feita de modo reativo a cada nova requisição de fluxo gerada onde o endereço MAC do dispositivo é comparada ao seu papel, e então decidido se o dispositivo tem acesso ao fluxo solicitado. Já o Resonance [39] propõe a autenticação através de um serviço *web* para redes definidas por *software*, também conhecido por *captive portal*. A proposta utiliza o LBAC, modelo de controle de acesso baseado na interação entre objetos e sujeitos, similar ao ABAC mas baseado em modelos matemáticos. Inicialmente, o controlador SDN permite apenas tráfegos referentes a autenticação através do *captive portal*. Após autenticado, o dispositivo ganha acesso a uma lista limitada de serviços conforme descrito pela política associada ao seu usuário.

Em [44], os autores propõem AA para redes elétricas inteligentes baseado em *Named Data Networking* (NDN). O NDN é uma arquitetura proposta para a *Internet* do Futuro com o foco nos dados ao invés de foco nos dispositivos. A autenticação é similar aos modelos tradicionais: assinatura de pacotes de forma nativa proposta pelo NDN, ou a autenticação mútua através de chaves (similar ao TLS). Apesar do foco desse artigo ser o problema de escalabilidade do protocolo IP, os autores propõem o controle de acesso através do modelo ACL. Como o ACL necessita da criação de novas políticas para cada nova ação de cada novo usuário, esse modelo também apresenta um problema de escalabilidade, o qual não é discutido pelos autores. Outro desafio da utilização do paradigma NDN é sua interoperabilidade com sistemas legados, ou IEDs atuais, sendo necessário um conversor de pacotes IP, ou quadros *ethernet*, para o formato especificado pela NDN, conforme apontado pelos autores.

O modelo proposto em [41] é voltado para o acesso de usuários que são operadores da rede elétrica. Para esse cenário, é utilizado uma autenticação em dois passos: primeiro, o IED autentica o usuário através da assinatura dos pacotes. Em seguida, o sistema envia um *One-Time Password* (OTP) para o celular do usuário. Os autores propõem a utilização do modelo RBAC para definição de políticas de acesso no servidor, que é o sistema supervisório, e um modelo ABAC implementado no próprio IED para computação dinâmica dos atributos que determinado usuário terá acesso. Entretanto, é necessário uma avaliar se os IEDs possuem poder computacional para tal.

Finalmente, a norma IEC 62351 [19], também desenvolvida pelo comitê técnico 57 do IEC, apresenta soluções de segurança para a norma IEC 61850. Para a autenticação, é proposta a assinatura de quadros GOOSE e SV, e a utilização de TLS para pacotes MMS. A norma ainda define a utilização do modelo RBAC para o controle de acesso. Para a

implementação do RBAC, a norma propõe a extensão de certificados para informar o papel do IED, além de um atributo `área de responsabilidade`. Este atributo `área de responsabilidade` funciona de forma similar ao atributo `contexto`, nativo do modelo ABAC. Em [43], os autores apontam a complexidade desnecessária de se utilizar esse tipo de certificado, além de destacar que qualquer mudança nas associações de um papel requer a geração de novos certificados.

Apesar das propostas [51, 39] não serem voltadas para redes elétricas inteligentes, podem ser facilmente adaptadas para o cenário. Diferente dos trabalhos citados anteriormente, o 3AS, proposta desta dissertação, além de prover apenas um mecanismo de autenticação para os três protocolos de comunicação, IEEE 802.1X autenticando GOOSE, SV e MMS, e propor a utilização do modelo ABAC associado ao processo de autenticação, ainda propõe um sistema integrado de auditoria, registrando eventos de autenticação, autorização e utilização de recursos da rede de comunicação.

3.3 Autenticação, Autorização e Auditoria

Apesar da norma IEC 62351 citar parcialmente a auditoria, seu foco é a Autenticação e Autorização (AA). Um trabalho que discute integralmente a Autenticação, Autorização e Auditoria (AAA) é proposto em [26].

Khan *et al.* [26] propõem a utilização da tecnologia *Worldwide Interoperability for Microwave Access* (WiMAX) para o cenário de cobrança em redes elétricas inteligentes. O WiMAX é uma tecnologia de comunicação sem-fio que conta com mecanismos para AAA: autenticação através de assinatura por RSA ou canal seguro por TLS; a autorização proposta pelos autores é através de serviços pré-pagos. Para um veículo elétrico ou o medidor inteligente de uma casa poderem consumir a energia da rede, o usuário precisa ter créditos. A auditoria é integrada ao servidor, que mantém as informações de créditos dos usuários, permitindo assim o registro de eventos de autenticação e autorização.

Em cenários de teleproteção na rede elétrica inteligente, o sistema deve apresentar alta disponibilidade. Caso um IED que participe do esquema de proteção da rede elétrica deixe de enviar, ou receber mensagens de proteção, o sistema pode apresentar perda financeira ou até mesmo dano a equipamentos [37, 32]. Portanto, o modelo proposto por Khan *et al.* é limitado, não atendendo a todos os cenários de redes elétricas inteligentes, uma vez que um simples ataque de interferência ao meio sem-fio [53] poderia tornar o IED inacessível.

O 3AS preocupa-se em atender cenários diversos de redes elétricas inteligentes, desde

a introdução de veículos elétricos na rede, até o sistema de teleproteção da rede elétrica. Diferente de alguns trabalhos, o 3AS propõe a utilização de apenas um mecanismo de autenticação que atende aos três protocolos de comunicação definidos pela norma IEC 61850. Através da utilização do modelo ABAC para a autorização, as políticas de acesso granulares permitem a criação de diferentes níveis de acesso, além de identificar erros de configuração nos IEDs conforme será explicado no Capítulo 4. Por fim, diferente da maioria dos trabalhos, o 3AS propõe um modelo de autenticação e autorização integrado à auditoria, permitindo o registro de eventos da rede de forma centralizada.

A Tabela 3.1 apresenta uma comparação qualitativa entre os trabalhos discutidos neste capítulo. Diferente do FlowIdentity [51], que também utiliza o padrão IEEE 802.1X para autenticação, o 3AS permite a autorização tanto reativa quanto proativa. Saxena *et al.* [41] implementam o modelo ABAC para a interação entre um usuário e um IED, enquanto a comunicação entre IEDs ou com o sistema supervisório é feita através de RBAC. Já o 3AS se beneficia da granularidade do modelo ABAC para todos os tipos de comunicação na subestação. Por fim, Khan *et al.* [26] propõem uma arquitetura de AAA específica para cenários de cobrança por consumo de energia, ou seja, a comunicação entre IEDs e o sistema supervisório. Já o 3AS, foi modelado para atender a diversos cenários e protocolos de comunicação para redes elétricas inteligentes.

Tabela 3.1: Relação das pesquisas sobre AAA para Redes Elétricas Inteligentes.

Trabalho	**Mecanismo de Autenticação**	**Modelo de Autorização**	**Auditoria**	**Protocolos de Comunicação**	**Rede de Comunicação**	**Cenário**	**Foco**
Li, Q. e Cao, G. [28]	Assinatura	Não Discutido	Não Discutida	GOOSE, SV	Independente	Rede Elétrica Inteligente	Autenticação
Chowdhury, M. M. R. *et al.* [8]	TLS	Não Discutido	Não Discutida	MMS	Independente	Rede Elétrica Inteligente	Autenticação
Aftab, M. A. *et al.* [2]	TLS, SASL	Não Discutido	Não Discutida	MMS	Independente	Veículos Elétricos	Autenticação
Scarselli, R. B. *et al.* [42]	Assinatura	Não Discutido	Não Discutida	GOOSE, SV	Independente	Rede Elétrica Inteligente	Autenticação
Aydeger, A. *et al.* [6]	IPSec, EAP-PSK	Não Discutido	Não Discutida	IEC 61850	SDN	Entre Subestações	Autenticação
FlowIdentity [51]	802.1X	RBAC	Não Discutida	Independente	SDN	Rede Definida por *Software*	AA
Resonance [39]	HTTP	LBAC	Não Discutida	Independente	SDN	Acesso a Internet	AA
Shang, W. *et al.* [44]	Assinatura, TLS	ACL	Não Discutida	Não Especifica	NDN	Rede Elétrica Inteligente	AA
Saxena, N. *et al.* [41]	Assinatura, OTP	RBAC, ABAC	Não Discutida	IEC 61850	Independente	Acesso de usuários	AA
IEC 62351 [19]	Assinatura, TLS	RBAC	Parcial	IEC 61850	Independente	Rede Elétrica Inteligente	AA
Khan, R. *et al.* [26]	Assinatura, TLS	Não Especifica	Completa	Não Especifica	Não Especifica	Consumo pré-pago	AAA
3AS	802.1X	ABAC	Completa	IEC 61850	SDN	Rede Elétrica Inteligente	AAA

Capítulo 4

Proposta do 3AS

Apesar dos benefícios apresentados pela introdução de uma rede de comunicação, novas vulnerabilidades são incorporadas à rede elétrica inteligente. Assim como o controle remoto dos IEDs facilita a manutenção da rede elétrica, atacantes obtêm um novo meio de acesso indevido aos dispositivos da rede. Através da implementação de mecanismos que respeitem os requisitos de autenticação, autorização e auditoria, a gestão de identidade visa reduzir vulnerabilidades na comunicação de redes elétricas inteligentes.

A proposta Autenticação, Autorização e Auditoria para *Smart Grids* (3AS) estende o *framework* ARES [30] para a implementação de mecanismos de segurança que interagem diretamente com os módulos ARES. Um mecanismo de autenticação baseado no protocolo IEEE 802.1X é utilizado para autenticar cada dispositivo permitindo o envio de mensagens de acordo com os três protocolos de comunicação definidos pela norma IEC 61850 [46]. Além disso, o 3AS realiza a autorização utilizando o modelo ABAC, que permite um controle de acesso granular. Por fim, o 3AS mantém um sistema de auditoria integrado, registrando eventos de autenticação, auditoria e utilização de recursos da rede.

Os componentes da arquitetura do 3AS, Autenticação, Autorização e Auditoria, são adicionados ao plano de controle ARES e podem ser vistos na Figura 4.1 e são descritos a seguir:

- `Módulo de Autenticação`, responsável por identificar os IEDs e informar ao controlador SDN o resultado de cada processo de autenticação. Atua como autenticador e servidor de autenticação baseado no protocolo IEEE 802.1X;
- `Módulo de Autorização`, responsável por informar ao controlador SDN o nível de acesso específico de cada IED, permitindo a comunicação de acordo com a autori-

zação do dispositivo. Utiliza o modelo ABAC para o controle de acesso;

- `Módulo de Auditoria`, responsável por manter o registro dos eventos de comunicação de cada dispositivo na rede de comunicação, como autenticação e autorização. Este módulo é encarregado também de manter o registro de eventos da rede elétrica conforme informado pelo sistema supervisório, o SCADA-NG;

- `Plano de Controle ARES`, aplicações ARES dentro do controlador SDN, responsável por instalar e remover as regras de fluxos de cada comutador da rede de comunicação, respeitando as decisões do nó de autenticação e do controle de acesso. A API ARES deve repassar as informações necessárias ao SCADA-NG para que este possa supervisionar os IEDs.

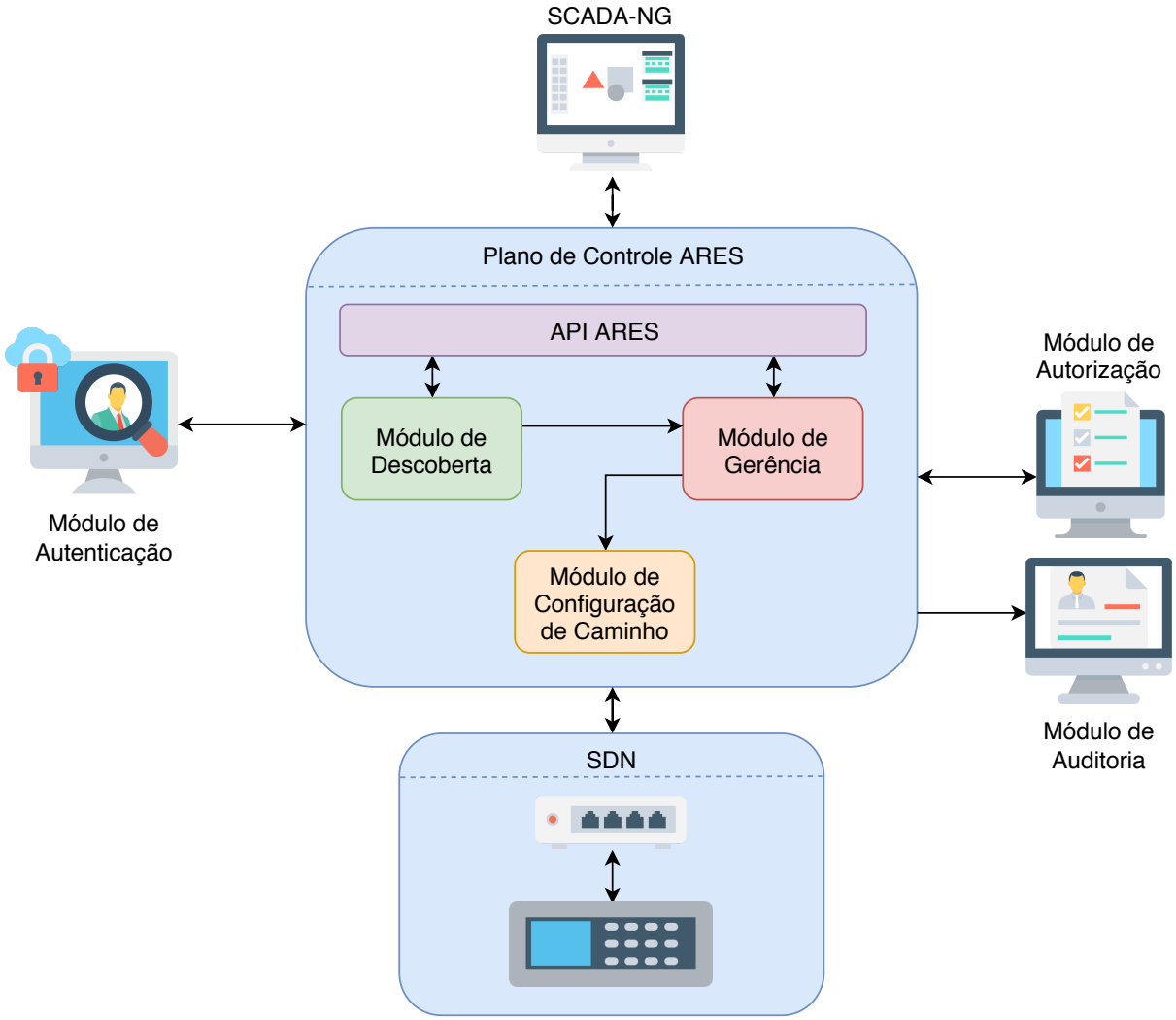


Figura 4.1: Componentes da arquitetura do 3AS.

