# Gestão de Identidade e Acesso para Dispositivos IoT na Smart Grid

**Vilmar Abreu Jr.[1], Altair O. Santin[1], Eduardo K. Viegas[1], Cleverton J. A. Vicentini[2], Mateus N. da Silva[1]**

[1]Programa de Pós-Graduação em Informática (PPGIa)
Pontifícia Universidade Católica do Paraná (PUCPR), 80.215-901 - Curitiba - PR

[2]Instituto Federal do Paraná (IFPR)
Curitiba - PR

{vilmar.abreu, santin, eduardo.viegas, nunes.mateus}@ppgia.pucpr.br,
cleverton.vicentini@ifpr.edu.br

***Resumo.*** *Redes elétricas inteligentes (SG, Smart Grid) são compostas por dispositivos da internet das coisas (IoT, Internet of Things) que possuem restrições computacionais que impedem a adoção de protocolos tradicionais de comunicação e segurança. Assim, esse trabalho propõem uma abordagem de segurança fim-a-fim na comunicação entre os elementos da SG, permitindo que um usuário autenticado transporte suas credenciais obtidas na Internet para o contexto de IoT. Essa abordagem tem como principal vantagem a utilização do protocolo multicast na comunicação, sem comprometer a segurança. Apesar dessa proposta prover segurança na comunicação, não é capaz de prover controle fino no acesso aos recursos protegidos da IoT. Dessa maneira, propomos um controle de acesso leve baseado em duas etapas baseado para prover autorizações baseadas em papéis no contexto da IoT. A avaliação do protótipo mostrou-se mais eficiente e flexível do que os trabalhos encontrados na literatura.*

***Abstract.*** *The smart grid (SG) is composed of IoT devices, that are resource constrained devices that restrict the use of traditional communication and security protocols. In the light of this, this work proposes an end-to-end secure communication between the elements in the SG, allowing an authenticated user to transport her credentials obtained on the Internet to the IoT context. This approach has as its main advantage the higher efficiency in the message exchanges, by adopting the multicast communication, without compromising the security. Even though this process provides secure communication, it is not capable of enforcing fine-grained access control on protected resources. Therefore, we propose a two-step lightweight access control that builds upon the established configuration to provide role-based authorization in IoT context. The prototype evaluation was more efficient and flexible than those found in the literature.*

## 1. Introdução

Redes elétricas inteligentes (SG, *Smart Grid*) consistem em sistemas de energia elétrica que através de inteligência computacional e tecnologias de comunicação atuam de maneira integrada na geração, transmissão, distribuição e consumo de energia [Fang et

al. 2012]. Portanto, são sistemas responsáveis pelo controle e supervisão de infraestruturas críticas [NIST 2014]. Infraestruturas críticas são sistemas e ativos, virtuais ou físicos, que são vitais a uma nação, de modo que a indisponibilidade ou destruição dessas infraestruturas podem causar grandes impactos na segurança e na economia.

Nos últimos anos, pesquisas demonstraram que os sistemas de energia elétrica são vulneráveis e, consequentemente, sujeitos a ataques cibernéticos [Cárdenas et al. 2008]. Um dos principais fatores que justificam esse cenário é a substituição dos controladores de processamento lógicos (CLP) tradicionais por microprocessadores, sistemas embutidos e principalmente por dispositivos da Internet das Coisas (IoT, Internet of Things), os quais permitem o acesso remoto interativo através da Internet [Mallmann et al. 2020]. A utilização de dispositivos dessa natureza, que contêm sensores, poder de processamento e de atuação, é uma tendência natural adotada na Indústria 4.0. Entretanto, a exposição desses dispositivos na Internet pode comprometer toda infraestrutura crítica [NIST 2014].

A cibersegurança para SG emergiu como interesse crítico de organizações governamentais, devido a diversos incidentes [Tomio et al. 2021]. Por exemplo, o centro de controle de uma usina elétrica foi atacado em 2010, o que resultou numa perda de 900MW (Megawatts) em menos de 7 segundos [Y. Ashibani e Q. Mahmoud 2017]. No mesmo ano, a usina nuclear de Natanz, localizada no Irã, foi atacada pelo Stuxnet [Langner 2011]. Os prejuízos foram incalculáveis e provocaram sérias deteriorações na infraestrutura física [Peng et al. 2013]. De acordo com um relatório da CIA (Central Intelligence Agency), diversos sistemas de energia nos EUA foram invadidos por hackers, causando apagões em diversas cidades [Y. Ashibani e Q. Mahmoud 2017].

Para proteger os sistemas de energia elétrica, mais especificamente da SG, foram definidos requisitos padronizados por entidades conceituadas, como a IEC (*International Electrotechnical Commission*), NERC (*North American Electric Reliability Corporation*) e IEEE (*Institute of Electrical and Electronic Engineers*). Entretanto, esses requerimentos apresentam normas e procedimentos com granularidade grossa. Adicionalmente, a IEC também realizou um mapeamento de normas para SG [IEC 2010], no qual apresenta as diferentes aplicações de SG e suas respectivas normas e lacunas (gaps). Esse estudo concluiu que os padrões de cibersegurança existentes, inclusive os padrões que apresentam relatórios técnicos, não são suficientes para cobrir toda a complexidade da arquitetura da SG. Além disso, o estudo demonstra que existe uma lacuna significativa em relação a abrangência de dispositivos ubíquos, mais especificamente da IoT.

A segurança dos dispositivos da IoT (e.g. medidores inteligentes) é essencial, pois comprometendo um único dispositivo é possível comprometer toda a SG [Viegas et al. 2021]. A principal dificuldade em garantir a segurança está relacionada às restrições de poder computacionais, que impossibilitam a utilização de protocolos tradicionais de comunicação e segurança. Isso cria uma lacuna tecnológica de interoperabilidade que impede a implantação de mecanismos tradicionais de Gestão de Identidade e Acesso (IAM, *Identity and Access Management*).

Nossa proposta tem como objetivo permitir que um usuário autenticado no IAM transporte suas credenciais para o contexto da IoT, mantendo a autenticidade e confidencialidade da comunicação. Para isso, propomos uma abordagem baseada em senhas descartáveis (OTP, *One Time Password*) para cifrar e autenticar a comunicação (*unicast*/*multicast*) entre as entidades da IoT e da Internet. Apesar dessa abordagem

garantir a segurança fim-a-fim na comunicação, não é capaz de garantir o controle de acesso fino nos recursos protegidos da IoT. Para tanto, o IAM utiliza um controle de acesso leve (*lightweight*) adequado as restrições dos dispositivos da IoT para controlar o acesso dos usuários aos recursos protegidos da IoT.

