Redes de Computadores aprimoradas por SDN e NFV com o uso de Gêmeos Digitais

Francisco Paiva Knebel
Instituto de Informática
Universidade Federal do Rio Grande do Sul
Email: francisco.knebel@inf.ufrgs.br

I. Introdução

Um gêmeo digital é uma representação virtual e digital de um sistema real físico, podendo ser utilizado para prever estados futuros da entidade física. O gêmeo digital é integrado com outras tecnologias, como inteligência artificial, mineração de dados, computação em nuvem e a Internet das Coisas (*Internet of Things*, IoT). Através de protocolos de comunicação, o gêmeo digital e seu equivalente físico estão intrinsecamente conectados, gerando um fluxo de informações em tempo real dos sensores físicos ao gêmeo, e dele para atuadores do sistema físico. Isso permite a coleta de informações do funcionamento do sistema e a sugestão por parte do gêmeo de ações sobre o sistema real, permitindo um produto mais eficiente e criando inteligência pela análise dos processos efetuados.

A arquitetura de um gêmeo digital implica na criação de uma réplica digital de algo, sendo ela uma pessoa ou objeto quaisquer, em um ambiente virtual e então conectando ambos através de uma conexão de rede, permitindo a troca de informação em tempo real entre os gêmeos. Implementando-se em um sistema industrial, uma máquina conectada poderia ser modificada por humanos interagindo com seu gêmeo digital, com operações sendo despachadas do ambiente virtual para o gêmeo real [1]. Um gêmeo digital de um componente é uma entidade de software que espelha outro componente, podendo ele ser um sistema ciberfísico (CPS, *Cyber Physical System*), como um sensor ou uma linha de produção, até um processo de produção ou uma fábrica inteira. Esses componentes digitais podem ser utilizados para simular e testar a operação de um produto antes de comprometer o sistema real a funcionar da mesma forma [2].

Com este trabalho, é pretendido obter o estado da arte de Gêmeos Digitais para Redes de Computadores, com ênfase em trabalhos quem implementem ou discutam possíveis soluções no contexto de redes programáveis baseadas em software, utilizando as tecnologias de SDN (*Software Defined Networking*) e NFV (*Network Functions Virtualization*).

O trabalho está separado da seguinte forma: na seção II está descrito a metodologia de pesquisa, como foram obtidos os trabalhos e os critérios de inclusão e exclusão utilizados; na seção III, o conteúdo da pesquisa é apresentado, separado pela classificação dos temas dos artigos; e na seção IV é efetuada a conclusão sobre os resultados obtidos.

II. Metodologia

Por se tratar de uma pesquisa sistemática, foram seguidas regras estritas para a seleção de trabalhos. Como ferramenta de busca, o levantamento de artigos foi feito com o auxílio do Google Scholar, efetuando a busca manualmente pelos principais artigos retornados para cada *query* de pesquisa. Uma série de pesquisas foram efetuadas separadamente, de forma a incluir trabalhos que cobrem suficientemente o assunto da pesquisa. Em seguida, após a obtenção dos trabalhos, foi feito a classificação dos artigos para incluir nesta pesquisa.

A. Pesquisa

O objetivo inicial da pesquisa é definir o estado da arte da pesquisa de gêmeos digitais nos contextos de redes programáveis, em específico sobre as contribuições que utilizam os conceitos de SDN e NFV. Efetuando um corte dos trabalhos que relacionam essas três palavras-chave, conforme a Fig. 1, podemos obter de qual forma o uso de SDN e de NFV estão sendo usados no contexto de gêmeos digitais para a criação e manutenção de redes de computadores.

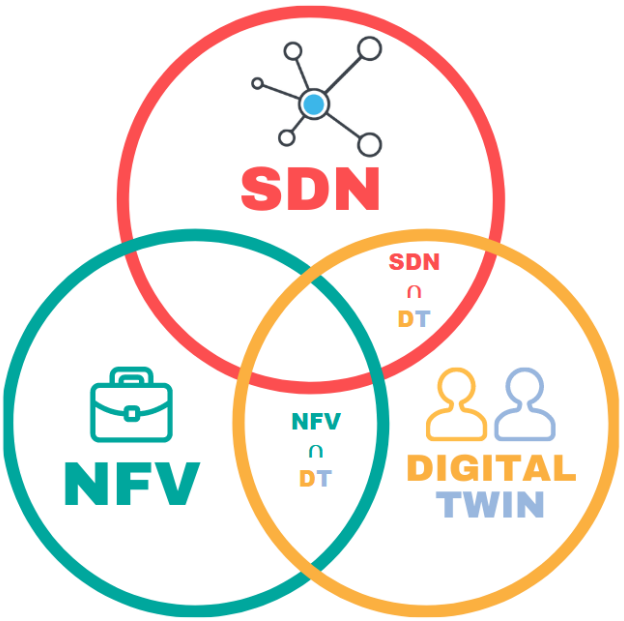

Fig. 1. Assuntos-chave da pesquisa.