4.1 Requisitos para implantação do 3AS

O 3AS necessita que a rede elétrica inteligente seja preparada para atender aos seguintes requisitos:

- Os dispositivos devem ser capazes de se autenticar através do protocolo IEEE 802.1X, seja nativamente ou através de um dispositivo externo ligado diretamente a ele;
- A rede de comunicação deve ser preparada para atender aos requisitos do ARES, uma vez que o 3AS é uma extensão desse *framework*: uma rede definida por *software* baseada no protocolo OpenFlow e a comunicação dos IEDs através dos protocolos especificados pela norma IEC 61850;
- Infraestrutura de chaves públicas e um sistema para cadastro de senhas por parte dos usuários;
- Uma base de dados para cadastro da identidade dos IEDs e seus níveis de autorização. Essa base pode ser populada, por exemplo, por um operador ou através da importação do arquivo SCL.

4.2 Módulo de Autenticação

A autenticação é o primeiro processo para garantir a segurança da rede elétrica inteligente. Uma vez que dispositivos elétricos de diferentes naturezas podem entrar e sair do sistema a qualquer momento, é importante identificá-los a cada nova entrada para que o acesso à rede de comunicação possa ser controlado apropriadamente. Dessa forma, para a autenticação dos IEDs, é proposta a utilização do protocolo 802.1X [15], que autentica a porta física do comutador SDN na qual o IED está diretamente conectado. Dessa forma, após ser autenticado, o IED passa a ter acesso ao envio dos quadros e mensagens configurados em sua modelagem. A Figura 4.2 apresenta a sequência de eventos de acordo com uma autenticação bem sucedida.

Inicialmente (1), o suplicante, IED, solicita a autenticação através da camada de enlace para o nó de autenticação. O suplicante envia seus quadros de autenticação para o destino *multicast* `01:80:c2:00:00:03` e o controlador SDN direciona esses quadros para o nó de autenticação, evitando a necessidade de efetuar o *broadcast* desses quadros. Em seguida (2), o autenticador faz a ponte entre o suplicante e o servidor de autenticação,

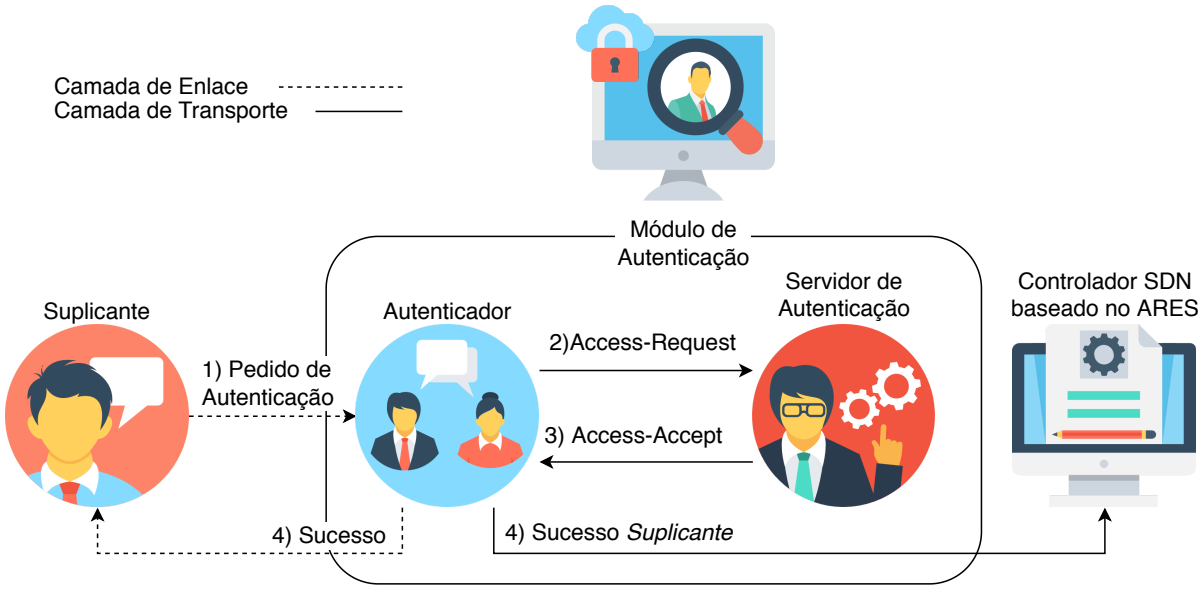


Figura 4.2: Processo de autenticação aceito através do nó de autenticação do 3AS.

encapsulando quadros EAP enviados pelo suplicante para pacotes RADIUS a serem recebidos pelo servidor de autenticação e vice-versa. Após validar a identificação do IED, o servidor de autenticação informa ao autenticador (3). Finalmente, o autenticador informa simultaneamente a autenticação bem sucedida ao suplicante, através de quadros EAPoL, e ao controlador SDN, através da API ARES (4).

A Figura 4.3 apresenta o mesmo processo descrito anteriormente, entretanto no passo (3) o servidor de autenticação nega o pedido ao IED, seja por um certificado expirado, uma credencial incorreta, ou até mesmo pela tentativa de autenticação ilegítima. Em seguida, no passo (4), o autenticador informa a autenticação negada ao IED e ao controlador SDN.

Para identificar o IED, o controlador SDN associa o endereço MAC do IED à porta física e ao comutador SDN. Dessa forma, caso um novo suplicante tente se autenticar utilizando o endereço MAC de um IED já autenticado, o suplicante será negado, impedindo, assim, ataques de personificação.

4.3 Módulo de Autorização

Após a autenticação, deve-se avaliar quais recursos o IED tem direito de acesso. Assim, o 3AS inicia o processo para definir as regras de controle de acesso baseadas em atributos. A rede elétrica inteligente possui diversos atributos que podem ser utilizados como base para ABAC. Os atributos podem ser: (1) sujeitos, representados por IEDs ou usuários; (2) ações, representadas pelo envio, ou recebimento, de mensagens IEC 61850 (GOOSE,

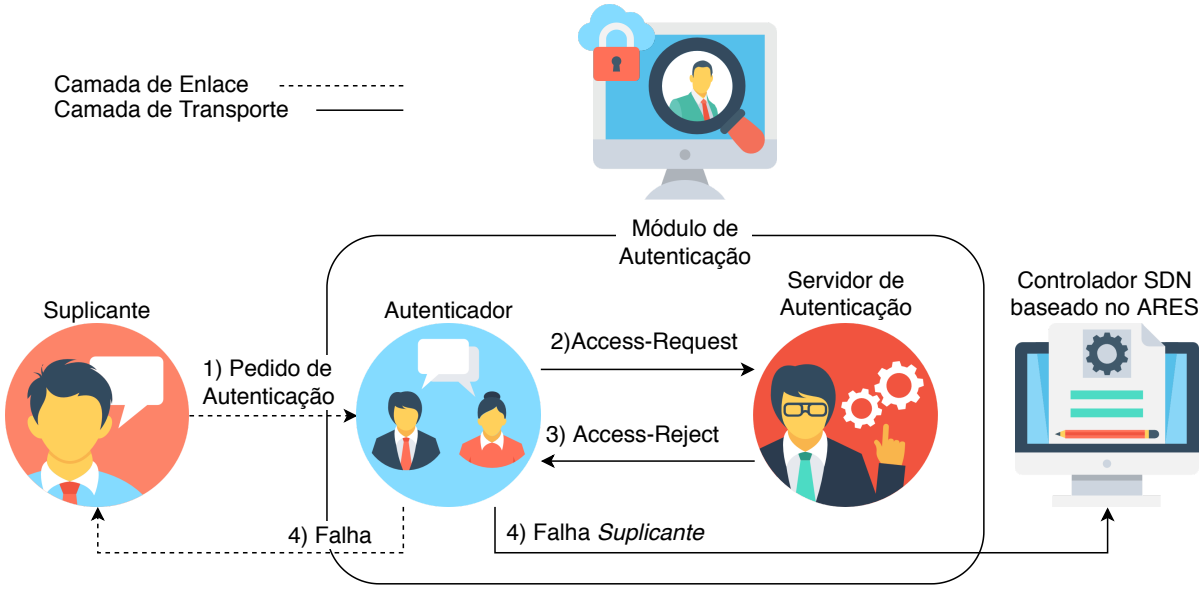


Figura 4.3: Processo de autenticação negada através do nó de autenticação do 3AS.

SV e MMS); e (3) recursos, representados pelos comutadores SDN ou outros IEDs.

O processo de autorização do 3AS ocorre com base nos atributos MMS. As políticas de acesso são relacionadas às seguintes atividades:

1. troca de mensagens MMS com o sistema supervisório SCADA-NG, ou outro IED atuando como um *gateway*;
2. publicar quadros para um grupo GOOSE;
3. assinar (receber) quadros de um grupo GOOSE;
4. publicar quadros para um grupo SV ou para um único IED;
5. assinar (receber) quadros de um grupo SV, ou de um único IED;
6. enviar e receber mensagens para sincronização de relógios;
7. enviar e/ou receber mensagens de gerência de rede de comunicação; e
8. outras ações relacionadas a outros protocolos cujos comportamentos podem ser configurados pelo operador da rede.

A título de exemplo, um IED configurado conforme a Figura 2.5, terá como atributos:

- Publicação de quadros GOOSE representados pelo elemento `GSE`, identificados por `gcbAnalogValues`;

- Publicação para o grupo GOOSE `01:0C:CD:01:00:01`;
- Publicação de quadros SV representados pelo elemento `SMV`, identificados por `Volt`;
- Publicação para o grupo SV `01:0C:CD:04:00:01`.

Ao restringir o acesso a essas atividades, o 3AS reduz as vulnerabilidades de segurança, como por exemplo: evitar que uma entidade não-autorizada receba mensagens destinadas a outros IEDs; evitar que uma entidade não-autorizada controle outros IEDs; ou negar a comunicação de protocolos que não fazem parte da da rede elétrica inteligente e poderiam representar um ponto de vulnerabilidade.

A Figura 4.4 apresenta o processo de autorização bem sucedido.

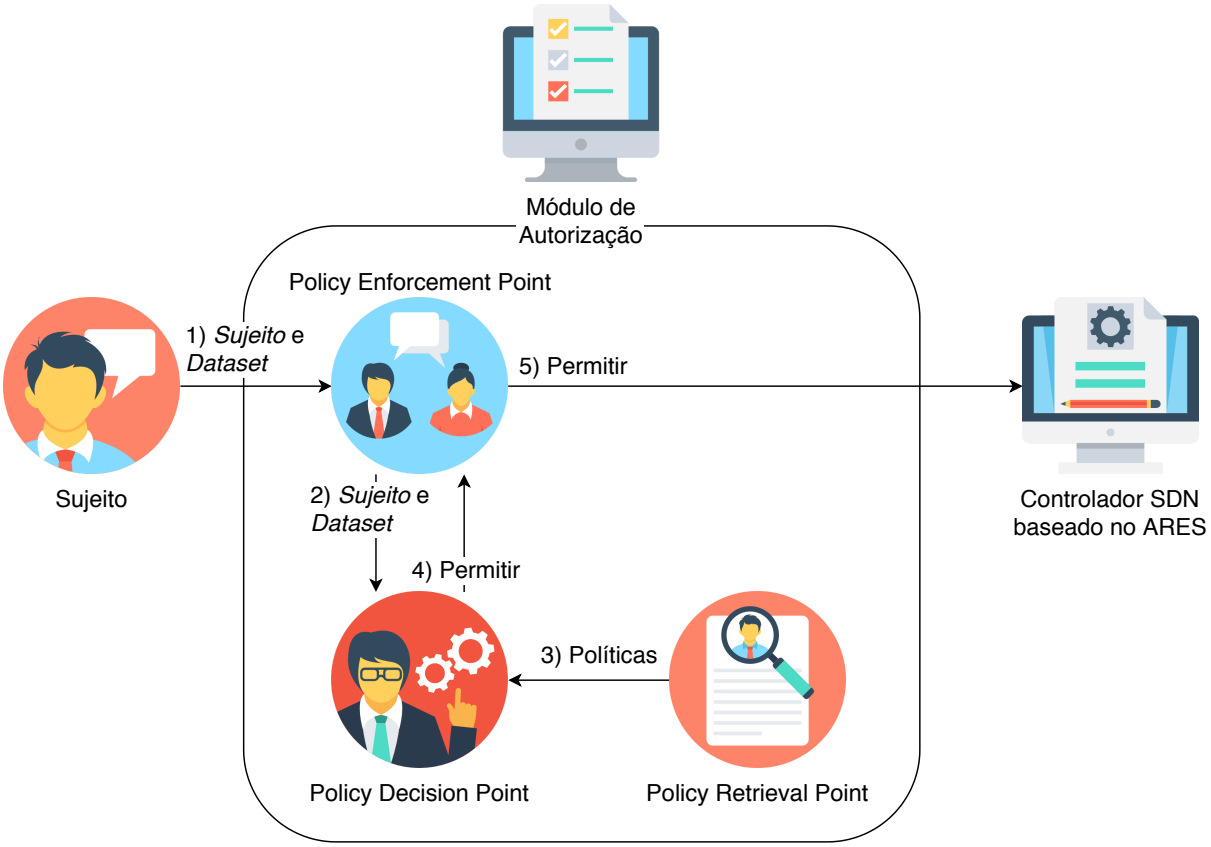


Figura 4.4: Processo de autorização aceita através do controle de acesso do 3AS.

Inicialmente (1), o sujeito, IED, solicita a autorização informando suas intenções na rede de comunicação, onde o *dataset* possui informações como: publicar quadros GOOSE para um determinado grupo ou assinar (receber) quadros SV de um determinado grupo. Em seguida (2), o *Policy Enforcement Point* (PEP) envia o pedido ao *Policy Decision Point* (PDP), que verifica os dados recebidos com as políticas informadas pelo *Policy Retrieval Point* (PRP) (3), e decide que ele está autorizado a executar as ações solicitados

e informa ao PEP (4). Finalmente (5), o PEP informa ao controlador que o IED está autorizado a executar todas as ações solicitadas.

A Figura 4.5 apresenta o mesmo processo descrito anteriormente, entretanto no passo (4) o PDP não autoriza o IED, seja por uma configuração errada, ou até mesmo pela tentativa de acesso ilegítimo. Em seguida (5), o PEP informa a autorização negada ao controlador SDN.