As principais contribuições do trabalho são: (i) um protocolo de comunicação *multicast* seguro para IoT, adequado as restrições computacionais; (ii) uma abordagem dinâmica e segura para definição da chave DTLS (*Datagram Transport Layer Security*) usada na criptografia da comunicação da IoT; (iii) um controle de acesso leve para IoT baseado em papéis; (iv) uma abordagem de comunicação segura fim-a-fim usando OTP entre entidades da Internet e dispositivos da IoT.

## *2*. Fundamentação

Esta seção apresenta os conceitos relacionados à SG e gestão de identidade e acesso. Tais conceitos são fundamentos substanciais para o entendimento da proposta.

### 2.1 *Redes Elétricas Inteligentes (SG, Smart Grid)*

A SG utiliza fluxos bidirecionais de eletricidade e informação para criar um sistema automatizado de distribuição de energia. Mais especificamente, a SG pode ser considerada como um sistema que utiliza informações, tecnologias de comunicação bidirecionais, cibersegurança e inteligência computacional de maneira integrada para geração, transmissão, distribuição e consumo de energia [Fang et al. 2012]. A SG tem o propósito de disponibilizar um sistema limpo, seguro, confiável, resiliente, eficiente e sustentável, contemplando desde a geração da energia até o consumidor final [Vicentini et al. 2019]. A evolução da SG não está relacionada somente com os avanços tecnológicos, mas também na sofisticação do monitoramento, análise, otimização, segurança e controle a partir do sistema central (SC) da empresa de energia. A medição inteligente de energia é o mecanismo mais importante usado na SG, utilizado para coletar e gerenciar informações dos consumidores e dos dispositivos em campo [Ramos et al. 2021]. Essas atividades são de responsabilidade da AMI (*Automatic Metering Infrastructure*), sendo que suas principais funcionalidades são: coletar diagnósticos, consumo de energia e informações de estado dos medidores inteligentes (MI) de energia para serem transferidos para o SC com o objetivo de faturamento, análise e resolução de problemas. A AMI, presente na SG, tem como grande diferencial a comunicação por duas vias, que permite a transmissão de informações quase em tempo real e sob demanda, possibilitando o aperfeiçoamento das operações do sistema e gerenciamento por parte do consumidor.

Na perspectiva do consumidor, a medição inteligente de energia oferece potenciais benefícios. Por exemplo, o consumidor pode estimar o valor de sua fatura no final do mês, assim podendo gerenciar o consumo para reduzir sua fatura. Na perspectiva da empresa de energia, as empresas podem disponibilizar em tempo real o valor da energia para encorajar os consumidores a reduzir a demanda em horários de picos ou aproveitarem horários com a tarifa reduzida.

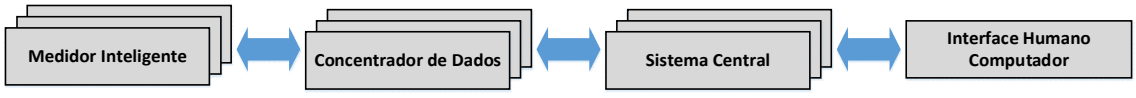


**Fig. 1. Arquitetura típica de um sistema de medição na SG. Adaptado de [Fang et al. 2012].**

A arquitetura típica da AMI de uma SG, apresentada na Figura 1, é composta de MIs, que são instalados nas residências dos consumidores. Os MIs viabilizam a comunicação de duas vias com o SC. Para tanto, os medidores normalmente são medidores eletrônicos responsáveis por armazenar o consumo de energia em um intervalo de no máximo uma hora para ser enviado ao SC, pelo menos uma vez por dia, com propósito de monitoramento e faturamento. Adicionalmente, o MI pode conectar e desconectar remotamente um dispositivo do usuário (*appliance*) para gerenciar a carga da residência.

Os MIs são alvos atrativos para os atacantes (adversários), uma vez que as vulnerabilidades podem ser facilmente monetizadas [P. McDaniel e S. McLaughlin 2009]. Atacantes que comprometem os MIs podem manipular o consumo de energia ou até mesmo forjar a geração de energia para ganhar dinheiro. Além de ganhos financeiros, atacantes podem forjar informações de consumo energético em diversos MIs para fazer com que a empresa de energia elétrica tome decisões erradas em relação à capacidade da rede. Adicionalmente, é habitual que empresas de energia elétrica disponham de milhares de MIs instalados em seus consumidores, que são controlados por alguns SCs. Dessa maneira, caso o atacante obtenha o controle do SC, poderia interromper o fornecimento de energia de toda uma região.

O MI possui diversos requisitos [Gungor 2010]: (i) frequentemente são dispositivos de baixo custo, com recursos computacionais limitados que restringem o uso de protocolos de comunicação e segurança tradicionais. Dessa maneira, devido às restrições de processamento, bateria, memória e rede conseguem apenas implementar algumas funcionalidades limitadas e unitárias; (ii) devem ser acessíveis e configuráveis (parametrizáveis) remotamente; (iii) a segurança física e lógica é um aspecto essencial, pois comprometendo um único MI, os adversários podem comprometer toda a operação da SG.

O Concentrador de Dados (CD) é responsável por agregar e concentrar as informações fornecidas pelos MIs para transmitir para o SC. O SC, por sua vez, é responsável por realizar a parte de negócios do sistema. Possui uma infraestrutura robusta, normalmente alocada em nuvens computacionais, possuindo processamento de larga escala. Suas principais funcionalidades são: coletar, monitorar e supervisionar os dados. O SC é considerado o elemento crítico da arquitetura, uma vez que possui uma ampla visão da situação dos medidores, com potencial de tomada de decisões estratégicas a respeito do negócio. Finalmente, um usuário (operador) pode acessar o sistema para gerenciar a infraestrutura através da Interface Humano Computador (IHC).

### 2.2 *Gestão de Identidade e Acesso (IAM, Identity and Access Management)*

A identidade representa uma entidade em um contexto particular [Cao e Yang 2010]. Tipicamente, uma identidade é formada por um identificador com credenciais e atributos que representam características da entidade. A Gestão de Identidade e Acesso (IAM) tem a função de estabelecer o relacionamento entre uma pessoa e os recursos que essa deve acessar para exercer sua função de trabalho [NIST 2014]. Dessa forma, o IAM disponibiliza identidades que são associadas a credenciais que, por sua vez, são utilizadas para controlar o acesso a recursos protegidos.