Para obter cada um dos subgrupos de artigos utilizados como referência para este estudo, foi efetuado uma série de pesquisas via Google Scholar, utilizando o seu algoritmo próprio para classificar a relação da pesquisa com a qualidade do artigo. Todas as pesquisas foram efetuadas em Abril de 2022 e não efetuaram corte de artigos pelo período de publicação. Os seguintes termos foram utilizados:

1) **"Digital Twin" SDN**: inclusão de trabalhos que ligam diretamente gêmeos digitais com SDN. Obtido 980 resultados.
2) **"Digital Twin" NFV**: inclusão de trabalhos que ligam diretamente gêmeos digitais com NFV. Obtido 425 resultados.

Cada uma das pesquisas efetuadas retornou uma quantidade considerável de artigos para seleção, o que gera uma preocupação com a obtenção de artigos suficientes. Por não se tratar de uma pesquisa sistemática exaustiva, foram obtidos os primeiros 100 artigos para cada pesquisa, utilizando a ordenação por relevância do próprio Google Scholar como critério de exclusão. Dessa forma, por se tratarem de duas pesquisas, foram obtidos uma lista de 200 artigos para serem classificados.

B. Classificação

Com a lista de artigos obtida, várias etapas de classificação foram efetuadas para reduzir a lista de artigos que seriam incluídos na leitura manual. Os seguintes critérios de exclusão foram utilizados, efetuando análise manual sobre o conjunto de artigos:

1) **Exclusão por duplicata**: Artigos que apareceram em mais de uma das pesquisas, além de artigos que aparecem repetidos dentro de uma pesquisa. Exclusão de 43 artigos.
2) **Exclusão por linguagem**: Artigos publicados em outra linguagem além da língua inglesa. Exclusão de 7 artigos.
3) **Exclusão por acesso ao artigo**: Artigos que não puderam ser livremente obtidos ou através de distribuidoras com fácil acesso foram excluídos. Na maioria dos casos, os resultados são livros ou capítulos de livros. Exclusão de 13 artigos.
4) **Exclusão por falso-positivo**: Filtro manual, efetuado durante leitura final da lista, por entradas que apenas mencionam as palavras-chaves, mas que não apresentam contribuições, além de casos óbvios de inclusão incorreta feita pelo Google Scholar, como trabalhos de outro contexto, não de redes de computadores, fora do contexto da pesquisa. Exclusão de 70 artigos.

Dessa forma, da lista inicial de 200 artigos incluídos pela pesquisa, 133 foram removidos devido aos critérios de exclusão. Deste montante, restaram após a filtragem por todos critérios um total de 67 trabalhos incluídos na pesquisa final[1].

[1]Dados da pesquisa, incluindo a lista completa e cada etapa do processo de exclusão podem ser vistos em uma planilha pública, disponível em: https://github.com/Open-Digital-Twin/article-sdn-nfv-digital-twins/raw/main/TF-Research.xlsx

III. Pesquisa

Com a leitura dos artigos, foram definidas múltiplas categorias de trabalhos, sendo o seu conteúdo resumido nas subseções seguintes e seus artigos classificados.

A. Gêmeos Digitais para Redes

O IETF (Internet Engineering Task Force) possui um grupo atualmente trabalhando na padronização do conceito de uma plataforma de gêmeos digitais para redes [3], emulando os elementos da rede digitalmente. A principal diferença entre sistemas tradicionais de gerenciamento é a interatividade virtual e real, digital e físico, construindo um sistema fechado e automatizado, que se comunica para aprender. Através da integração de dados em tempo real da rede física com sua equivalente digital, a plataforma pode ser simplificada, se tornar mais resiliente e efetuar manutenção sobre todo o ciclo de operação. O gêmeo digital construído possibilita a rápida detecção e solução de problemas na rede, predição de status futuro da rede e melhora na sua confiabilidade por eliminar riscos conhecidos antes de acontecerem.