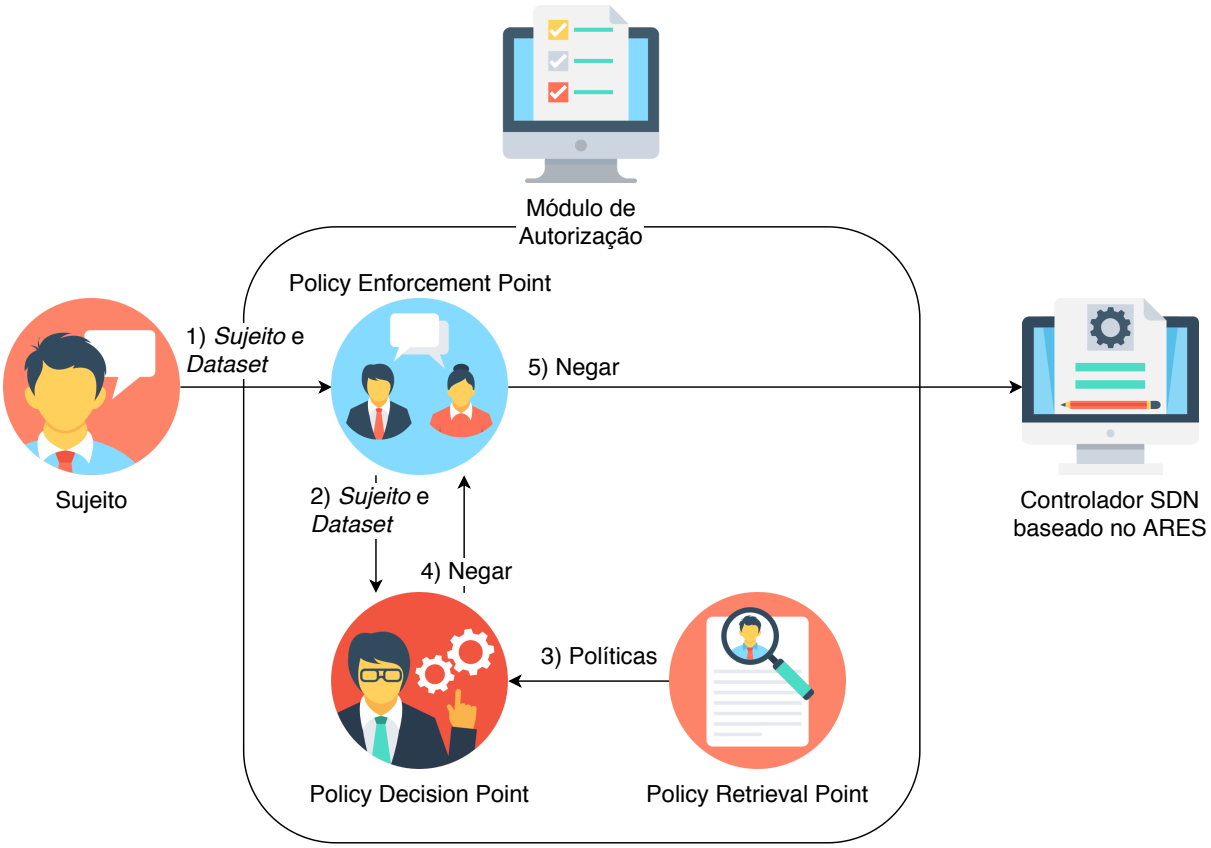


Figura 4.5: Processo de autorização negada através do controle de acesso do 3AS.

O processo de autorização pode ser feito de forma proativa ou reativa e será melhor detalhado na Seção 4.4. É importante ressaltar que o processo de autorização ocorre apenas uma vez por fluxo de comunicação, portanto o atraso gerado por esse mecanismo ocorre apenas para a primeira mensagem enviada em um fluxo. Uma vez autorizado, as mensagens seguintes fluem sem o atraso gerado pela autorização.

O modelo ABAC permite a criação de políticas para autorizar e negar acessos. A título de exemplo, podemos criar duas regras básicas para controlar o acesso e prevenir erros de configuração: (1) IEDs do grupo 1 estão autorizados a enviar quadros GOOSE para o grupo *multicast* 01:0C:CD:01:00:**01**. Assim, IEDs do grupo 1 podem enviar apenas quadros GOOSE e com destino conforme especificado; e (2) quadros GOOSE devem

possuir o prefixo `01:0C:CD:01` no endereço MAC de destino. Assim, IEDs podem enviar quadros GOOSE para qualquer grupo desde que possua o formato especificado pela norma.

Um diferencial do ABAC quanto comparado ao RBAC é a criação de políticas. Por exemplo: um primeiro IED participa dos grupos *multicast* GOOSE 1 e 2, enquanto outro IED participa dos grupos 2 e 3, e um terceiro IED participa dos grupos 3 e 1. Desta forma, os atributos relacionados a cada IED são necessários para definir as ações as quais ele terá acesso. Caso essa política fosse construída no modelo RBAC, deveriam ser criados diversos papéis para atender a cada um desses casos específicos. Assim, o controle de acesso não se restringe ao papel do IED, mas é definido de acordo com os atributos de cada IED, que podem, inclusive, ser dinâmicos.

4.4 Controlador SDN baseado no ARES

O controlador SDN irá manter o estado de cada IED, podendo assumir os valores:

- **Não Autenticado**, onde mensagens de autenticação serão repassadas para o nó de autenticação. Qualquer outra mensagem será desconsiderada;
- **Autenticado**, onde o IED poderá se comunicar com o controlador SDN através do protocolo MMS para informar ao controlador suas ações na rede de comunicação;
- **Autorizado**, onde será permitido ao IED se comunicar na rede conforme seu nível de autorização.

Inicialmente, todos os IEDs estão no estado Não Autenticado, no qual o 3AS permite apenas o processo de autenticação, note que é possível instalar regras de fluxos nos comutadores OpenFlow que limitem a taxa de envio de mensagens EAPoL, minimizando possíveis ataques de negação de serviço contra o controlador SDN e o autenticador [13]. Após se autenticar, o estado passa a Autenticado e o IED consegue repassar ao controlador os serviços desejados, mas não consegue fazer uso de nenhum outro serviço da rede. Por fim, após passar pelo controle de acesso, o estado passa a Autorizado e o IED tem acesso a todos os serviços que requisitou e tem direito de uso via rede de comunicação. Caso o IED se desconecte da rede por qualquer motivo, ele automaticamente volta ao estado de Não autenticado.

O controle de acesso pode funcionar de duas maneiras: (1) proativa, onde após a autenticação, o controlador SDN faz a leitura das informações do IED através do MMS

para verificar suas possíveis ações na rede de comunicação e em seguida instala as devidas regras de fluxos. O controle de acesso proativo visa a redução da latência para a comunicação na rede elétrica inteligente. Em cenários com requisitos temporais rígidos, como em sistemas de teleproteção, novas mensagens geradas na rede não possuem o atraso de autorização, uma vez que aquela mensagem foi autorizada previamente; ou (2) reativa, onde após a autenticação, o IED inicia o envio de mensagens na rede, e a cada novo fluxo, o controlador SDN acessa sua base de dados (PRP) e verifica se o fluxo respeita o nível de autorização solicitado. O controle de acesso reativo visa a redução da carga de controle para a comunicação na rede elétrica inteligente. Em cenários sem requisitos temporais rígidos, regras de fluxos são instaladas apenas quando solicitadas, diminuindo a quantidade de mensagens de controle trafegadas na rede.

A Figura 4.6 apresenta a sequência de eventos bem sucedida no modelo reativo. Após ser autenticado, o IED envia uma nova mensagem na rede (1). Como o comutador não possui nenhuma regra de fluxo para aquela mensagem, o comutador pergunta ao controlador SDN o que deve ser feito[1] (2). Em seguida, o módulo de gerência ARES traduz o fluxo para o modelo das políticas e pergunta ao ABAC se aquele IED está autorizado a enviar aquele tipo de mensagem para o destino especificado (3). Então, o ABAC informa ao módulo de gerência que o acesso ao recurso solicitado foi autorizado (4). Logo após, o módulo de gerência faz o registro da autorização bem sucedida no nó de auditoria e solicita o provisionamento para o módulo de configuração de caminho ARES (5). Finalmente, o módulo de configuração de caminho instala as regras de fluxos necessárias para a entrega da mensagem e permite que o quadro seja encaminhado.

Já para alguns cenários do sistema elétrico, como é o caso, por exemplo, da teleproteção, onde mensagens críticas possuem restrições temporais rígidas, a instalação de regras de fluxos sob demanda pode ser um problema. Para diminuir possíveis atrasos, o 3AS também permite o controle de acesso feito imediatamente após a autenticação, provisionando os fluxos necessários proativamente. Após o processo de autenticação efetuado pelo nó de autenticação, esse informa ao controlador SDN o resultado do processo. A Figura 4.7 apresenta a sequência de eventos bem sucedida no modelo proativo.

Após o nó de autenticação informar a autenticação bem sucedida (1), o ARES atualiza o estado do novo IED para `autenticado` e inicia o processo de descoberta das informações através do módulo de descoberta ARES (2). O módulo de descoberta, através do MMS, faz a leitura das informações do IED e envia para o módulo de gerência (3). O módulo

[1]Em uma implementação utilizando o OpenFlow, essa ação se dá através da mensagem `PacketIn`.

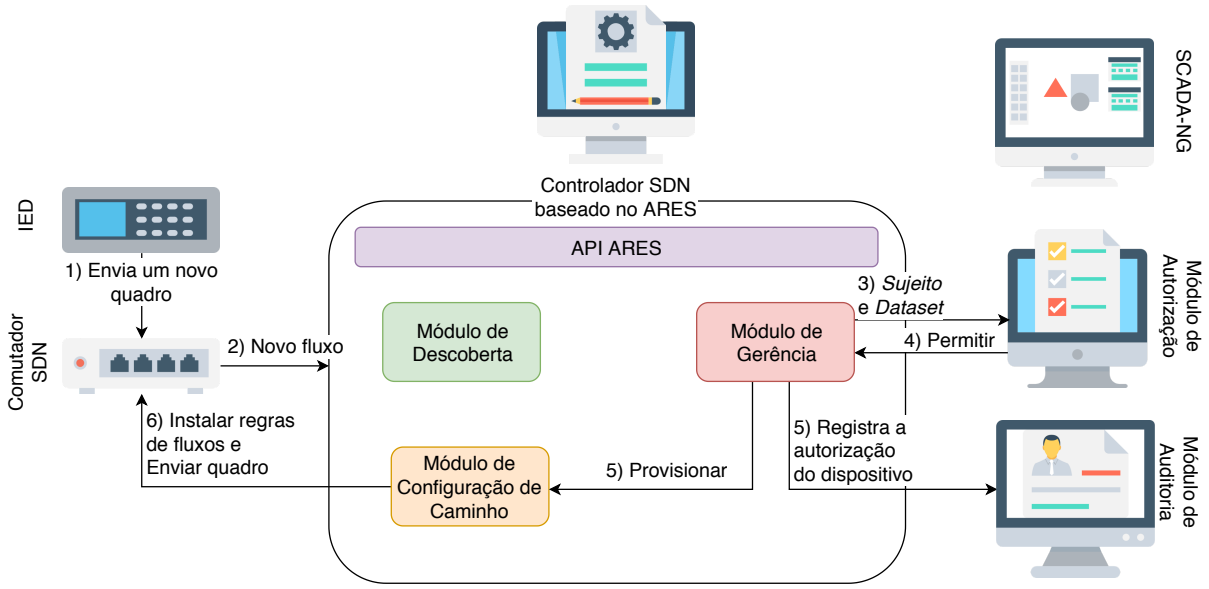


Figura 4.6: Processo de autorização de instalação de fluxos para controle de acesso reativo.

de gerência traduz as informações do IED para solicitações de acesso e envia ao ABAC (4). Após validar a solicitação, o ABAC informa ao módulo de gerência que a solicitação foi autorizada (5). Então, o módulo de gerência muda o estado do IED para `autorizado`, faz o registro da autenticação e autorização bem sucedida e solicita o provisionamento para o módulo de configuração de caminho (6). Finalmente, o módulo de configuração de caminho instala proativamente as regras de fluxos que serão utilizadas pelo IED e o controlador SDN informa ao SCADA-NG a descoberta de um novo IED (7), resolvendo o problema de escalabilidade conforme explicado em [46].

De forma análoga, caso falhe algum dos passos descritos anteriormente, seja no controle de acesso reativo ou proativo, o controlador SDN deverá registrar o evento de falha e instalar regras de fluxos que impeçam a comunicação do IED na rede de comunicação. Uma solicitação de acesso negada deve ser vista como um possível ataque à rede ou um erro de configuração no IED. Ambos os casos podem trazer prejuízos à rede [37] e devem ser notificados ao operador para averiguação.

Finalmente, o 3AS também possui o registro de eventos de desconexão, como mostrado na Figura 4.8. Após um IED se desconectar da rede de comunicação, um veículo elétrico por exemplo, o nó de autenticação informa ao controlador SDN (1) que inicia o processo de desinstalação das regras de fluxos associadas àquele IED (2). O módulo de gerência ARES solicita o *desprovisionamento* das regras de fluxos associadas ao IED (3). Em seguida, o módulo de configuração de caminho ARES desinstala as regras associadas ao IED (4), impossibilitando que o dispositivo continue se comunicando na rede, e coleta as

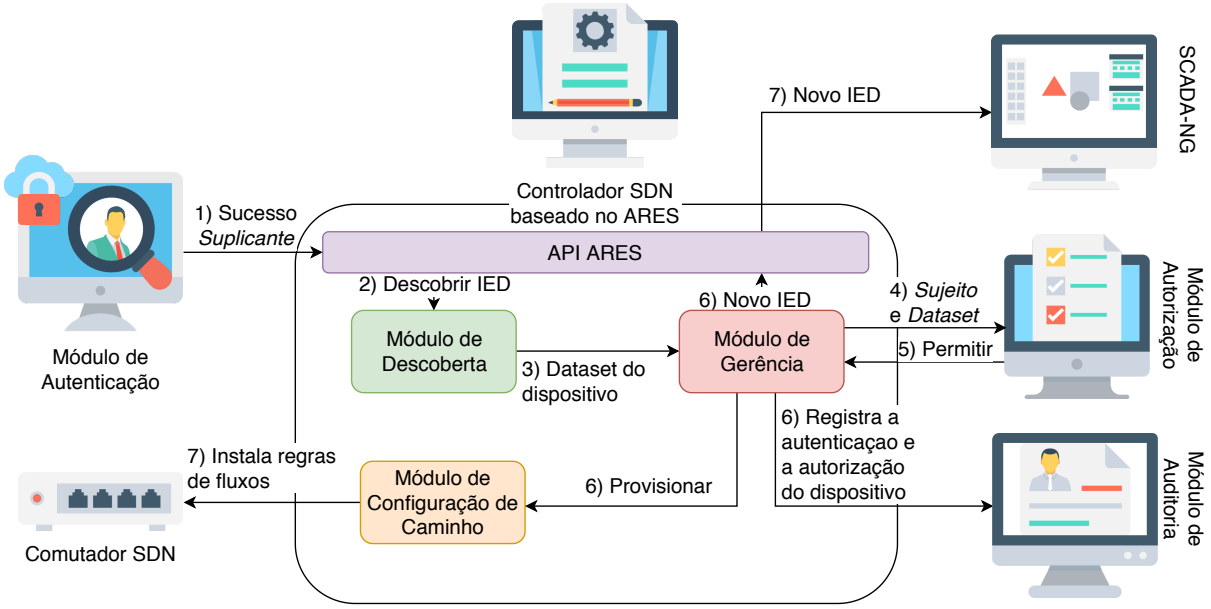


Figura 4.7: Processo de autorização de instalação de fluxos para controle de acesso proativo.

informações dos fluxos desinstalados (5), como a quantidade de quadros e tamanho das mensagens encaminhadas por essas regras. Então, o módulo de configuração de caminho repassa as informações ao módulo de gerência (6), que finalmente registra a desconexão do IED e os recursos de rede utilizados por ele.