Dessa forma, a utilização de um IAM possui quatro objetivos dominantes: (i) fornecimento de identidade – baseado em registro único no provedor de identidades (IdP, *Identity Provider*), diversos provedores de serviços (SP, *Service Provider*) podem utilizar

diferentes identidades para o mesmo usuário; (ii) autenticação única (SSO, Single Sign-On) – baseado em uma única autenticação em um SP, diversos SPs acessam o mesmo IdP; (iii) compartilhamento de atributos – os atributos de identidade especificados em determinado SP podem ser reutilizados em outros SPs; (iv) autorização de acesso – restringe o acesso de um SP a um recurso protegido sem precisar acessar as credenciais do usuário.

O IAM é responsável por emitir *tokens de acesso* que autorizam usuários autenticados a acessar serviços protegidos. O *token de acesso* contém um escopo de acesso que permite definir a visibilidade do recurso e seu tempo de vida (duração). Quando o tempo de duração é expirado, o *token de acesso* é invalidado e o IAM deve emitir um novo. Portanto, o *token de acesso* garante que apenas usuários autenticados e autorizados podem ser admitidos no sistema.

A validação do *token de acesso* pode ser realizada de forma online, ou seja, um SP que deseja validar um *token de acesso* deve consultar o IAM. Assim, a cada operação do usuário no SP, o mesmo deve fornecer seu *token de acesso* para ser validado no IAM. O acesso é permitido se o *token de acesso* for válido e contiver o escopo apropriado, se não o acesso é negado.

## 3. Trabalhos Relacionados

A literatura apresenta inúmeros trabalhos relacionados à segurança de dispositivos da IoT. Além das funcionalidades específicas ao contexto, um dispositivo da IoT tipicamente é capaz de informar ao fabricante que está com problemas técnicos. Assim, o fabricante pode acessar remotamente o dispositivo para reparar ou atualizar o firmware. Nesse caso, é comum que o fabricante necessite acessar centenas ou milhares de dispositivos remotamente, necessitando a autenticação individual em cada dispositivo. Para atender essa demanda, os trabalhos explorados na literatura isolam o dispositivo por questões de segurança [Lu et al. 2010, Witkovski et al. 2015]. Adicionalmente, esses trabalhos indicam que a comunicação e o acesso ao dispositivo devem ser controlados.

A autenticação e autorização no contexto da IoT é um desafio significativo discutido na literatura, uma vez que, devido às restrições de poder computacional, mecanismos tradicionais de segurança não podem ser aplicados na IoT. É habitual encontrar soluções de mercado que utilizam uma senha ou chave única para todos os dispositivos. Essa abordagem tem como vantagem o baixo consumo de recursos. Entretanto, uma vez que a senha/chave é descoberta, todos os dispositivos tornam-se vulneráveis [Hackernews, 2015], [Infoword, 2015] e [ZDnet, 2021]. Ademais, atualizar a senha ou chave de todos os dispositivos não é uma tarefa trivial, e esse desafio desencadeou diversas propostas para tratar essa demanda.

O trabalho de Liu et al. (2012) definiu um método de autenticação e controle de acesso para IoT. A proposta do trabalho utiliza o OpenID e o RBAC (*Role-based Access Control)* no contexto da IoT. Entretanto, apesar do trabalho selecionar mecanismos de segurança popularmente conhecidos, os autores não mencionam como realizar a implantação no contexto da IoT, que possui diversas restrições de recursos computacionais. Além disso, a confidencialidade na comunicação ou SSO não foram tratados.

A pesquisa de Ammayappan et al. (2006) propôs um protocolo de autenticação para SG que utiliza criptografia simétrica e assimétrica para garantia da autenticação e

confidencialidade durante a comunicação. Apesar do trabalho considerar que a proposta é leve (*lightweight*), a mesma utiliza criptografia assimétrica, que não é uma prática recomendada para dispositivos da IoT [Vicentini et al. 2018]. O trabalho de Chin et al. (2016), apresentou uma plataforma de autenticação baseada em M2M (*Machine-to-machine)* para SG. A proposta é baseada em assinaturas digitais, nas quais a troca de chaves entre os contextos é realizada no concentrador. Isso é um problema, pois gera um ponto de falha único, além de utilizar criptografia de chave pública no contexto de IoT.

O trabalho de Chavan et al. (2016) observou que a adoção do protocolo HTTP é ineficiente em ambientes com restrições computacionais. Assim, os autores utilizaram o protocolo CoAP (*Constrained Application Protocol*) com DTLS para garantir a confidencialidade na comunicação. Porém, combinaram esses protocolos com o uso de chaves públicas. Por outro lado, a pesquisa do Hou et al. (2018) demonstrou matematicamente a importância da segurança e do SSO na autenticação de dispositivos da IoT.

O trabalho de Garcia et al. (2013) realizou uma análise de segurança no protocolo DTLS e observou que existem vulnerabilidades conhecidas, assim como existem no TLS (*Transport Layer Security*). Para mitigar essas vulnerabilidades, o trabalho de Shivraj et al. (2015) propôs um esquema de autenticação baseado em dois fatores que utiliza OTP. O trabalho combinou o algoritmo de *Lamport* com curvas elípticas para garantir a autenticação fim-a-fim na IoT. O protótipo apresentou ser eficiente quando avaliado em um smartphone Android. Entretanto, os autores não avaliaram o desempenho do trabalho em dispositivos com restrições de processamento, bateria, memória e largura de banda.

O trabalho de Witkovski (2015) apresenta um esquema de autenticação baseada em chaves criptográficas para IoT, que permite o SSO. A proposta é baseada na ANSI X.9.17, na qual adota dois níveis hierárquicos de chaves simétricas para realizar a comunicação entre as entidades da Internet e IoT. O trabalho de Witkovski (2015) é discutido na seção da avaliação. O trabalho de Shanta et al. (2016) realizou uma revisão sistemática sobre técnicas de autenticação para IoT. Os autores concluíram que os mecanismos de autenticação e proteção de dados devem ser rápidos e leves sem comprometer a segurança do sistema.