Digitalização de um sistema físico para o gêmeo digital necessita de desacoplamento de informação e de funções. Desacoplamento de informação (ou desacoplamento de dados) permite a representação do estado geral do sistema, efetuando o design do sistema de forma independente dos dispositivos de rede [4]. Desacoplamento de função se refere a alocação de recursos, de administração de mobilidade, desacoplando as funções de gerenciamento da camada física para a camada virtual. Pode ser implementado pelo fatiamento de rede baseado em NFV e SDN, separando o plano de controle da interação física para facilitar a administração das funções de rede. O uso de SDN simplifica e torna mais eficiente a elevação de processos mais complexos, que necessitam de supervisionamento e administração dinâmica de recursos, requerendo reconfiguração dos elementos de rede [1].

Um gêmeo digital separa as funções de controle, implantadas como um sistema logicamente centralizado, dos dispositivos físicos sob controle, de forma similar ao SDN. Em uma arquitetura de rede baseada em SDN, o plano de controle é separado do plano de dados, permitindo ao SDN centralizar o processo de controle e permitir a implementação de uma rede programável, dinamicamente alterando-se com as demandas de tráfego exigidas [5], além de expôr visibilidade total das configurações da rede e o seu estado, além de efetuar o controle de fluxos [6]. O controlador SDN coleta informações sobre todo o sistema interconectado, podendo ser o local de formulação de estratégias para garantir o seu funcionamento [7], além de fornecer informações e a conexão necessária para aprendizado sobre o estado global da rede [8]. Da mesma forma, gêmeos digitais permitem a realização de tomada de decisões e controle de processos em um ambiente centralizado, separando o processo de controle (no ambiente virtual) do plano de dados (ambiente real), definindo os fluxos e interações entre os dispositivos conectados e sua interação com o ambiente.

Outro aspecto de gêmeos digitais é a virtualização de objetos e processos físicos, uma visão paralela à NFVs, que permitem a implementação de funções de redes em forma de software, que pode ser executado em máquinas virtuais genéricas, ao invés de depender de equipamentos especializados, o que flexibiliza o desenvolvimento de novas funcionalidades para a rede. Gêmeos digitais estendem o conceito para a virtualização de qualquer função lógica vinda de objetos ou processos.

Uma rede implementada com gêmeos digitais permite o desenvolvimento de soluções com otimizações ótimas, solucionando problemas, efetuando análise de cenários e planejando melhoras na rede levando em consideração simulações do crescimento esperado. Além disso, todos esses processos podem ser efetuados sem prejudicar a rede física, ocorrendo puramente no ambiente virtualizado. Operadores de rede podem reproduzir falhas anteriores, para descobrir a origem da disrupção de serviço, além de auxiliar em soluções para prevenir disrupções futuras. Estudos sobre gargalos, más configurações de rede, observação de performance em caso de perda de *links* e detecção automática de anomalias são alguns benefícios fornecidos por uma implementação baseada em gêmeos digitais [9].

Em um ambiente NFV, detecção, diagnóstico e resolução de componentes falhos na rede dependem de intervenção humana, mas com o crescimento e diversificação das redes, como pela customização de funções virtualizadas de rede (VNF, *Virtualized Network Function*) baseadas em requisições dos usuários para gerarem funções personalizadas, soluções para resolução de problemas operacionais de forma autônoma são necessárias. Para resolver esse problema, algumas soluções são sugeridas: detecção de anomalias para encontrar padrões em dados que não são esperados; análise de causa raiz (Root Cause Analysis, RCA) serve para encontrar componentes falhos causando anomalias e encontrar as causas para degradação de serviço, como latência, que podem ser causadas por diferentes razões; e compensação, para executar ações e recuperar a rede para seu estado anterior, antes da falha, após corrigido. Para obter a dependência de uma relação com falhas anômalas e implementar essas soluções, um gêmeo digital pode ser introduzido, continuamente se atualizando com o ciclo de vida da rede. Através do monitoramento da rede física, o gêmeo digital é capaz de capturar a dependência anômala, além de poder facilmente criar e transferir o conhecimento para uma nova instância dessa dependência [10]–[12].