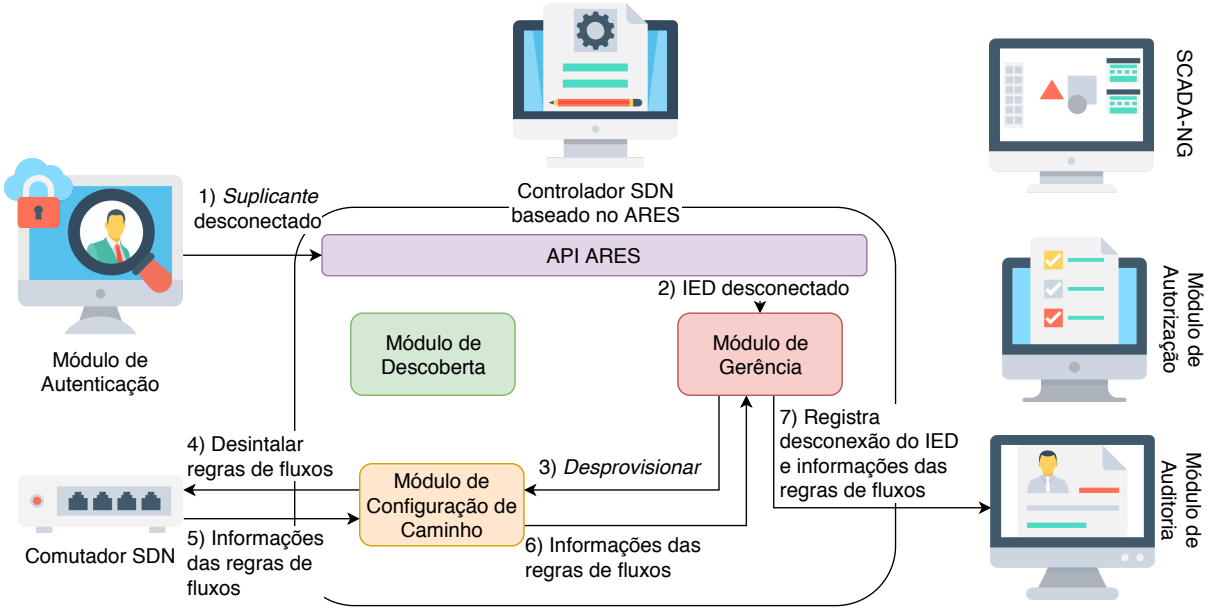


Figura 4.8: Processo de desconexão de IEDs.

Os passos (5) até (7) podem ser repetidos periodicamente para manter o registro constante dos eventos ocorridos na rede de comunicação.

4.5 SCADA *Next Generation*

O *Supervisory Control and Data Acquisition* de Nova Geração (SCADA-NG) é o sistema supervisório responsável por supervisionar e controlar os dispositivos da rede elétrica, sejam estes IEDs – e qualquer equipamento conectado a eles – ou comutadores da rede de comunicação. Sempre que um novo IED é autenticado e autorizado, o controlador SDN informa ao SCADA-NG para que este possa se conectar automaticamente ao IED e começar a supervisioná-lo (passo 7 da Figura 4.7). Esse é um grande diferencial do ARES, que permite a configuração da rede de comunicação que dá suporte a rede elétrica inteligente de maneira dinâmica. Outra característica é que essa solução elimina a necessidade do sistema supervisório conhecer previamente o local e o momento em que o dispositivo irá se conectar ao sistema elétrico, que seria um problema de escalabilidade em um cenário com veículos elétricos se conectando à rede de forma dinâmica [46].

Conforme descrito nos requisitos para implantação do 3AS, deve-se criar uma base de dados contendo a identidade e autorização de cada IED do sistema elétrico. Uma forma de facilitar a gerência dinâmica dos veículos elétricos seria através da utilização de estações de recarga. Dessa forma, a empresa responsável pela distribuição de energia teria conhecimento das suas próprias estações de recarga, e as autorizações de cada uma dessas estações. Assim, o motorista do veículo elétrico poderia cadastrar apenas uma credencial através de um sistema fornecido pela empresa de distribuição para ser cobrado devidamente. Logo, o veículo elétrico faria a autenticação através da estação de recarga, enquanto a autorização seria feita de acordo com as ações que a estação de recarga está autorizado a executar.

A Figura 4.9 apresenta a sequência de eventos para o registro periódico do estado da rede elétrica inteligente, através dos dados de cada IED supervisionado. Através da API do ARES, o SCADA-NG mantém uma comunicação regularmente com o controlador SDN para solicitar o registro de relatórios atualizados sobre o estado da rede elétrica (1). Em sequência, a API solicita o registro para módulo de gerência que envia as informações para o nó de auditoria.

A criação de novas políticas e introdução de novas identidades poderá ser feita de diversos modos: criação manual pelos operadores diretamente na interface do SCADA-NG; importação de arquivos de configuração, como por exemplo o SCL [16], para criar identidades e políticas de acesso de forma automatizada; ou até mesmo os próprios motoristas poderão cadastrar um usuário e senha em uma página *web* disponibilizada pela companhia

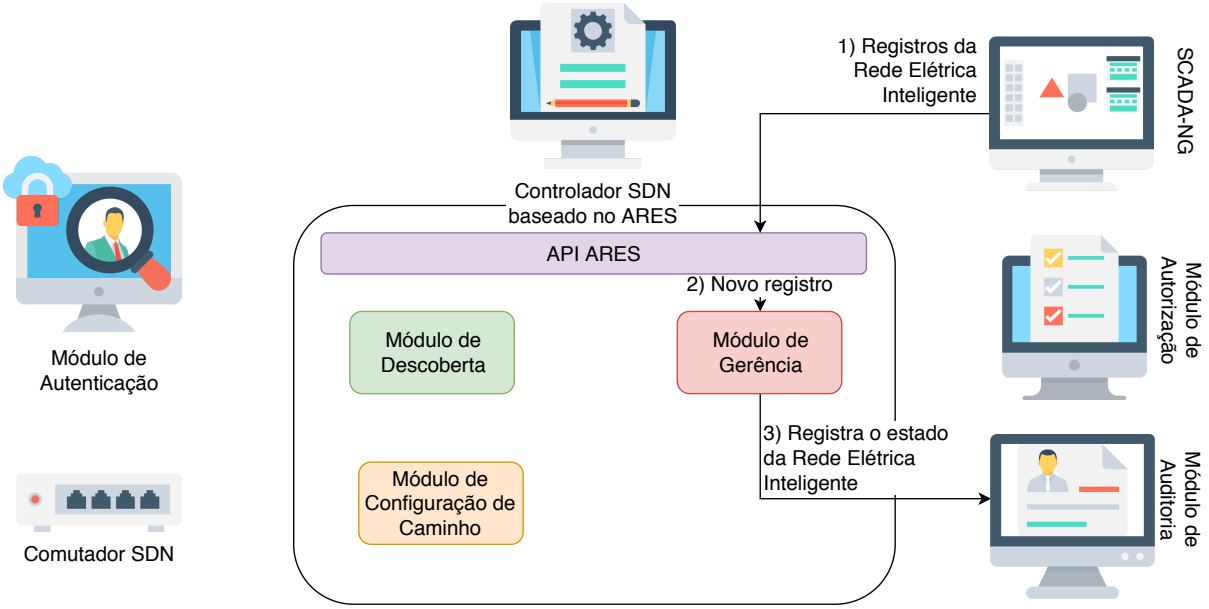


Figura 4.9: Processo de registro do estado da rede elétrica inteligente.

elétrica, e em seguida efetuar o *login* na rede de comunicação como se estivesse associando seu celular a uma rede sem-fio. Ao conectar seu veículo elétrico na tomada de uma estação de recarga, o usuário poderá digitar suas credenciais para efetuar a autenticação e assim poder recarregar seu veículo.

4.6 Modelo de Atacante

Possíveis ataques devem ser considerados para a avaliação do 3AS. Em [1], os autores definem alguns ataques como:

- Ataque passivo, quando o atacante obtém informações sobre a rede de comunicação sem impactar o funcionamento da mesma;
- Ataque ativo, quando o atacante modifica o comportamento, ou o desempenho, da rede de comunicação;
- Ataque interno, originado de dentro da rede de comunicação, ou seja, quando o atacante possui acesso legítimo;
- Ataque externo, originado de fora da rede de comunicação, ou seja, quando o atacante adquire acesso ilegal.

Para que um atacante externo consiga acesso à rede, ele deverá obter a credencial de um IED e garantir que o dispositivo não esteja conectado na rede de comunicação, uma

vez que o 3AS permite apenas uma conexão ativa por identidade. Após autenticado, o atacante deverá implementar o envio de mensagens MMS equivalentes aos atributos do IED, pois o 3AS só permite a comunicação se os atributos do IED forem compatíveis com as registradas no banco de dados. Assumindo que o atacante tem acesso físico ao IED e suas informações, como credenciais e atributos MMS, ainda assim o atacante ficará limitado ao acesso que o IED comprometido possui, limitando assim as ações do atacante.

Portanto, os IEDs e suas informações como credenciais e atributos MMS devem ser devidamente protegidas por cada entidade que tem acesso ao sistema. O 3AS não lida com casos de roubo de certificados ou de senha, o que demandaria métodos para detecção de atacantes.

Como dito anteriormente, assumindo que um IED interno foi comprometido, suas ações serão limitadas. Por exemplo, em [24] os autores propõem um ataque de homem no meio onde um dispositivo interno comprometido consegue interceptar uma comunicação MMS insegura e afetar o comportamento da rede elétrica. O ataque proposto acontece em três etapas. Primeiro é feito um ataque passivo, onde o dispositivo comprometido captura o tráfego MMS entre um IED e o sistema supervisório para conhecer ambos os endereços IPs. Essa primeira parte seria prevenida nativamente pelo 3AS, uma vez que o tráfego MMS seria entregue apenas às duas pontas da comunicação, o IED legítimo e sistema supervisório, logo o dispositivo comprometido não conseguiria capturar o tráfego MMS.

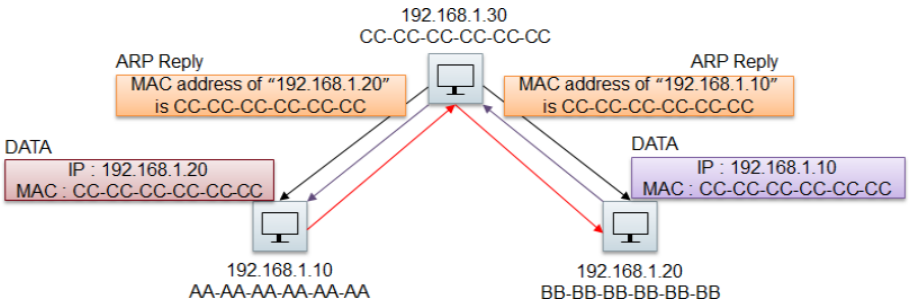


Figura 4.10: Técnica de ARP *poisoning* [24].

Assumindo que o atacante conhece o endereço IP do sistema supervisório e de um IED legítimo, o segundo ataque ocorre através da técnica de *Address Resolution Protocol* (ARP) *poisoning*. Resumidamente, o atacante envia pacotes ARP falsos, de forma que o sistema supervisório identifique o atacante como o IED legítimo, e o IED legítimo identifique o atacante como sistema supervisório. Logo, o atacante fica no meio da comunicação entre o IED legítimo e o sistema supervisório de forma transparente para ambos, como pode ser visto na Figura 4.10. Esse segundo ataque também seria impossibilitado

pelo 3AS uma vez que o dispositivo comprometido não possuiria acesso para envio de pacotes ARP com endereços diferentes dos permitidos para o dispositivo comprometido.

Por fim, a terceira etapa do ataque ocorre da seguinte forma: (1) o sistema supervisório inicia uma conexão MMS com o dispositivo comprometido supondo que este é o IED legítimo; em seguida (2), o dispositivo comprometido inicia uma conexão MMS com o IED legítimo, que é aceita pelo IED pois este supõe que o dispositivo comprometido é de fato o sistema supervisório; por fim (3), todo o tráfego entre o IED legítimo e o sistema supervisório é mediado pelo dispositivo comprometido, assim, este possui o poder de ler as mensagens enviadas, alterar, e até mesmo não retransmitir. Esta terceira etapa também seria bloqueada pelo 3AS pois o dispositivo comprometido não teria acesso para se comunicar através de MMS com o IED legítimo.

Concluindo, o 3AS estende o módulo de gerência do ARES para se comunicar com o mecanismo de autenticação e o ABAC. O mecanismo de autenticação é baseado no protocolo IEEE 802.1X, comunica-se com o ARES para informar o resultado das autenticações. Já o mecanismo de autorização é baseado no protocolo MMS, onde o ARES obtém as ações requisitadas pelo IED e verificar com as políticas cadastradas no modelo ABAC. Através do AAA proposto pelo 3AS, a rede elétrica inteligente passa a atender aos requisitos de autenticação, identificando cada IED, de autorização, permitindo acesso apenas ao necessário para cada IED, e de auditoria, registrando os eventos na rede de comunicação e ações efetuadas por cada IED.

Capítulo 5

Análise do 3AS

Diversos experimentos emulados foram executados para avaliar a efetividade da proposta desta dissertação. O mecanismo de autenticação foi avaliado através da: latência em um cenário com diversos dispositivos se autenticando ao mesmo tempo; e carga de controle gerada pelo processo de autenticação, comparando com a proposta do *Resonance* [39]. O controle de acesso e o registro dos eventos da rede de comunicação foram avaliados através de um cenário com dois IEDs, onde um atua como publicador GOOSE e outro como assinante (recebedor) GOOSE.

5.1 Ambiente de Testes

Para validar o 3AS, a proposta foi implementada e avaliada em cenários emulados através do Mininet[1]. O Mininet v2.2.2 é uma ferramenta de emulação de redes definidas por *software*, que virtualiza comutadores SDN através do Open vSwitch[2] v2.9.2 e permite a interligação desses comutadores virtualizados com um controlador SDN. A Figura 5.1 apresenta a topologia dos experimentos e as diversas ferramentas utilizadas. Os experimentos foram executados em uma máquina Ubuntu[3] v18.04 virtualizada através do VirtualBox[4] v5.2.32, com processador Intel® Core™ i7-8700 e 16 GBytes de memória RAM.

O nó de autenticação foi configurado com um autenticador e um servidor de autenticação. O autenticador utilizado foi o hostapd[5] v2.7, modificado para informar os resultados

[1]Disponível em mininet.org.
[2]Disponível em openvswitch.org.
[3]Disponível em ubuntu.com.
[4]Disponível em virtualbox.org.
[5]Disponível em github.com/arthurazs/sdn-hostapd.