## 4. Proposta

Essa seção apresenta a abordagem de segurança fim-a-fim baseada em senhas descartáveis e pelo controle de acesso leve baseado em papéis para IoT.

### 4.1 *Segurança fim-a-fim baseada em senhas descartáveis*

Nossa proposta considera às restrições de poder computacional intrínsecas da IoT (discutida na seção 2.1), que impossibilitam a adoção de padrões de segurança tradicionais da Internet (e.g. TLS). Dessa forma, com objetivo de garantir a segurança fim-a-fim na comunicação, a proposta considera dois níveis de criptografia. No nível externo, utiliza a criptografia simétrica para as entidades da IoT (DTLS), e criptografia de chave pública para as entidades na Internet (TLS). No nível interno a criptografia de chave simétrica foi empregada, pois exige menor poder de processamento, quando comparado com a criptografia de chave pública.

Para mitigar a possibilidade de comprometimento da chave simétrica utilizada no nível interno, nossa proposta adota o conceito de senha descartável (OTP). Essa senha

descartável é utilizada como chave simétrica para criptografar a comunicação entre as entidades da Internet e IoT. Assim, para realizar a comunicação fim-a-fim entre o SC e o MI é utilizado o método TOTP (*Time-based One Time Password*) [Raihi et al. 2011], que é baseado no HMAC (*Hashed Message Authentication Code*).

Dessa maneira, cada MI possui uma chave simétrica compartilhada com o SC (Figura 2). Essa chave simétrica adota o conceito de chave mestre (LMK, *Local Master Key*), no qual nunca é trafegada pela rede, pois é armazenada em linha de produção no MI de maneira protegida por hardware (e.g. *smartcard*). Já no SC, a LMK é armazenada em uma base de chaves com proteção adequada, similar à que é empregada no *Key Distribution Center* (KDC) do Kerberos.

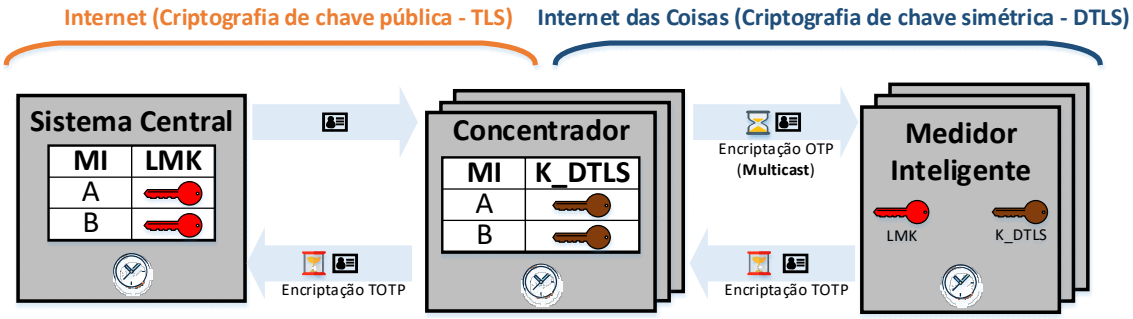


**Figura 2. Abordagem baseada em OTP.**

O valor gerado pelo TOTP também depende de um contador dinâmico e incremental compartilhado entre as entidades da IoT e da Internet. Dessa maneira, um contador é compartilhado entre o CS e o MI para garantir a comunicação fim-a-fim, e outro contador é compartilhado entre o DC e o MI para proteger a comunicação *multicast*. O objetivo dessa comunicação *multicast* é reduzir o número de trocas de mensagem, uma vez que é comum que o SC requisite informações de diversos MIs. Assim, a senha descartável gerada pelo TOTP é usada como chave de grupo na comunicação.

Com exceção da LMK, os demais parâmetros, como a chave DTLS e contadores (MI-SC, MI-CD) são definidos dinamicamente de maneira segura pela rede. Para isso, o CD gera uma nova K_DTLS e cifra a mesma na chave pública do SC. Em seguida, encaminha a requisição para o SC cifrar a K_DTLS com a LMK. Assim, o SC decifra a mensagem usando sua chave privada para poder cifrar na LMK. O CD recebe a mensagem cifrada em sua chave pública e decifra com sua chave privada. Finalmente, o CD encaminha a K_DTLS cifrada para o MI, no qual será decifrada na LMK do MI. Esse processo também é utilizado para definir o contador compartilhado entre o CD e o MI.

É importante observar que toda comunicação é cifrada, sendo que a comunicação entre o SC e o CD é protegida pela criptografia de chave pública. Por outro lado, a comunicação entre o SC e o MI é protegida por uma criptografia de chave simétrica, no qual a LMK nunca é transmitida/exposta na rede.

A comunicação *multicast*, adotada entre o CD e os MI, utiliza o método convencional de OTP, ao invés do TOTP. O método OTP não utiliza uma chave criptográfica (LMK) para produzir a senha descartável. Essa escolha foi motivada por duas razões: (i) evita a necessidade do compartilhamento de uma chave criptográfica entre o CD e o MI; (ii) de maneira geral as requisições não contêm conteúdos sensíveis, apenas as respostas que estão cifradas em duas camadas de criptografia. Assim, a camada interna

é cifrada utilizando a senha (chave) produzida pelo TOTP, enquanto a camada mais externa é cifrada no K_DTLS. Dessa forma, o CD consegue apenas decifrar a camada externa, não sendo considerado um ponto único de falhas (Figura 2).

Após essa configuração inicial, é possível aplicar o protocolo de segurança fim-a-fim utilizando a abordagem OTP. Primeiramente, um operador autenticado no IAM requisita através do SC, por exemplo, o consumo de energia atual de todos os MIs de uma determinada região, fornecendo seu *token de acesso*. O CD valida o *token de acesso* no IAM, e caso seja válido gera uma nova chave utilizando o OTP para ser utilizada como chave de grupo. Assim, a requisição do SC é cifrada na chave de grupo e transmitida para todos os MIs através do *multicast*. Todos os MIs pertencentes ao grupo *multicast* recebem a mensagem cifrada na chave de grupo. Cada MI gera uma nova chave de grupo utilizando o OTP para decifrar a requisição. Assim, após processar a requisição do SC, o MI gera uma chave utilizando o TOTP, parametrizado pela LMK. Essa chave é usada para cifrar a resposta que será enviada para o CD, cifrada no K_DTLS.