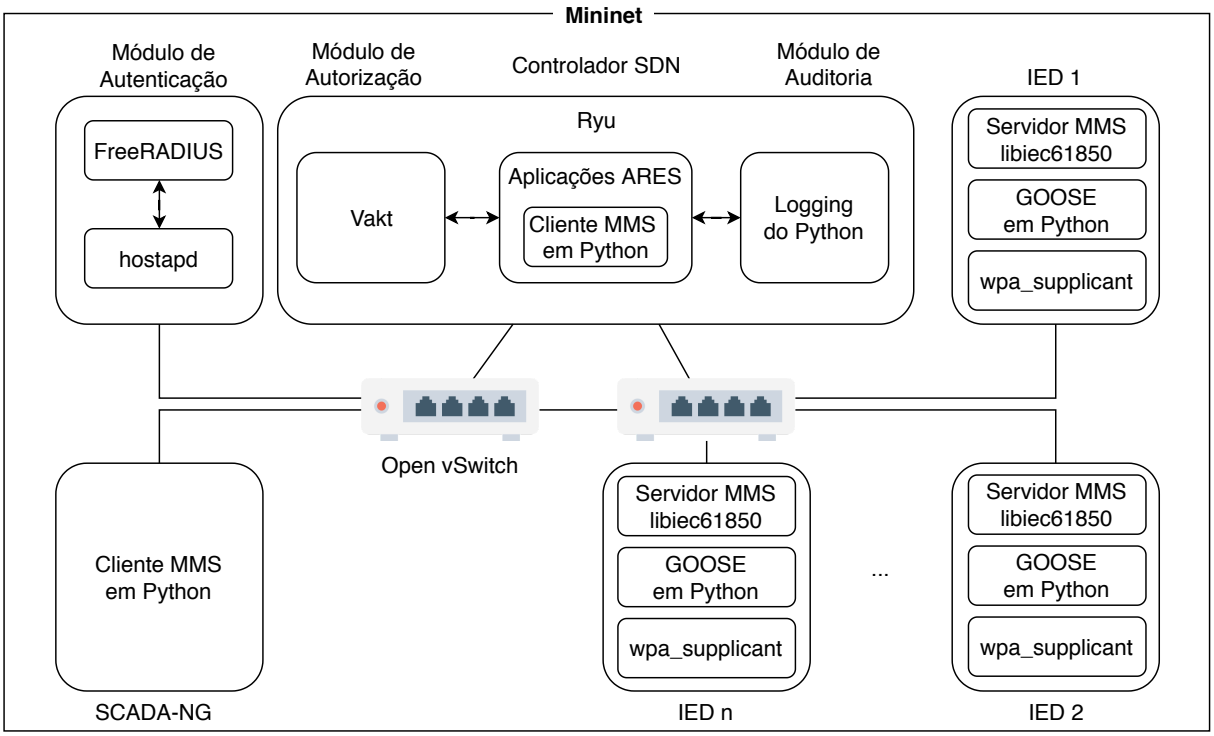


Figura 5.1: Topologia dos experimentos contendo o SCADA-NG e Nó de Autenticação conectados a um comutador SDN e um número variável de IEDs conectados a outro comutador SDN.

das autenticações ao controlador através da API ARES. O servidor de autenticação utilizado foi o FreeRADIUS[6] v3.0.16.

Uma das contribuições desta dissertação é uma implementação parcial do *framework* ARES[7] em cima do controlador Ryu[8] v4.32. O Ryu é um controlador SDN implementado em Python e amplamente utilizado pelo meio acadêmico para validação de propostas SDN [5, 25, 3]. O plano de controle ARES se comunica com o autenticador através da API ARES, implementada em *Representational State Transfer* (REST). Foi utilizada a biblioteca Vakt[9] v1.2.1 para efetuar o controle de acesso baseado em atributos. Como registro de eventos, foi utilizada a própria biblioteca de registro de eventos do python chamada logging[10].

Para simular os IEDs, ou servidores MMS, foi utilizada a biblioteca libiec61850[11] v1.3.3 que permite a emulação do comportamento de um IED. O Ryu, o plano de controle ARES, o cliente MMS, o controle de acesso e o sistema de registro de eventos foram desenvolvidos

[6]Disponível em freeradius.org.
[7]Disponível em bit.ly/3AS_ARES.
[8]Disponível em osrg.github.io/ryu.
[9]Disponível em github.com/kolotaev/vakt.
[10]Disponível em docs.python.org/3/library/logging.html.
[11]Disponível em libiec61850.com/libiec61850.

com a linguagem Python. O cliente MMS foi utilizado tanto no plano de controle ARES para obtenção do *dataset* dos IEDs, quanto para atuar como SCADA-NG. Também foi desenvolvido um gerador genérico de quadros GOOSE para que o IED possa atuar como publicador. Os IEDs também foram configurados com wpa_supplicant[12] v2.6 para atuar como suplicante IEEE 802.1X e poder autenticar-se na rede SDN.

5.2 Experimentos

Diversos experimentos foram executados para avaliar a efetividade do 3AS. Primeiramente, foi avaliado o mecanismo de autenticação em um cenário com múltiplos veículos elétricos autenticando ao mesmo tempo [46] e, em seguida, foram avaliados o controle de acesso e o registro dos eventos da rede de comunicação.

5.2.1 Autenticação: Comportamento

O primeiro experimento valida o comportamento do mecanismo de autenticação com um veículo elétrico autenticando-se na rede de comunicação utilizando usuário e senha através do modelo EAP-PEAP para solicitar a recarga de sua bateria. A topologia do cenário deste experimento pode ser vista na Figura 5.2.

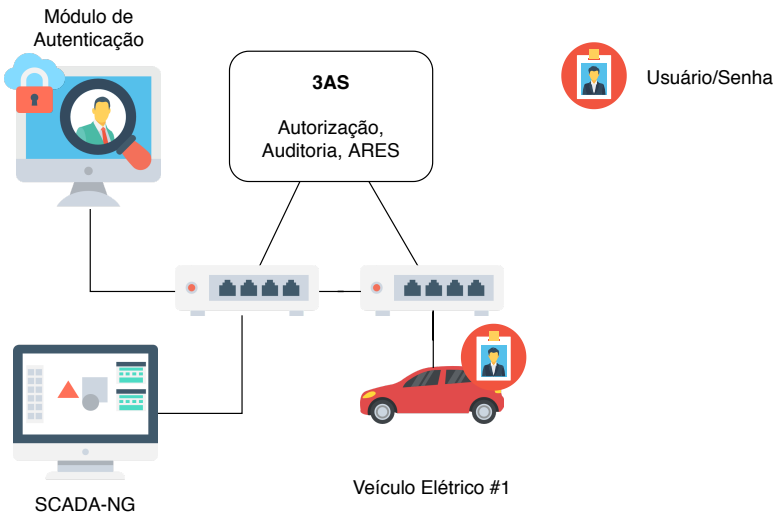


Figura 5.2: Topologia do primeiro cenário onde um veículo elétrico autentica-se na rede de comunicação através de usuário e senha para solicitar a recarga de sua bateria.

A Figura 5.3 mostra a sequência de eventos desde o início do processo de autenticação até a liberação da função de recarga no veículo elétrico. O processo de autenticação inicia

[12]Disponível em w1.fi/wpa_supplicant.

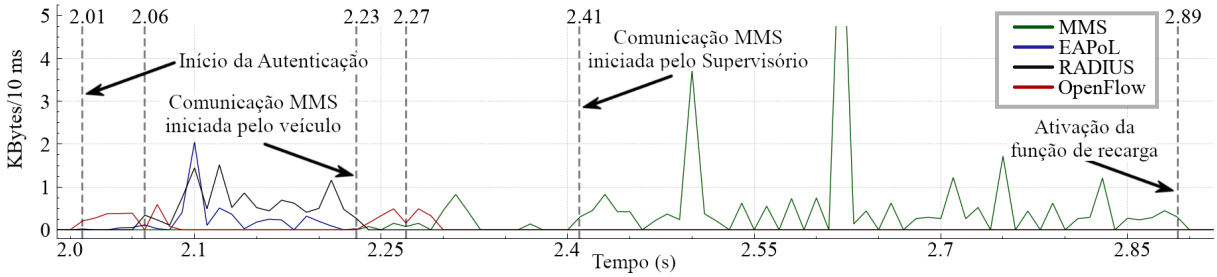


Figura 5.3: Sequência de eventos para o processo de autenticação e comunicação MMS. O mecanismo gera tráfego OpenFlow no início para instalar as regras de fluxos para permitir a autenticação IEEE 802.1X. A comunicação MMS inicia somente após o término do processo de autenticação[13].

em 2,01 segundos, seguido por pacotes OpenFlow solicitando a instalação de regras de fluxos do suplicante para o autenticador. O controlador SDN instala os fluxos necessários para que os comutadores SDN possam encaminhar automaticamente o restante dos quadros de autenticação. Em 2,06 segundos, há outro tráfego OpenFlow para instalar o caminho de volta do autenticador para o suplicante. Assim que o veículo termina a autenticação (2,23 segundos representado pelo fim do tráfego EAPoL), o veículo inicia sua conexão com o SCADA-NG através do protocolo MMS. Como resultado, o comutador SDN envia um novo pacote OpenFlow para o controlador SDN, solicitando a instalação de regras de fluxo para a comunicação MMS. Em seguida, o controlador verifica que o veículo está autenticado e instala as regras de fluxos necessárias para a comunicação MMS do veículo para o SCADA-NG. Em 2,27 segundos, o SCADA-NG envia a primeira resposta à solicitação de conexão do veículo, gerando um novo tráfego OpenFlow para a instalação do caminho de volta, do SCADA-NG para o veículo elétrico. O restante da comunicação MMS segue sem tráfego OpenFlow, pois todos os fluxos necessários já foram instalados reativamente. Finalmente, depois de fazer a leitura (`MMS.Read`) dos dados do veículo elétrico, o SCADA-NG envia uma mensagem para o veículo (`MMS.Write`), ativando sua função de recarga aos 2,89 segundos, concluindo o experimento com um tempo total entre o início da autenticação até a liberação de função de recarga inferior a 1 segundo.

5.2.2 Autenticação: Carga de Controle e Latência

O segundo experimento analisa a carga de controle gerada durante a autenticação de veículos elétricos, através do modelo EAP-PEAP, e avalia a progressão do tempo de autenticação, alterando o número de veículos elétricos que se autenticam ao mesmo tempo,

[13]Para um melhor entendimento do comportamento do mecanismo de autenticação, ver: youtu.be/kmi3gL3Qzxc?t=55.

com intervalo de confiança de 95%. A topologia do cenário deste experimento pode ser vista na Figura 5.4.

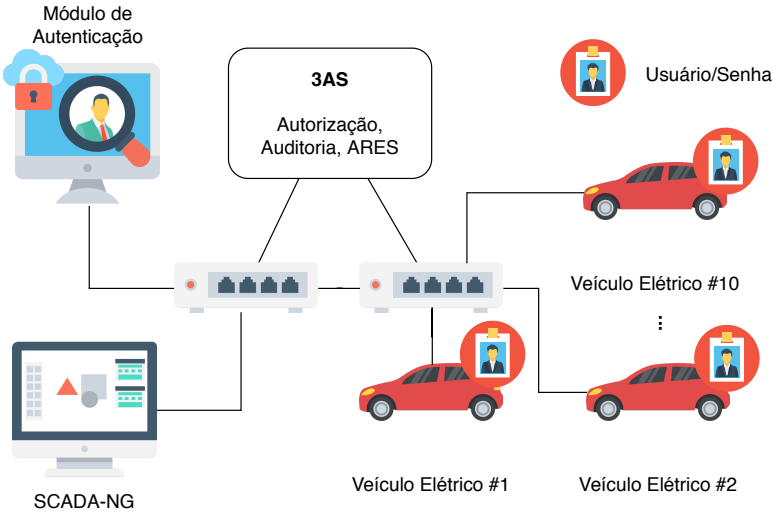
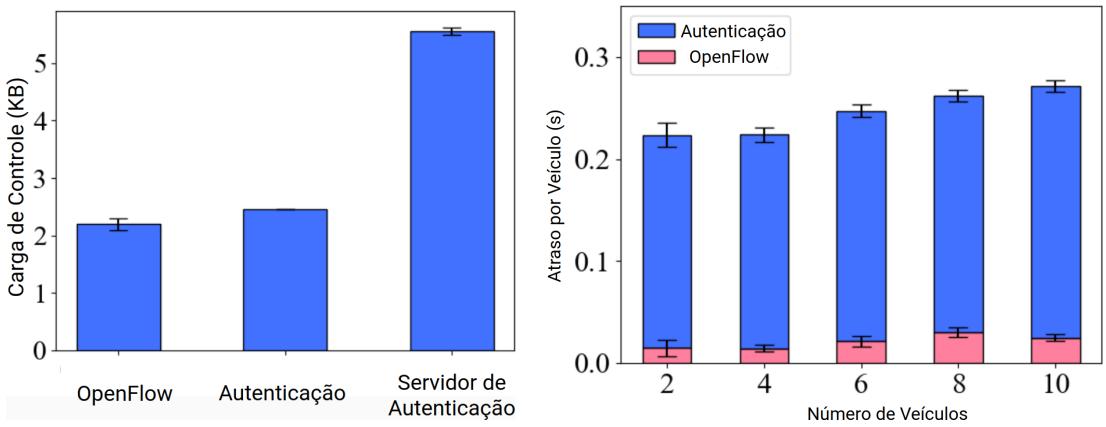


Figura 5.4: Topologia do segundo cenário onde veículos elétricos autenticam-se na rede de comunicação através de usuário e senha. O número de veículos elétricos autenticando-se ao mesmo tempo é alternado para avaliar a progressão da latência do mecanismo de autenticação.



(a) Carga de controle gerada pelo processo de autenticação de um veículo elétrico.

(b) Atraso introduzido pelo processo de autenticação por número de veículos elétricos autenticando ao mesmo tempo.

Figura 5.5: Experimentos para validação da eficiência do mecanismo de autenticação.

A Figura 5.5(a) demonstra que o tráfego OpenFlow e EAPoL tem uma carga de controle de 2,20 KBytes e 2,45 KBytes, respectivamente. Caso o autenticador (hostapd) e o servidor de autenticação (FreeRADIUS) estivessem em máquinas diferentes, o tráfego RADIUS entre eles adicionaria 5,56 KBytes de carga de controle, além da carga extra do OpenFlow para a instalação das regras de fluxos referentes ao tráfego RADIUS na rede

SDN. Como o hostapd e o FreeRADIUS estão na mesma máquina, essa carga de controle é desconsiderada[14]. Portanto, a carga de controle gerada pelo processo de autenticação nesse cenário é de apenas 4,65 KBytes.

Alterando o número de veículos elétricos que se autenticam ao mesmo tempo, é possível analisar a progressão do tempo de autenticação. Este experimento leva em consideração o número de veículos elétricos que podem estar conectados ao mesmo tempo em uma única estação de recarga, variando de dois[15] a dez[16] conectores por estação de recarga. A latência é medida do início do processo de autenticação até o pedido de conexão enviado pelo veículo elétrico. A Figura 5.5(b) revela que mesmo com dez veículos se autenticando ao mesmo tempo, o atraso introduzido pela autenticação para cada dispositivo apresentou um tempo similar, aumentando apenas 18.18%, de 209 milissegundos para 247 milissegundos, permanecendo abaixo de 250 milissegundos em todos os testes. O atraso do OpenFlow foi ainda menor, apresentando tempos abaixo de 25 milissegundos para cada veículo. O tempo total, considerando a autenticação mais a instalação das regras de fluxos de maneira reativa, variou entre 223 milissegundos e 271 milissegundos, para dois veículos e para dez veículos, respectivamente.

5.2.3 Autenticação: Comparação

O terceiro experimento compara a carga de controle gerada pela autenticação através da proposta desta dissertação (IEEE 802.1X), utilizando o modelo EAP-PEAP, com a autenticação através de um *captive portal* (HTTP) proposto por Resonance [39]. A topologia do cenário deste experimento é o mesmo da Seção 5.2.1, onde um veículo elétrico autentica-se utilizando usuário e senha, e pode ser vista na Figura 5.2. É importante que mecanismos introduzidos na rede elétrica inteligente gerem baixa carga de controle para evitar possíveis congestionamentos na rede de comunicação. Quanto mais bits trafegam na rede, mais difícil fica garantir requisitos temporais conforme normatizado pela parte 5 da IEC 61850 [17].

Neste experimento foi utilizado o CapFlow[17], um *captive portal* simples para SDN

[14] É importante notar que o tráfego RADIUS também pode ser desconsiderado caso o servidor de autenticação esteja em uma máquina separada, mas diretamente conectada ao hostapd, sem enviar tráfego para a rede SDN.