Observe que esse processo garante a segurança fim-a-fim na comunicação, pois todas as comunicações estão cifradas. Nesse contexto, o CD é capaz de ler o conteúdo das requisições realizadas pelo SC para os MIs. Entretanto, não é capaz de ler as respostas dos MIs porque são cifradas utilizando a chave gerada pelo TOTP que utiliza a LMK compartilhada entre o SC e o MI. Uma possível variação nesse processo seria permitir que o CD atue como agregador de dados. Nessa variação, a resposta do MI seria cifrada apenas na K_DLTS ao invés do TOTP. Assim, o CD é capaz de decifrar o conteúdo para agregar e consolidar informações para serem transmitidas para o SC, reduzindo seu processamento.

### 4.2 *Controle de acesso leve*

Apesar da abordagem proposta prover segurança fim-a-fim na comunicação entre dispositivos da IoT, o controle de acesso para IoT continua sendo um desafio a ser resolvido. Isso ocorre porque a autorização provida pelo *token de acesso* limita o acesso a um recurso protegido, mas não suporta políticas determinando operações sobre esses recursos. Assim, não é possível estabelecer um controle de acesso fino nos recursos protegidos.

A arquitetura tradicional de um controle de acesso é tipicamente composta por um monitor de referência, uma base de autorização e um mecanismo guardião [Ferraiolo et al. 2003]. Entretanto, essa arquitetura não é adequada às restrições de recursos computacionais dos dispositivos da IoT. Com base nisso, propomos um controle de acesso leve, do ponto de vista de processamento, transmissão, memória e criptografia simétrica. Esse mecanismo aproveita as configurações estabelecidas na seção 4.1 para propor um controle de acesso baseado em papéis, no qual o usuário possui direitos de acesso de acordo com o seu papel na organização. Entretanto, esse mecanismo não adota o conceito de sessões, definido no modelo RBAC [Ferraiolo et al. 2003], para simplificar a implementação e implantação em dispositivos da IoT.

Para acessar um determinado MI, três papéis podem ser definidos, por exemplo: (i) *operador*: realiza consultas (operações de leitura) nos recursos protegidos; (ii) *administrador*: realiza parametrizações (operações de escrita) nos recursos protegidos; (iii) *fabricante*: realiza operações de leitura e escrita nos MI, inclusive atualizações de *firmware*. Outros papéis e permissões poderiam ser definidos, porém para simplificar consideramos somente esses três. Cada um desses papéis possui um *contador dinâmico*

de TOTP associado, tanto no SC quanto no MI (Figura 3). Assim, quando um determinado administrador desejar acessar um MI, ele deve cifrar a requisição utilizando a senha descartável produzida pelo TOTP associado. Nesse caso, o TOTP utiliza um *contador dinâmico* de administrador com a LMK de um MI específico para produzir a senha descartável que será utilizada como chave simétrica.

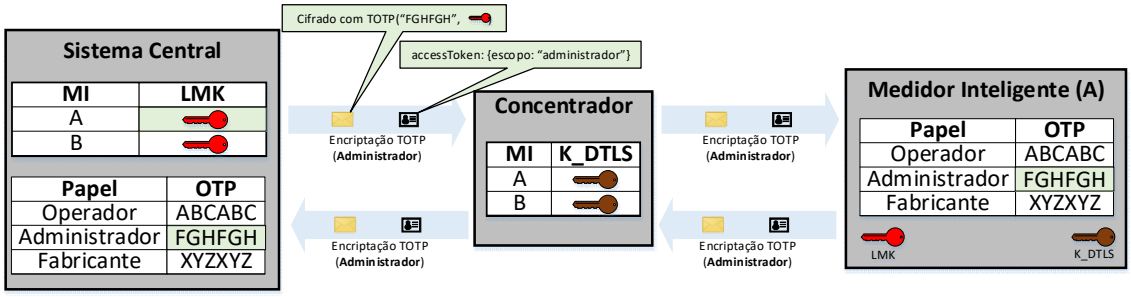


**Figura 3. Administrador acessando um recurso protegido da IoT.**

Quando o MI receber a requisição, tentará decifrar a mensagem utilizando cada *contador* associado aos papéis, começando pelo operador, seguido do administrador e fabricante. Essa sequência poderia ser ordenada pela frequência de operações de cada papel, por exemplo. Para garantir que o MI obtenha sucesso na decifração, o SC encaminha o identificador da requisição decifrado e o mesmo identificador cifrado na chave gerada pelo TOTP. Se o identificador decifrado for igual ao identificador recebido, isso significa que o *contador* utilizado está correto, sendo possível inferir no papel vinculado.

Além disso, esse controle de acesso é baseado em duas etapas, pois para que o usuário obtenha autorização no controle de acesso, ele deve atender a dois requisitos: (i) possuir um *token de acesso* com o escopo apropriado a requisição realizada; (ii) conseguir decifrar a resposta do MI, que foi cifrada na LMK e no *contador* do papel. Ou seja, para que o adversário consiga comprometer o MI, deve possuir o *token de acesso* e o *contador* do papel.

## 5. Protótipo

O protótipo foi desenvolvido com a utilização de padrões, tecnologias consolidadas e bibliotecas de código aberto. A implementação do IAM utilizou como base a plataforma WSo2 Identity Server, que é um servidor de gestão de identidade e acesso que permite a utilização de diversos protocolos, como: OpenID, OpenID Connect, SAML, Passive STS etc. Para realizar a autenticação, o protocolo OpenID Connect foi configurado como IdP no WSo2. O protocolo OAuth 2.0, presente no OpenID Connect é responsável pela autorização de acesso que emite *tokens de acesso* no formato JWT (*JSON Web Token*).

A Figura 4 apresenta a arquitetura proposta ressaltando a pilha de protocolos utilizada em cada uma das entidades para garantir a comunicação segura. Na perspectiva da Internet, é utilizado o HTTPS. Já na perspectiva da IoT, é utilizado o CoAP com o DTLS, que é popularmente chamado de CoAPs. O protocolo CoAP é baseado na arquitetura REST, nos quais os recursos são acessados a partir de uma URL. O CoAP utiliza o UDP na camada de transporte, pois é um protocolo adequado aos dispositivos com poucos recursos computacionais.