[15] "Terra HP Chargers"com dois conectores. Notícia retirada do site: insideevs.com/here-are-the-350-kw-nad-150-kw-abb-chargers-for-electrify-america. Acesso em: fev. 2019.

[16] "Cada estação de recarga pode atender entre cinco e dez veículos ao mesmo tempo". Notícia retirada do site: asia.nikkei.com/Business/India-s-Tata-to-build-1-000-electric-vehicle-charging-spots. Acesso em: fev. 2019.

[17] Disponível em github.com/ederlf/CapFlow.

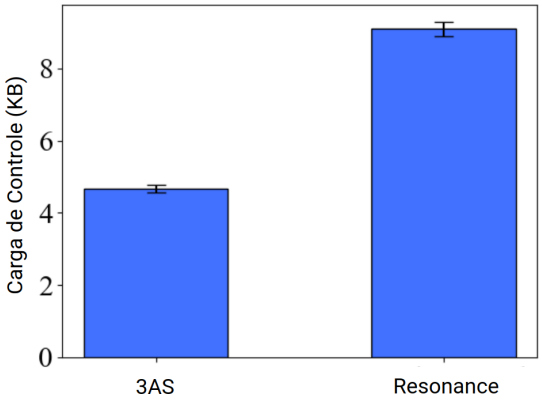


Figura 5.6: Comparação da carga de controle gerada entre a autenticação por IEEE 802.1X e *Captive Portal*.

desenvolvido para o controlador Ryu. A Figura 5.6 apresenta a diferença de carga de controle gerada por ambas as propostas. As duas propostas apresentaram pequena variação nos experimentos, 2,27% para a autenticação IEEE 802.1X e 2,20% para a solução com *captive portal*. Como o IEEE 802.1X opera sobre a camada de enlace, sua carga de controle é 48,84% menor do que a do *captive portal*, que opera sobre a camada de transporte (TCP/IP).

5.2.4 Autenticação: Credenciais

Como explicado na Seção 2.2, o protocolo IEEE 802.1X permite a autenticação através de diferentes modelos, como o EAP-PEAP visto nos experimentos anteriores. O modelo EAP-PEAP utiliza usuário e senha para efetuar a autenticação. Esse modelo faz sentido no cenário de veículos elétricos, onde o motorista pode fazer o cadastro da sua conta em um serviço provido pela companhia elétrica, e em seguida efetuar seu *login* no terminal da estação de recarga. Entretanto, este cenário não faz sentido em cenários de teleproteção, onde os próprios IEDs irão se autenticar. Para este cenário de dispositivos autônomos, o modelo EAP-TLS é mais indicado por utilizar certificados para efetuar a autenticação. A topologia do cenário deste experimento pode ser vista na Figura 5.7.

O quarto experimento, portanto, avalia o atraso e a sobrecarga de controle gerados pela autenticação e autorização utilizando os diferentes modelos de autenticação. A Figura 5.8 apresenta a comparação entre a autenticação e autorização utilizando login/senha e utilizando certificados, com intervalo de confiança de 95%. A Figura 5.8(a) não possui barra de erro pois o processo de autenticação é sempre o mesmo e não apresenta variação no tamanho dos quadros enviados. A utilização de certificados apresenta um aumento de aproximadamente 50,59% na quantidade de bytes enviados. Entretanto, o atraso ge-

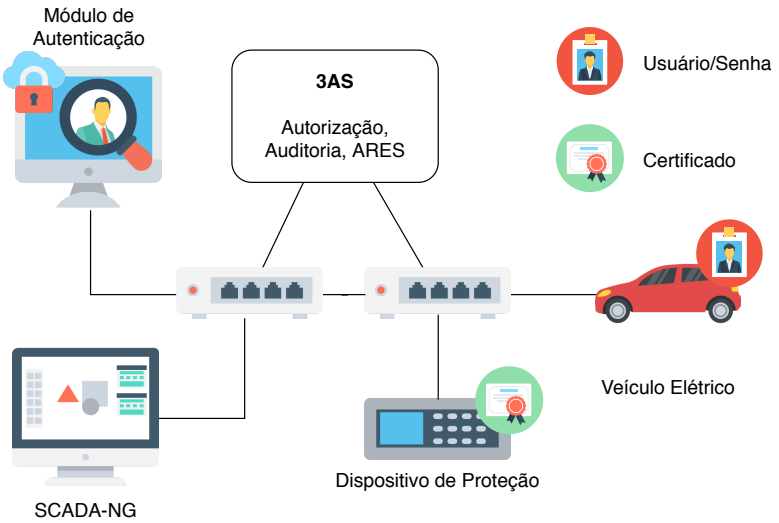
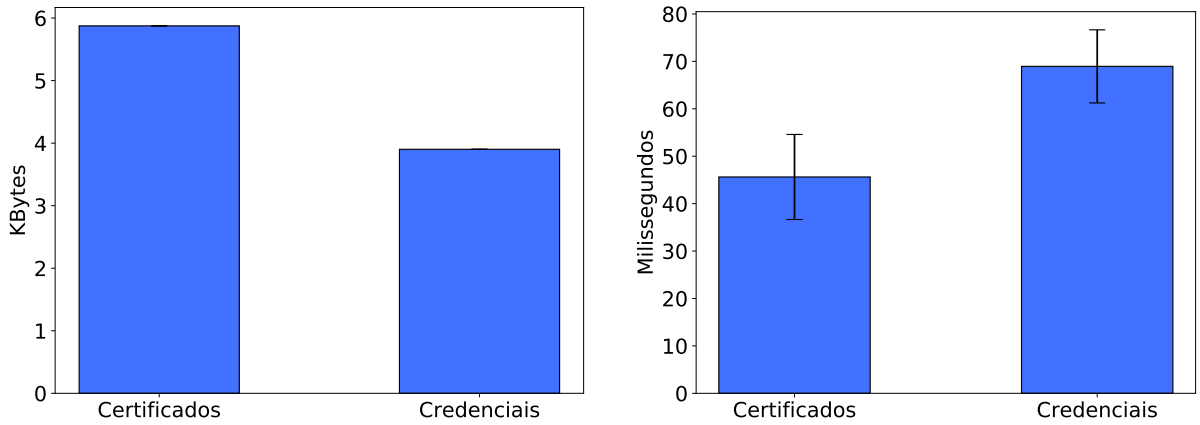


Figura 5.7: Topologia do terceiro cenário onde veículos elétricos autenticam-se na rede de comunicação através de usuário e senha e dispositivos de proteção autenticam-se através de certificados.

rado pela utilização de certificado apresenta uma melhora de aproximadamente 51,13%, conforme pode ser visualizado na Figura 5.8(b).



(a) Comparação entre a carga de controle gerada pela utilização de credencial e pela utilização de certificado.

(b) Comparação entre o atraso gerado pela utilização de credencial e pela utilização de certificado.

Figura 5.8: Comparação entre a utilização de credencial e certificado.

A melhora no tempo de autenticação e autorização se dá através do maior número de troca de mensagens no modelo EAP-PEAP (credencial). Enquanto no modelo EAP-PEAP o suplicante deve resolver uma série de desafios enviados pelo servidor de autenticação (Figura 5.9), no modelo EAP-TLS o suplicante efetua apenas a troca de certificados com o servidor de autenticação (Figura 5.10), explicando a melhora no tempo de autenticação.

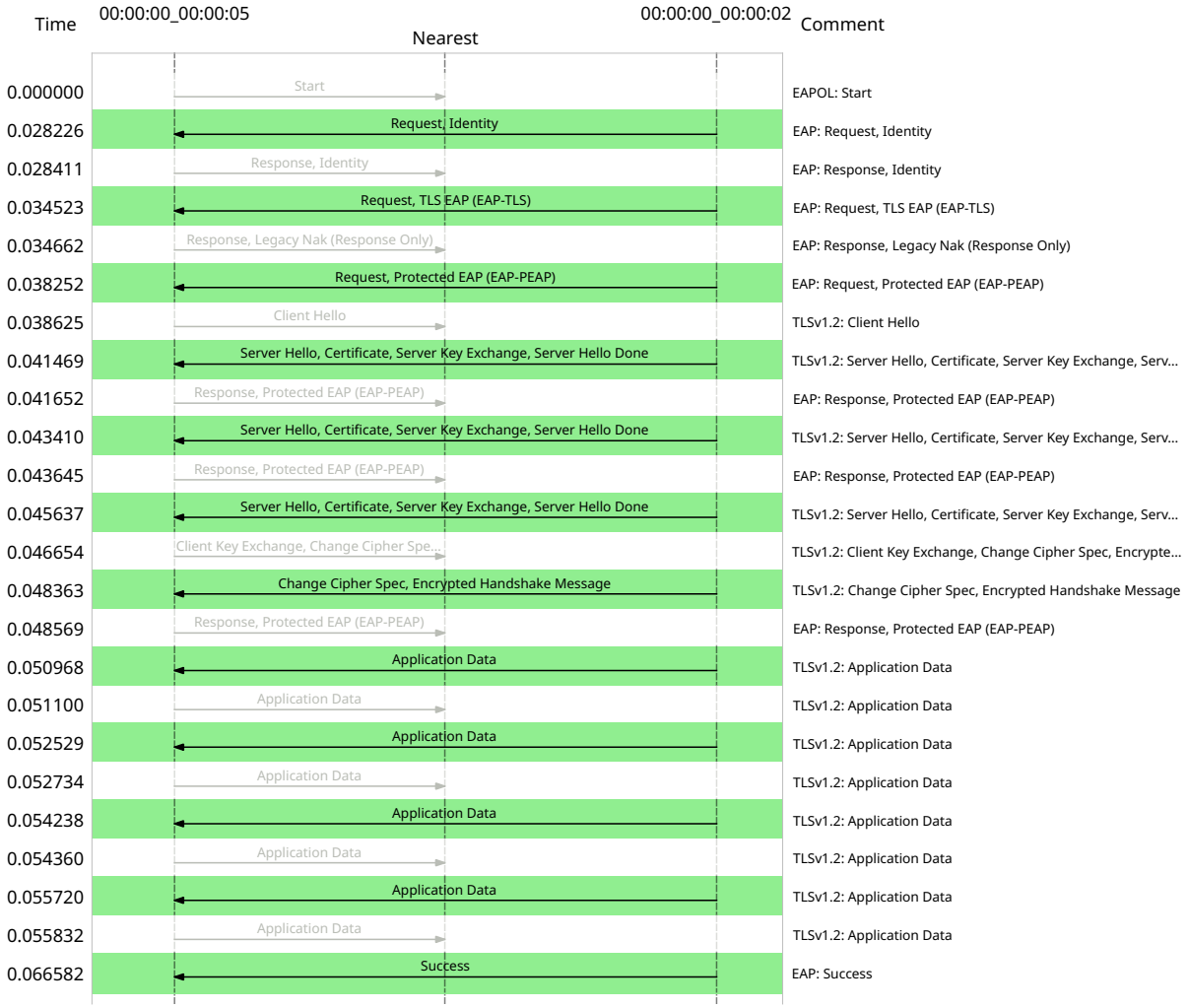


Figura 5.9: Sequência de eventos para a autenticação por credencial (EAP-PEAP).

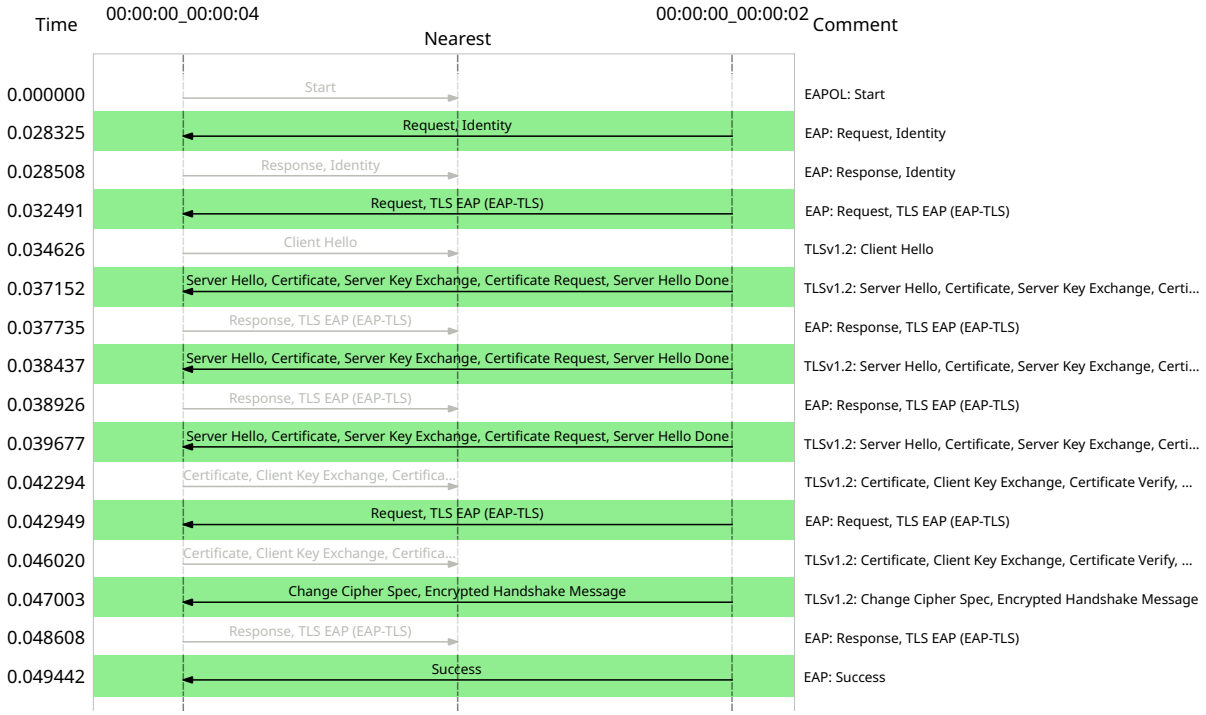


Figura 5.10: Sequência de eventos para a autenticação por certificado (EAP-TLS).

5.2.5 Autorização: Proativa x Reativa

O quinto experimento compara a latência entre o controle de acesso proativo, quando a autorização ocorre através do MMS logo após a autenticação, e reativo, quando a autorização ocorre apenas quando um novo fluxo é identificado pelo comutador SDN. Este experimento ocorre em um cenário de teleproteção, onde os IEDs de proteção autenticam-se através de certificados. Neste cenário, além da autenticação, ambos dispositivos passam pelo processo de autorização (proativo e reativo). Enquanto o IED 1 solicita acesso para publicar quadros GOOSE para o grupo 1 (`01:0c:cd:01:00:01`), o IED 2 solicita acesso para receber quadros GOOSE do grupo 1. A topologia desse cenário pode ser vista na Figura 5.11.

Este experimento é executado em duas partes e o gráfico gerado apresenta um intervalo de confiança de 95%. Na primeira parte, foi mensurado o atraso na entrega dos quadros GOOSE pela autorização proativa, enquanto na segunda parte foi mensurada o atraso na entrega dos quadros GOOSE pela autorização reativa. O experimento inicia com a autenticação de ambos os IEDs e após 10 segundos, o IED 1 inicia o envio de quadros GOOSE para o IED 2.

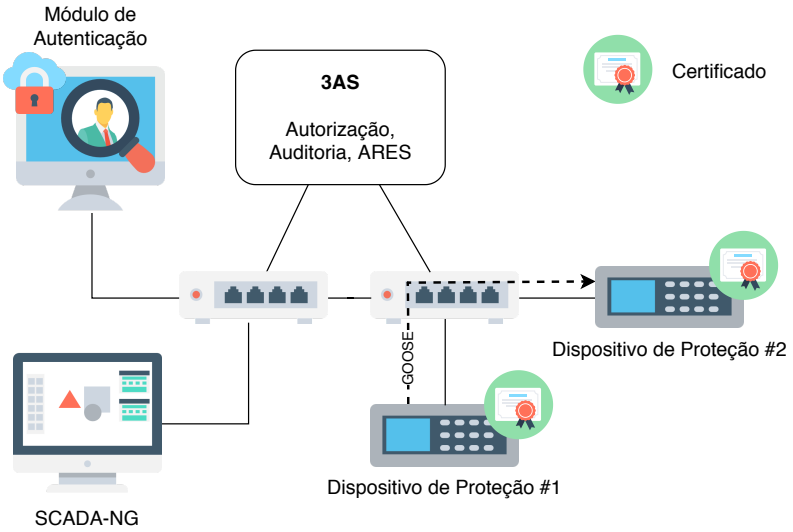


Figura 5.11: Topologia do quarto cenário onde dispositivos de proteção autenticam-se na rede de comunicação através de certificados e o dispositivo 1 publica quadros GOOSE para o dispositivo 2.

A Figura 5.12 apresenta a comparação entre o atraso da parte 1, onde a autorização proativa foi avaliada, e o atraso da parte 2, onde a autorização reativa foi avaliada. Como na autorização proativa as regras de fluxos são instaladas antes mesmos do primeiro envio de quadro GOOSE, o atraso de 0,27 milissegundos representa o tempo em que o comutador leva para processar o quadro GOOSE e comutar para a porta correta, conforme a regra previamente instalada.

Na autorização reativa, o atraso de 3,75 milissegundos ocorre pois o comutador não possui nenhuma regra de fluxo referente aquele quadro GOOSE. Portanto, o comutador envia uma requisição ao controlador SDN, que em sequência comunica-se com o controle de acesso para verificar se esse fluxo é permitido. Por fim, o controlador SDN responde à requisição do comutador e permite o envio do quadro GOOSE.

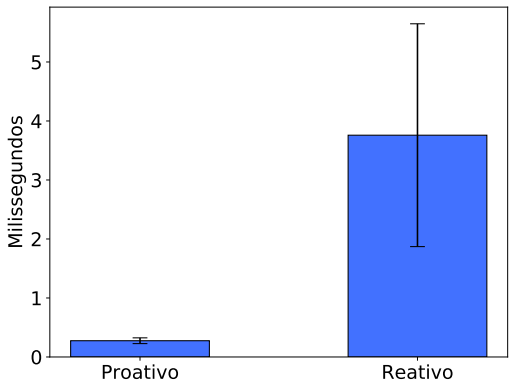


Figura 5.12: Comparação entre o atraso gerado pela autorização proativa e autorização reativa.

Esse atraso ocorre apenas para o primeiro pacote, seja para autorização proativa ou reativa, pois após a instalação da regra de fluxo, todos os quadros seguintes corresponderão à regra de fluxo já instalada. Consequentemente, todos os próximos pacotes terão latência equivalente à apresentada pela autorização proativa.

Conclui-se também, que para cenários de teleproteção, a autorização proativa faz-se necessária, uma vez que a autorização reativa gera uma latência maior que 3 milissegundos, tempo inaceitável de acordo com a parte 5 da norma IEC 61850 [17].

5.2.6 Autorização e Auditoria: Comportamento

O sexto experimento valida o funcionamento do controle de acesso e registro de eventos em um cenário de teleproteção. Este experimento utiliza o mesmo cenário da Seção 5.2.5, entretanto o processo de autorização é feito apenas de maneira proativa. A topologia desse cenário pode ser vista na Figura 5.11.

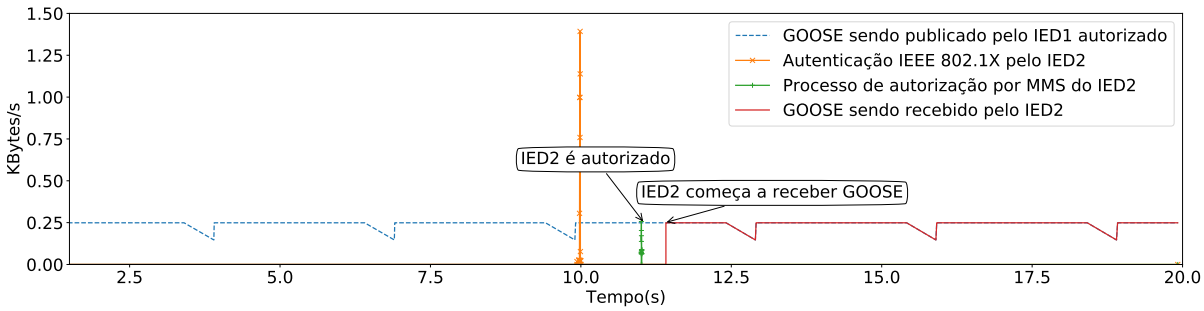


Figura 5.13: IED2 recebe os quadros GOOSE apenas após ser devidamente autenticado e autorizado.

Neste cenário, dois IEDs autenticam-se na rede SDN. Inicialmente, o `IED1` se autentica e solicita permissão para publicar quadros GOOSE para o endereço MAC *multicast* `01:0c:cd:01:00:01`. Após dez segundos, o `IED2` se autentica e solicita permissão para assinar (receber) quadros GOOSE do endereço MAC *multicast* `01:0c:cd:01:00:01`. Após ser autorizado, o `IED2` passa a receber os quadros GOOSE do MAC *multicast* `01:0c:cd:01:00:01`, conforme pode ser visto na Figura 5.13.

A Figura 5.14 apresenta a sequência de mensagens recebidas e enviadas pelo controlador SDN, que possui o endereço IP 10.0.0.1, durante o processo de autenticação e autorização. O autenticador, que tem o endereço IP 10.0.0.2, após confirmar a identidade do IED, envia uma requisição através da API ARES informando a autenticação do IED. Ao receber essa confirmação, o controlador SDN inicia uma conexão MMS com o IED para verificar quais ações estão sendo requisitados pelo dispositivo, por exemplo, publicar

quadros GOOSE para o endereço *multicast* `01:0c:cd:01:00:01`. Após obter essas informações através do `MMS.Read` (encapsulado no `confirmed-RequestPDU`), o controlador SDN pergunta ao Vakt (biblioteca ABAC) se o IED está autorizado. Após obter a confirmação do Vakt, o controlador SDN instala as devidas regras de fluxos proativamente e confirma a autorização ao autenticador.

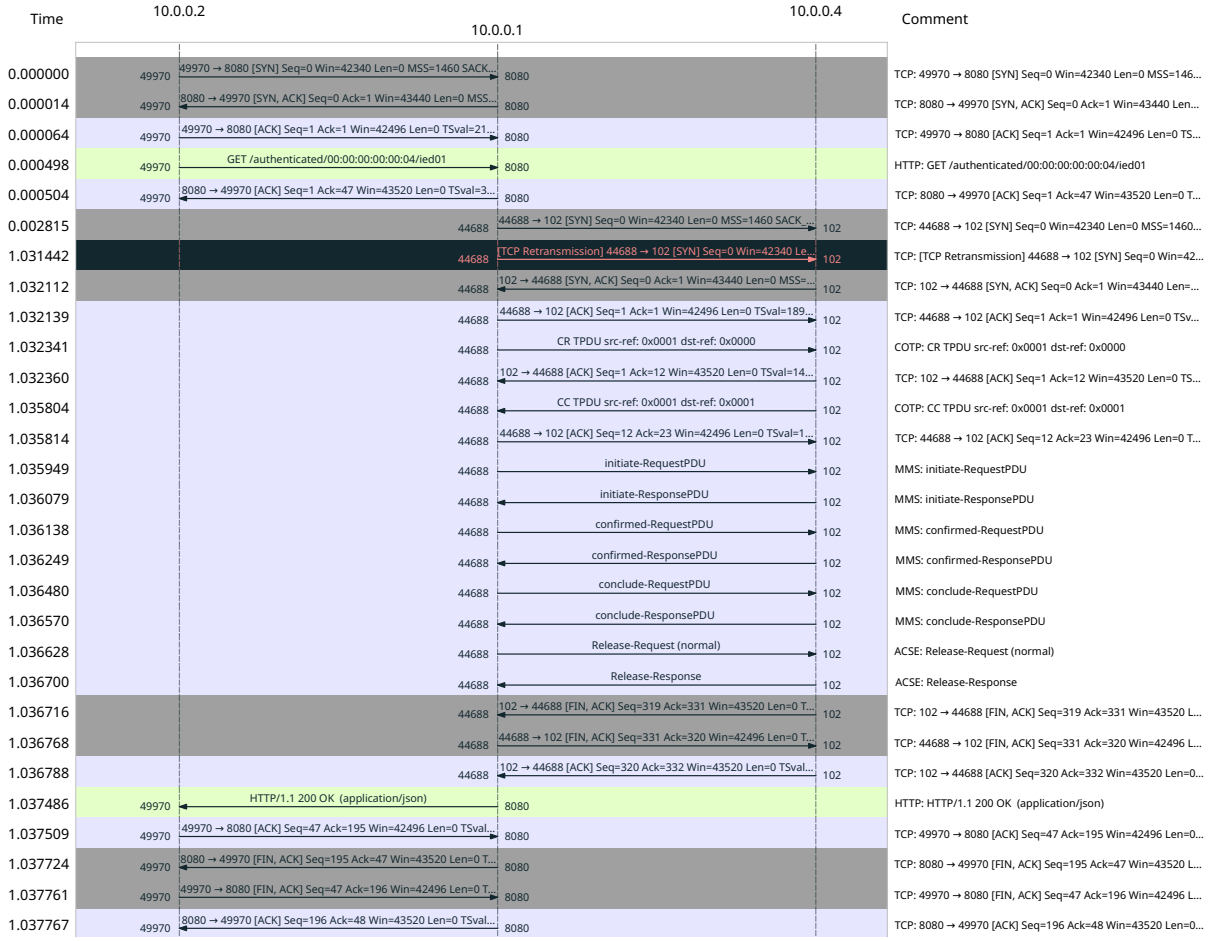


Figura 5.14: Sequência de eventos para a autorização através da API ARES e do protocolo MMS.

Por fim, todos os eventos apresentados anteriormente foram registrados pelo ARES. O `IED1` inicia o envio de quadros GOOSE imediatamente após conectar-se na rede, junto com seu processo de autenticação. Naturalmente, o controlador SDN instala uma regra de bloqueio para esses pacotes, pois o IED ainda não foi autenticado e nem autorizado. Após receber a confirmação da autenticação do IED, o controlador SDN instala as regras de fluxos para poder se comunicar através do protocolo MMS com o IED. Após conectar-se com o IED e fazer a leitura dos serviços requisitados por esse dispositivo, o controlador SDN pergunta ao controle de acesso se o IED está autorizado a publicar quadros GOOSE para o endereço *multicast* `01:0c:cd:01:00:01`. Após receber a confirmação, o

controlador SDN muda o estado do IED para autorizado, mas ainda não instala as regras de fluxos pois não existe nenhum assinante na rede. Após 10 segundos, o `IED2` inicia o processo de autenticação e autorização que se repete de forma similar ao descrito anteriormente, com a diferença de que este IED deseja assinar (receber) quadros GOOSE. Após confirmar a autorização, o controlador SDN finalmente instala proativamente as regras de fluxos necessárias para permitir o envio dos quadros pelo `IED1` e o recebimento pelo `IED2`. O registro de eventos gerado automaticamente por todos esses passos é mostrado na Figura 5.15. O registro gerado por esse experimento possui 1,3 KByte.

```
2019-08-01 19:57:58.900703 s2: Drop GOOSE 00:00:00:00:00:04 (port 2) -> 01:0c:cd:01:00:01
2019-08-01 19:57:58.901238 REASON: 00:00:00:00:00:04 is not authenticated
2019-08-01 19:57:59.436417 ied01 (00:00:00:00:00:04) authenticated successfuly
2019-08-01 19:57:59.436535 Installing MMS flows (ied01 <-> controller)
2019-08-01 19:57:59.437836 Controller connecting to ied01 (MMS)
2019-08-01 19:58:00.464034 ied01 wants to publish GOOSE frames to 01:0c:cd:01:00:01
2019-08-01 19:58:00.468145 ABAC: can ied01 publish GOOSE frames to 01:0c:cd:01:00:01?
2019-08-01 19:58:00.471384 ied01 (00:00:00:00:00:04) authorized to publish GOOSE frames to
01:0c:cd:01:00:01

2019-08-01 19:58:09.501006 ied02 (00:00:00:00:00:05) authenticated successfuly
2019-08-01 19:58:09.501219 Installing MMS flows (ied02 <-> controller)
2019-08-01 19:58:09.502770 Controller connecting to ied02 (MMS)
2019-08-01 19:58:10.523540 ied02 wants to subscribe to GOOSE frames from 01:0c:cd:01:00:01
2019-08-01 19:58:10.524298 ABAC: can ied02 subscribe to GOOSE frames from 01:0c:cd:01:00:01?
2019-08-01 19:58:10.524599 ied02 permited to subscribe to GOOSE frames from 01:0c:cd:01:00:01
2019-08-01 19:58:10.524664 ied02 (00:00:00:00:00:05) authorized to subscribe to GOOSE frames
from 01:0c:cd:01:00:01
2019-08-01 19:58:10.525424 Installing flows requested by ied02
```

Figura 5.15: Registro de eventos gerados pelo 3AS para o experimento descrito.

Através desses experimentos, verificou-se que o mecanismo de autenticação mantém o tempo de autenticação inferior a 300 milissegundos mesmo com um maior número de IEDs se autenticando ao mesmo tempo, e produz baixa carga de controle, 4,65 KBytes, 48,84% menor comparado a trabalhos relacionados. O controle de acesso garante que os dispositivos enviem e recebam mensagens conforme os níveis de autorização, além de atender aos requisitos de autorização e auditoria conforme proposto pelo 3AS. Por fim, como discutido anteriormente, conclui-se que em cenários de teleproteção, a autorização proativa faz-se necessária, uma vez que a autorização reativa gera uma latência maior que 3 milissegundos, tempo inaceitável de acordo com a parte 5 da norma IEC 61850 [17].

Capítulo 6

Conclusão

A rede elétrica inteligente, ou *smart grid*, surge da necessidade de melhoria da rede elétrica tradicional, possibilitando, dentre outras características, o monitoramento e controle da rede elétrica com o auxílio de redes de comunicação e tecnologia da informação, conforme a norma IEC 61850. Apesar dos benefícios apresentados pela introdução de uma rede de comunicação, novas vulnerabilidades são também incorporadas à rede elétrica inteligente. Assim como o controle remoto dos IEDs facilita a manutenção da rede elétrica, atacantes obtêm um novo meio de acesso indevido aos dispositivos da rede.

A gestão de identidade pode ser definida como um conjunto de métodos que fornecem um nível adequado de segurança para os recursos de uma organização através de políticas impostas aos usuários, com foco nos requisitos de autenticação, autorização e auditoria. Através de mecanismos de autenticação, os dispositivos, ou usuários, são identificados no sistema, enquanto mecanismos de autorização devem permitir ou negar acesso aos recursos conforme definido pelas políticas de acesso. Por fim, mecanismos de auditoria devem garantir o registro dos eventos da rede.