O CD foi implementado em Java, sendo que sua interface com a Internet utiliza um servidor HTTP, enquanto a interface com a IoT utiliza a biblioteca Californium[1] que disponibiliza um servidor CoAP. Dessa maneira, o CD pode converter as mensagens entre HTTP e CoAP, e vice-versa. O MI foi implementado em Java, utilizando também a biblioteca Californium, e executado no ContikiOS[2]. Foi utilizado o algoritmo AES com chaves de 128 bits para criptografar as mensagens. A biblioteca Scandium[3], pertencente ao subprojeto da Californium, foi utilizada para realizar o DTLS versão 1.2. Para realizar a geração de senhas descartáveis, foi utilizada a biblioteca AeroGear[4], e a biblioteca Jersey[5] para disponibilizar serviços REST.

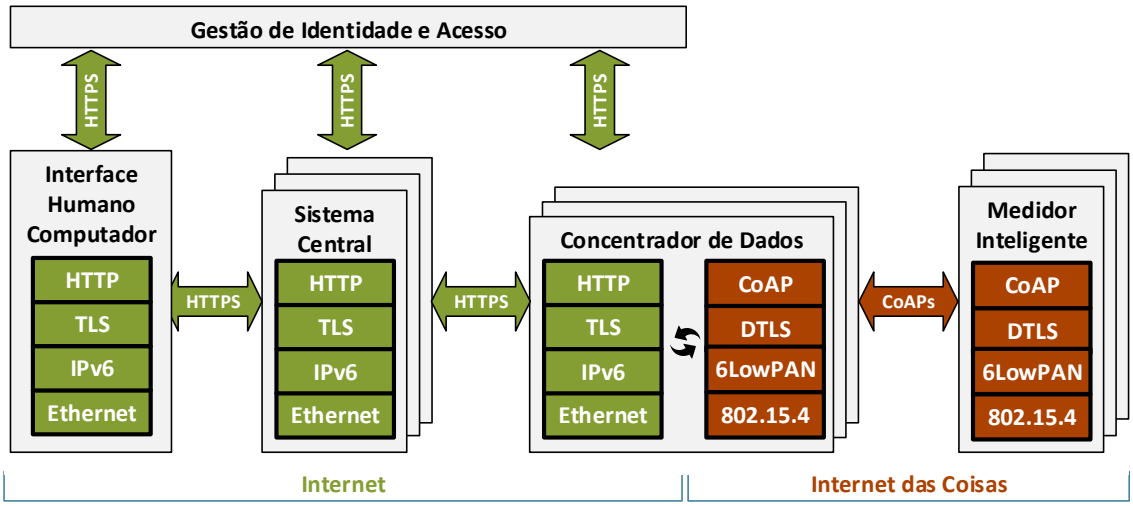


**Figura 4. Visão geral da pilha de protocolos de rede.**

## 6. Avaliação

Para realizar a avaliação um ambiente controlado foi desenvolvido, no sentido de prevenir possíveis interferências nas medições. Um total de quatro máquinas físicas foram conectadas em rede Gigabit. Todas as máquinas físicas possuem a mesma configuração de hardware, com processadores core i7 e 8 GB memória RAM. Uma máquina foi utilizada para hospedar o IAM, e as demais para executar os simuladores de Contiki[6]. Nossa abordagem utilizou o DTLS para proteger a comunicação entre dispositivos da IoT. A Figura 5 apresenta a comparação entre requisições CoAP e CoAPs (com DTLS), em que o eixo vertical apresenta o tempo de resposta em milissegundos, e o eixo horizontal apresenta o tamanho da requisição em bytes. Esse consumo está relacionado ao procedimento de autenticação no IAM. Observe que o impacto decorrente do DTLS não é proporcional, sendo vantajoso do ponto de vista de segurança.

[1] https://www.eclipse.org/californium/
[2] http://www.contiki-os.org/
[3] https://github.com/eclipse/californium.scandium
[4] https://aerogear.org/docs/specs/aerogear-security-otp/
[5] https://jersey.github.io/
[6] https://www.contiki.com

Para avaliar a abordagem proposta de segurança fim-a-fim utilizando OTP, foi realizado uma comparação com a abordagem proposta por Witkovski (2015). A abordagem proposta por Witkovski (2015) utiliza o conceito de hierarquia de chaves, na qual a comunicação é realizada de maneira desacoplada e assíncrona. Dessa maneira, o SC não consegue injetar informações diretamente no MI, apenas deposita informação no CD. Tal abordagem mitiga a possibilidade de o adversário injetar código malicioso ou controlar o MI, uma vez que não possui sessão interativa.

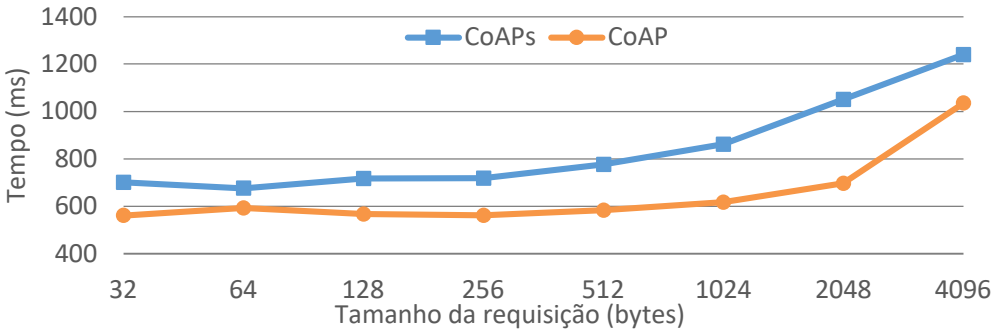


**Figura 5. Comparação de requisições CoAPs e CoAP.**

Para estabelecer a comunicação, o MI frequentemente consulta o CD, verificando se existem requisições pendentes. Da mesma maneira, após o SC realizar uma requisição no CD, frequentemente consulta pela resposta de sua requisição baseado no conceito de ticket. Esse desacoplamento entre entidades aumenta significativamente o número de mensagens trafegadas, devido ao *pooling* realizado. Essa característica é agravada quando o contexto de IoT é considerado, pois possui restrições de largura de banda e bateria. Além disso, para o SC e o MI obterem a DK, diversas mensagens são necessárias. Considerando um contexto cujo o número de MI é elevado, a situação se agrava ainda mais, uma vez que a comunicação é *unicast*.