Diferente dos trabalhos presentes na literatura, o Autenticação, Autorização e Auditoria para *Smart Grids* (3AS), proposta desta dissertação, além de prover um mecanismo de autenticação baseado em IEEE 802.1X para os três protocolos de comunicação GOOSE, SV e MMS, e propor a utilização do modelo ABAC associado ao processo de autorização, ainda propõe um sistema integrado de auditoria, registrando eventos de autenticação, autorização e utilização de recursos da rede de comunicação. Outros trabalhos encontrados na literatura atendem apenas a cenários específicos de redes elétricas inteligentes, enquanto o 3AS preocupa-se em atender cenários diversos de redes elétricas inteligentes, desde a introdução de veículos elétricos na rede, até o sistema de teleproteção da rede elétrica. Através da utilização do modelo ABAC para a autorização, as políticas de acesso

granulares permitem a criação de diferentes níveis de acesso, além de identificar erros de configuração nos IEDs. Por fim, diferente da maioria dos trabalhos, o 3AS propõe um modelo de autenticação e autorização integrado à auditoria, permitindo o registro de eventos da rede de forma centralizada.

Durante o desenvolvimento desta dissertação, o arcabouço ARES foi implementado parcialmente em código aberto[1] no controlador Ryu e estendido conforme especificado pela proposta do 3AS. Também foram criados geradores de quadros GOOSE e pacotes MMS para a emulação do sistema supervisório e comunicação entre IEDs com objetivo de avaliar o 3AS.

Através de experimentos emulados, foi constatado que o mecanismo de autenticação produz uma carga de controle de 4,65 KBytes, 48,84% menor do que o mecanismo proposto por Resonance [39]. A autenticação também foi validada através de dois modelos de autenticação diferentes: EAP-PEAP, voltado para veículos elétricos, e produz menos carga de controle; e EAP-TLS, voltado para subestações, apresentando menor atraso. O processo de autorização demonstrou-se eficiente, bloqueando a comunicação de dispositivos não-autenticados, e permitindo a comunicação após a autorização bem sucedida. Por fim, conclui-se que em cenários de teleproteção, a autorização proativa faz-se necessária, uma vez que a autorização reativa gera uma latência maior que 3 milissegundos, tempo inaceitável de acordo com a parte 5 da norma IEC 61850 [17].

6.1 Trabalhos futuros

Os experimentos desta dissertação levam em consideração cenários pequenos, como o de uma subestação ou de um ponto de recarga para 10 veículos elétricos. Por tanto, é importante estudar a escalabilidade dos mecanismos do 3AS para cenários mais complexos, como por exemplo, a recarga de veículos elétricos em toda uma cidade. De maneira análoga, é necessário estudar também o problema de escalabilidade de armazenamento no 3AS, uma vez que há a necessidade de armazenar: credenciais, como certificados ou usuário e senha; políticas de acesso; e registros para auditoria.

Além dos desafios da escalabilidade, os seguintes estudos também podem ser feitos: validação do requisito de disponibilidade medindo o atraso da reautenticação de IEDs; estudar a inclusão de mecanismos de integridade e confidencialidade para o 3AS; pesquisar o uso de *blockchain* para gestão dos registros auditáveis, garantindo a confidencialidade

[1] Disponível em github.com/arthurazs/3AS.

e não repúdio; investigar os outros métodos de autenticação como EAP-MD5 e EAP-TTLS; investigar a autorização com contexto de localização (ABAC *context-aware*) para aumentar a granularidade das políticas, garantindo por exemplo, que um IED de proteção só possa ganhar acesso se estiver dentro da subestação; e explorar o uso dos registros de autenticação e autorização para integrar um sistema de detecção de intrusão.

Referências

[1] Abomhara, M.; Køien, G. M. Security and privacy in the Internet of Things: Current status and open issues. In *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)* (May 2014), pp. 1–8.

[2] Aftab, M. A.; Hussain, S. M. S.; Ali, I.; Ustun, T. S. IEC 61850 and XMPP Communication Based Energy Management in Microgrids Considering Electric Vehicles. *IEEE Access 6* (2018), 35657–35668.

[3] Ali, J.; Lee, S.; Roh, B.-h. Performance Analysis of POX and Ryu with Different SDN Topologies. In *Proceedings of the 2018 International Conference on Information Science and System* (New York, NY, USA, 2018), ICISS '18, ACM, pp. 244–249.

[4] Almulla, S. A.; Chan Yeob Yeun. Cloud computing security management. In *2010 Second International Conference on Engineering System Management and Applications* (March 2010), pp. 1–7.

[5] Asadollahi, S.; Goswami, B.; Sameer, M. Ryu controller's scalability experiment on software defined networks. In *2018 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)* (Feb 2018), pp. 1–5.

[6] Aydeger, A.; Saputro, N.; Akkaya, K.; Uluagac, S. Assessing the overhead of authentication during SDN-enabled restoration of smart grid inter-substation communications. In *2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC)* (Jan 2018), pp. 1–6.

[7] Cheung, H.; Hamlyn, A.; Mander, T.; Yang, C.; Cheung, R. Role-based model security access control for smart power-grids computer networks. In *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century* (July 2008), pp. 1–7.

[8] Chowdhury, M. M. R.; Raddatz, H.; Rossebø, J. E. Y. Challenges when securing manufacturing message service in legacy industrial control systems. In *Proceedings of the 2014 IEEE ETFA* (Sep. 2014).

[9] Comissão de Estudo de Segurança Física em Instalações de Informática (CE-21:2-4.01). *Tecnologia da informação – Técnicas de seguranca – Código de prática para a gestão da segurança da informação*, 2005. ABNT NBR ISO/IEC 17799.

[10] Dong, X.; Lin, H.; Tan, R.; Iyer, R. K.; Kalbarczyk, Z. Software-Defined Networking for Smart Grid Resilience. *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security - CPSS '15* (2015), 61–68.

[11] Ergut, S.; Gungor, V.; Sahin, D.; Kocak, T.; Hancke, G.; Buccella, C.; Cecati, C. A Survey on Smart Grid Potential Applications and Communication Requirements. *IEEE Transactions on Industrial Informatics 9*, 1 (2012), 1–1.

[12] Farhangi, H. The Path of the Smart Grid. *IEEE Power and Energy Magazine 8*, 1 (2010), 18–28.

[13] Flathagen, J.; Mjelde, T. M.; Bentstuen, O. I. A combined network access control and qos scheme for software defined networks. In *2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)* (Nov 2018), pp. 1–6.

[14] Gusmeroli, S.; Piccione, S.; Rotondi, D. IoT Access Control Issues: A Capability Based Approach. In *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* (July 2012), pp. 787–792.

[15] Institute of Electrical and Electronics Engineers. *Standard for Local and metropolitan area networks – Port-Based Network Access Control*, 2010. IEEE 802.1x.

[16] International Electrotechnical Commission. *Communication networks and systems for power utility automation*, 2002–2019. IEC 61850.

[17] International Electrotechnical Commission. *Communication networks and systems in substations – Part 5: Communication requirements for functions and device models*, 2003. IEC 61850-5.

[18] International Electrotechnical Commission. *Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*, 2004. IEC 61850-8-1.

[19] International Electrotechnical Commission. *Power systems management and associated information exchange – Data and communications security*, 2007–2018. IEC 62351.

[20] International Electrotechnical Commission. *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*, 2009. IEC 61850-6.

[21] International Electrotechnical Commission. *Communication networks and systems for power utility automation – Part 90-8: Object model for E-mobility*, 2016. IEC 61850-90-8.

[22] International Organization for Standardization. *Industrial automation systems – Manufacturing Message Specification*, 2 ed., 2003. ISO 9506.

[23] Jyh-Cheng Chen; Yu-Ping Wang. Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience. *IEEE Communications Magazine 43*, 12 (Dec 2005), supl.26–supl.32.

[24] Kang, B.; Maynard, P.; McLaughlin, K.; Sezer, S.; Andrén, F.; Seitl, C.; Kupzog, F.; Strasser, T. Investigating cyber-physical attacks against iec 61850 photovoltaic inverter installations. In *2015 IEEE 20th Conference on Emerging Technologies Factory Automation (ETFA)* (Sep. 2015), pp. 1–8.

[25] Khalid, A.; Quinlan, J. J.; Sreenan, C. J. MiniNAM: A network animator for visualizing real-time packet flows in Mininet. In *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)* (March 2017), pp. 229–231.

[26] Khan, R.; Aditi, T.; Sreeram, V.; Iu, H. A Prepaid Smart Metering Scheme Based on WiMAX Prepaid Accounting Model. *Smart Grid and Renewable Energy 1*, 2 (2010), 63–69.

[27] Kim, J.; Filali, F.; Ko, Y. A lightweight CoAP-based software defined networking for resource constrained AMI devices. In *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (Nov 2015), pp. 719–724.

[28] Li, Q.; Cao, G. Multicast authentication in the smart grid with one-time signature. *IEEE Transactions on Smart Grid 2*, 4 (2011), 686–696.

[29] Li, X.; Liang, X.; Lu, R.; Shen, X.; Lin, X.; Zhu, H. Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges. *IEEE Communications Magazine 50*, 8 (2012), 38–45.

[30] Lopes, Y. *ARES: Um Arcabouço para Comunicação Autonômica e Resiliente em Redes Elétricas Inteligentes.* Tese de Doutorado, Universidade Federal Fluminense, 2019.

[31] Lopes, Y.; Bornia, T.; Farias, V.; Fernandes, N. C. Desafios de Segurança e Confiabilidade na Comunicação para Smart Grids. *SBSeg* (2016), 142–186.

[32] Lopes, Y.; Fernandes, N.; de Castro, T.; Farias, V.; Noce, J.; Marques, J.; Muchaluat-Saade, D. *Security Solutions and Applied Cryptography in Smart Grid Communications.* IGI Global, Idea Group Inc, 2016, ch. Vulnerabilities and Threats in Smart Grid Communication Networks.

[33] Lopes, Y.; Fernandes, N. C.; Bastos, C. A. M.; Muchaluat-Saade, D. C. SMARTFlow: A Solution for Autonomic Management and Control of Communication Networks for Smart Grids. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing* (New York, NY, USA, 2015), SAC '15, ACM, pp. 2212–2217.

[34] Lopes, Y.; Frazão, R. H.; Molano, D. A.; dos Santos, M. A.; Calhau, F. G.; Bastos, C. A. M.; Martins, J. S. B.; Fernandes, N. C. Smart Grid e IEC 61850: Novos Desafios em Redes e Telecomunicações para o Sistema Elétrico. In *Minicursos do XXX SBrT* (2012), SBrT, pp. 1–44.

[35] Matias, J.; Garay, J.; Mendiola, A.; Toledo, N.; Jacob, E. FlowNAC: Flow-based network access control. *Proceedings - 2014 3rd EWSDN* (2014), 79–84.

[36] Mattos, D. M. F.; Duarte, O. C. M. B. AuthFlow: authentication and access control mechanism for software defined networking. *Annals of Telecommunications 71*, 11-12 (2016), 607–615.

[37] Mattos, D. M. F.; Medeiros, D. S. V.; Fernandes, N. C.; Oliveira, M. T.; Carrara, G. R.; Soares, A. A. Z.; Magalhaes, L. C. S.; Passos, D.; Carrano, R. C.; Moraes, I. M.; Albuquerque, C. V. N.; Muchaluat-Saade, D. C. Blockchain para Segurança em Redes Elétricas Inteligentes: Aplicações, Tendências e Desafios. *Minicursos do XVIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais* (2018), 140–194.

[38] McKeown, N.; Anderson, T.; Balakrishnan, H.; Parulkar, G.; Peterson, L.; Rexford, J.; Shenker, S.; Turner, J. OpenFlow: Enabling Innovation in Campus Networks. *SIGCOMM Comput. Commun. Rev. 38*, 2 (Mar. 2008), 69–74.

[39] Nayak, A. K.; Reimers, A.; Feamster, N.; Clark, R. Resonance: Dynamic Access Control for Enterprise Networks. In *Proceedings of the 1st ACM* (2009), WREN '09, pp. 11–18.

[40] Neuman, C.; Tan, K. Mediating cyber and physical threat propagation in secure smart grid architectures. In *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (Oct 2011), pp. 238–243.

[41] Saxena, N.; Choi, B. J.; Lu, R. Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid. *IEEE Transactions on Information Forensics and Security 11*, 5 (May 2016), 907–921.

[42] Scarselli, R. B.; Soares, L. F.; Moraes, I. M. Uma Avaliação de Algoritmos Criptográficos em Redes IEC 61850: Uma Abordagem Prática. In *Workshop de Segurança Cibernética em Dispositivos Conectados* (2019), Anais do WSCDC, pp. 39–52.

[43] Schlegel, R.; Obermeier, S.; Schneider, J. A security evaluation of IEC 62351. *Journal of Information Security and Applications 34* (2017), 197 – 204.

[44] Shang, W.; Ding, Q.; Marianantoni, A.; Burke, J.; Zhang, L. Securing building management systems using named data networking. *IEEE Network 28*, 3 (May 2014), 50–56.

[45] Silva, E. F.; Muchaluat-Saade, D. C.; Fernandes, N. C. ACROSS: A generic framework for attribute-based access control with distributed policies for virtual organizations. *Future Generation Computer Systems 78* (2018), 1–17.

[46] Soares, A. A. Z.; Mattos, D. M. F.; Lopes, Y.; Medeiros, D. S. V.; Fernandes, N. C.; Muchaluat-Saade, D. C. An Efficient Authentication Mechanism based on Software-Defined Networks for Electric Vehicles. In *2019 IEEE 28th International Symposium on Industrial Electronics (ISIE)* (June 2019), pp. 2471–2476.

[47] Sotirov, A.; Stevens, M.; Appelbaum, J.; Lenstra, A. K.; Molnar, D.; Osvik, D. A.; de Weger, B. MD5 considered harmful today, creating a rogue CA certificate. *25th Annual Chaos Communication Congress* (2008).

[48] Ustun, T. S.; Khan, R. H.; Hadbah, A.; Kalam, A. An adaptive microgrid protection scheme based on a wide-area smart grid communications network. In *2013 IEEE Latin-America Conference on Communications* (2013), pp. 1–5.

[49] Ustun, T. S.; Ozansoy, C.; Zayegh, A. Modeling of a Centralized Microgrid Protection System and Distributed Energy Resources According to IEC 61850-7-420. *IEEE Transactions on Power Systems 27*, 3 (Aug 2012), 1560–1567.

[50] Wang, W.; Lu, Z. Cyber security in the Smart Grid: Survey and challenges. *Computer Networks 57*, 5 (2013), 1344 – 1371.

[51] Yakasai, S. T.; Guy, C. G. FlowIdentity: Software-defined network access control. In *IEEE Conference on NFV-SDN* (Nov 2015), pp. 115–120.

[52] Yan, Y.; Qian, Y.; Sharif, H. A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid. In *2011 IEEE Wireless Communications and Networking Conference* (March 2011), pp. 909–914.

[53] Zhang, H.; Cheng, P.; Shi, L.; Chen, J. Optimal DoS Attack Scheduling in Wireless Networked Control System. *IEEE Transactions on Control Systems Technology 24*, 3 (May 2016), 843–852.