Nossa abordagem baseada em OTP possui três principais vantagens em relação a abordagem de Witkovski (2015). Primeiramente, reduz o número de mensagens trocadas utilizando a comunicação *multicast* entre o SC e os MIs. É importante ressaltar que a abordagem mantém a segurança da comunicação utilizando criptografia de grupo nas requisições *multicast*. E as respostas das requisições são criptografadas em uma comunicação fim-a-fim utilizando chaves geradas pelo TOTP. Observe que a chave criptográfica utilizada na requisição (OTP) é mais fraca do que a chave criptográfica (TOTP) utilizada na resposta, uma vez que a resposta contém informações sensíveis.

| Característica | Witkovski (2015) | OTP |
|---|---|---|
| Quantidade de mensagens | $n * 13$ | $6 + (n*3)$ |
| Criptografia simétrica no contexto de IoT | $n * 4$ | $n * 4$ |
| Funções hash no contexto de IoT | 0 | n |
| Geração de chaves no contexto da IoT | $n * 2$ | $n * 3$ |
| Compartilhamento de *contador* | 0 | $n * 2$ |

**Tabela 1. Comparação entre as abordagens de comunicação fim-a-fim.**

Além disso, a abordagem baseada em OTP permite que a chave K_DLTS seja facilmente atualizada, enquanto na abordagem de Witkovski (2015) a K_DTLS deve ser

definida manualmente. Finalmente, nossa abordagem baseada em OTP adiciona flexibilidade no processo, pois permite que o CD atue como *gateway* ou como agregador. A tabela 1 apresenta a avaliação dos parâmetros entre as abordagens, considerando *n* o número de MIs na comunicação.

A comparação do número de mensagens necessárias nas abordagens é apresentada na Figura 6. Observe que a relação do custo de processamento (número de cifras, geração de chaves e funções hash) é semelhante entre as abordagens, sendo que a maior diferença entre as abordagens é apresentada quando o número de MI é elevando. Quando o número de MI é superior a 512, a abordagem de Witkovski (2015) se mostra que não é escalável. É importante destacar, que apesar de uma arquitetura de SG tipicamente ser composta por milhões de MIs, cada CD não possui um número elevado de MI.

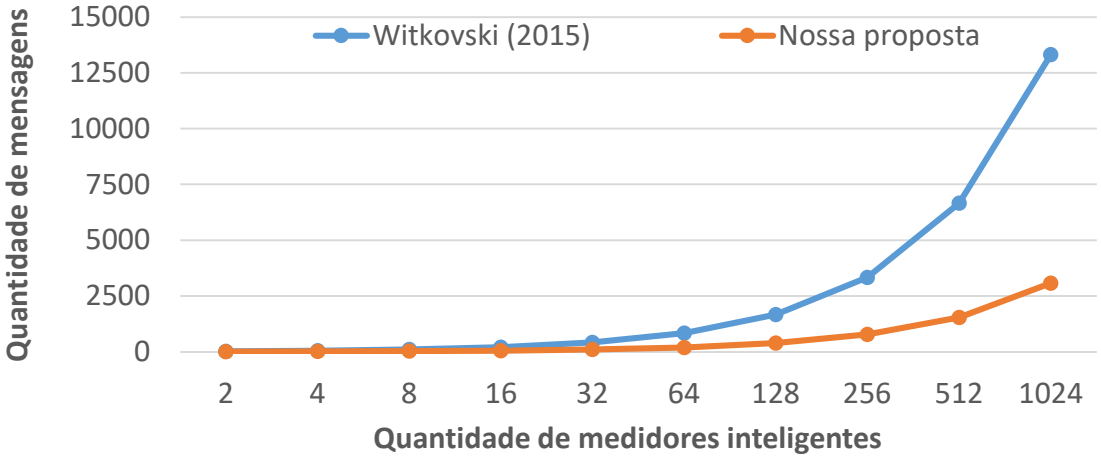


**Figura 6. Comparação entre as abordagens de comunicação fim-a-fim.**

Em termos de configuração inicial, nossa abordagem baseada em OTP possui mais parâmetros, que entretanto, são configurados de maneira dinâmica. Por outro lado, na abordagem de Witkovski (2015) os parâmetros são definidos manualmente. A Figura 7 apresenta o tempo de configuração inicial da abordagem baseada em OTP. Observe que o tempo de resposta é proporcional ao número de MI. Essa configuração inclui a distribuição segura da chave DTLS.

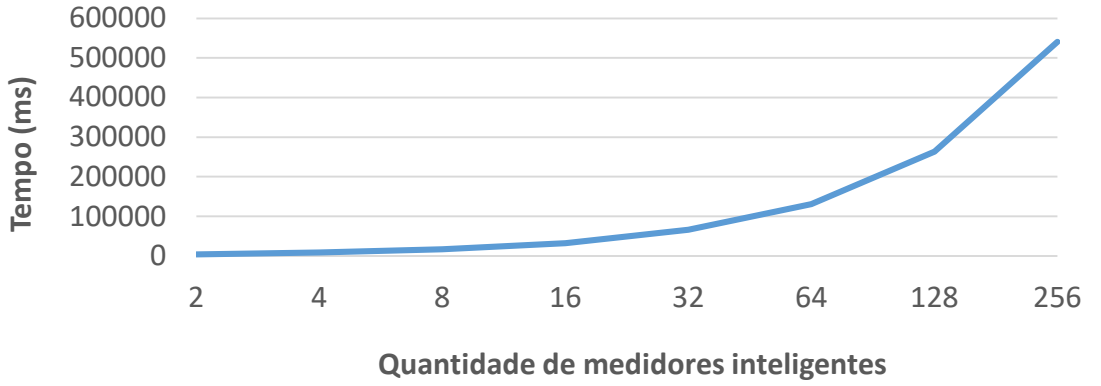


**Figura 7. Configuração inicial da abordagem baseada em OTP.**

## 6. Conclusão

A SG provê inúmeros benefícios para a sociedade através do emprego de inteligência computacional e tecnologias de comunicação de maneira integrada. Entretanto, esses benefícios implicam em desafios de cibersegurança que requerem mecanismos mais eficientes no combate aos frequentes ataques cibernéticos. A literatura carece de mecanismos de cibersegurança adequados às características da SG. Esse trabalho apresentou uma abordagem de comunicação *multicast* seguro para IoT baseado em OTP, adequado as restrições computacionais. Essa abordagem permitiu definir a chave DTLS de maneira dinâmica e segura. Além disso, esse trabalho apresentou um controle de acesso leve para IoT baseado em papéis, que permite o controle fino sobre os recursos protegidos. Nossa abordagem de segurança fim-a-fim baseada em OTP tem como principal vantagem a eficiência nas trocas de mensagens, adotando a comunicação *multicast* sem comprometer a segurança. A avaliação da proposta apresentou um desempenho superior ao trabalho identificado na literatura, além de apresentar maior flexibilidade na configuração dos parâmetros.

## Referências


A. A. Chavan and M. K. Nighot, “Secure and Cost-effective Application Layer Protocol with Authentication Interoperability for IOT,” in Physics Procedia, 2016, vol. 78, pp. 646–651.

A. Cárdenas, S. Amin, and S. Sastry, “Research Challenges for the Security of Control Systems,” Netw. Secur., p. 6, 2008.

A. Witkovski, A. Santin, V. Abreu, and J. Marynowski, “An IdM and key-based authentication method for providing single sign-on in IoT,” in 2015 IEEE Global Communications Conference, GLOBECOM 2015, 2015.

D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli, “Role-Based Access Control,” Components, vol. 2002, no. 10, p. 338, 2003.

D. M'Raihi, S. Machani, M. Pei and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm", RFC 6238, DOI 10.17487/RFC6238, 2011..

Hacker News, “Millions of IoT Devices Using Same Hard-Coded CRYPTO Keys,” 2015. [Online]. Disponível em: http://thehackernews.com/2015/11/iot-devicecrypto-keys.html.

IEC Smart Grid Standardization Roadmap. [Online]. Disponível em: https://www.iec.ch/smartgrid/downloads/sg3_roadmap.pdf.

Infoworld, “Millions of embedded devices use the same hard-coded SSH and TLS private keys,” 2015. [Online]. Disponível em: http://www.infoworld.com/article/3009667/security/millions-ofembedded-devices-use-the-same-hard-coded-ssh-and-tls-privatekeys.html.

J. L. Hou and K. H. Yeh, “Novel Authentication Schemes for IoT Based Healthcare Systems,” Int. J. Distrib. Sens. Networks, vol. 2015, 2015.

J. Liu, Y. Xiao, and C. L. P. Chen, “Authentication and Access Control in the Internet of Things,” International Conference on Distributed Computing Systems Workshops, 2012, pp. 588–592.

K. Ammayappan, A. Saxena, and A. Negi, “Mutual authentication and key agreement based on elliptic curve cryptography for GSM,” in Proceedings - 2006 14th International Conference on Advanced Computing and Communications, ADCOM 2006, 2006, pp. 183–186.

L. A. R. Shantha Mary Joshitta, “Authentication in IoT Environment: A Survey,” International J. Adv. Res. Comput. Sci. Softw. Eng., vol. 6, no. 10, 2016.

Mallmann, J., Santin, A. O., Viegas, E. K., dos Santos, R. R., and Geremias, J. (2020). PP-Censor: Architecture for real-time pornography detection in video streaming. Future Generation Computer Systems, 112:945–955.

NIST, “Framework for Improving Critical Infrastructure Cybersecurity,” 2014.

O. Garcia-Morchon, S. L. Keoh, S. Kumar, P. Moreno-Sanchez, F. Vidal-Meca, and J. H. Ziegeldorf, “Securing the IP-based internet of things with HIP and DTLS,” in ACM conference on Security and privacy in wireless and mobile networks WiSec, 2013, p. 119.

P. McDaniel and S. McLaughlin. Security and privacy challenges in the smart grid. IEEE Security & Privacy, 7(3):75–77, 2009.

Ramos, F., Viegas, E., Santin, A., Horchulhack, P., dos Santos, R. R., and Espindola, A. (2021). A machine learning model for detection of docker-based APP overbooking on kubernetes. In ICC 2021 - IEEE International Conference on Communications. IEEE.

R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” IEEE Secur. Priv., vol. 9, no. 3, pp. 49–51, 2011.

Tomio, R. L., Viegas, E. K., Santin, A. O., and dos Santos, R. R. (2021). A multi-viewintrusion detection model for reliable and autonomous model updates. In ICC 2021 -IEEE International Conference on Communications. IEEE.

Vicentini, C., Santin, A., Viegas, E., and Abreu, V. (2018). A machine learning auditing model for detection of multi-tenancy issues within tenant domain. 2018 IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CC-GRID).

Vicentini, C., Santin, A., Viegas, E., and Abreu, V. (2019). SDN-based and multitenant-aware resource provisioning mechanism for cloud-based big data streaming. Journal of Network and Computer Applications, 126:133–149.

Viegas, E., Santin, A. O., and Jr, V. A. (2021). Machine learning intrusion detection in big data era: A multi-objective approach for longer model lifespans. IEEE Transactions on Network Science and Engineering, 8(1):366–376.

V. C. Gungor, B. Lu, and G. P. Hancke. Opportunities and challenges of wireless sensor networks in smart grid. IEEE Trans. Ind. Electron., 57(10):3557–3564, 2010.

V. L. Shivraj, M. A. Rajan, M. Singh, and P. Balamuralidhar, “One time password authentication scheme based on elliptic curves for Internet of Things (IoT),” Natl. Symp. Inf. Technol. Towar. New Smart World, no. c, pp. 1–6, 2015.

W. L. Chin, Y. H. Lin, and H. H. Chen, “A Framework of Machine-to-Machine Authentication in Smart Grid: A Two-Layer Approach,” IEEE Com. Mag., vol. 54, no. 12, pp. 102–107, 2016.

X. Fang, S. Misra, G. Xue, and D. Yang, “Smart grid - The new and improved power grid: A survey,” IEEE Communications Surveys and Tutorials, vol. 14, no. 4. pp. 944–980, 2012.

Y. Ashibani and Q. H. Mahmoud, “Cyber physical systems security: Analysis, challenges and solutions,” Comput. Secur., vol. 68, pp. 81–97, 2017.

Y. C. Y. Cao and L. Y. L. Yang, “A survey of Identity Management technology,” 2010 IEEE Int. Conf. Inf. Theory Inf. Secur., pp. 287–293, 2010.

Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo, and F. Xie, “Cyber-physical system risk assessment,” in Proceedings - 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2013, 2013, pp. 442–447.

ZDnet, “Smart meter hacking tool released,” 2021. [Online]. Disponível em: http://www.zdnet.com/article/smart-meter-hacking-tool-released/.