B. 5G, 6G e Sistemas Wireless

SDN oferece a separação do plano de controle do plano de dados. Em um plano de controle típico de SDN, um único controlador centralizado é usado para controlar os múltiplos *switches*, que executam diferentes funções [13], [14]. Controladores formam o plano de controle, tomando controle da rede e comandando os dispositivos do plano de dados. Eles também coletam informações da rede física, e um gêmeo digital acoplado pode tomar vantagem dessa conexão para efetuar monitoramento da rede, efetuar manutenção preditiva e diagnosticar a rede. O funcionamento dependente de um único controlador centralizado pode sofrer com problemas de escalabilidade e confiabilidade, além de que o aumento de dispositivos irá causar um aumento de latência, por isso é sugerido uma implementação híbrida, contendo controladores centralizados e distribuídos, onde o controlador centralizado é responsável pelos controladores locais [4]. NFV oferece implementação eficiente e de custo-beneficio de funções de rede usando máquinas virtuais operando em hardware genérico [15].

O fatiamento de rede é uma estratégia proeminente para manter a mesma infraestrutura disponível para múltiplos operadores. Ele funciona através da virtualização dos recursos de rede e alocação de partes dele (logo o termo fatia) para cada parte interessada. SDN permite a administração dos recursos através de suas políticas implementadas, ao mesmo tempo que NFV desacopla as funções de rede dos dispositivos físicos que executam tais funções para implantação em máquinas virtuais [16]. As fatias de rede são isoladas logicamente e redes virtualizadas compartilhando uma infraestrutura física comum podem ser administrados e controlados para suportas um provisionamento de serviços flexível, afim de satisfazer as necessidades dos usuários [17]. Fatiamento de rede pode ser utilizado para prover recursos sob medida para a indústria 4.0, mas sua implementação, devido ao aumento de complexidade da rede é um desafio. A rede é dividida em fatias de rede baseadas nos serviços que ela suporta, mantendo a mesma infraestrutura física, que operam de forma independente e podem ser otimizados para a utilização para os requisitos de um usuário específico [18]. SDN e NFV decompõem o formato monolítico e proprietário de redes tradicionais em módulos menores chamados VNFs (Virtual Network Functions), sendo executadas em hardware genérico ao invés de *switches* dedicados. Um desafio de computação distribuída é criada pelo fatiamento: como acomodar múltiplas fatias de rede utilizando os mesmos recursos de rede. Exemplos são o isolamento de conectividade da fatia, ou seja, usuários de uma fatia não podem se comunicar com serviços de outras fatias, e de isolamento de performance, onde uma fatia não deve afetar o funcionamento de outra [19]. O escalonamento automático de VNFs, para lidar com a demanda, introduz vantagens em menor custo de implantação e taxa de insatisfação das requisições pelos serviços, além de maior capacidade de resiliência para falhas de hardware. Entretanto, sistemas distribuídos introduzem complexidade para a computação, podendo gerar inconsistência de dados e gerando problemas de sincronização [20].

Larsson [21] implementa virtualização da rede utilizando P4, avaliando em termos de escalabilidade de redes distribuídas, considerando cada rede como um gêmeo, que pode estar distribuído através de diferentes locais, conectados num *backbone* comum. Os resultados da implementação em P4 são comparados com implementações não-baseadas em P4, de trabalhos relacionados. Performance das diferentes tecnologias são avaliadas, e o autor considera duas soluções para virtualização da rede: uma com aprendizado baseado no

plano de dados e outra com aprendizado baseado no plano de controle. O nível de programabilidade fornecido por iniciativas como o P4 facilita a implementação de novos protocolos rapidamente, mas que não é possível concluir que o uso de uma tecnologia ou outra para virtualização de redes distribuídas é a melhor, pois dependo do contexto da aplicação, mas que a implementação em P4 permitiu grande escalabilidade sem *switches* físicos.

O uso de gêmeos digitais pode ser efetuado para criar uma representação virtual de redes fatiadas, afim de simular seus comportamentos e prever sua performance. A implementação é feita através de nodos e link, que podem ser divididos e isolados em contêineres e links virtuais, contendo VNFs. Gêmeos digitais podem beneficiar o gerenciamento das fatias de rede pela criação das representações virtuais dos pedaços físicos da rede, podendo ser usado para simular cenários sem afetar a rede real. [22]. Para tirar vantagem do fatiamento de rede, é crítico o monitoramento eficiente da rede, com geração de métricas suficientes para efetuar o gerenciamento autônomo e a orquestração dinâmica da rede para garantir os requisitos de QoS (Quality of Service) das aplicações. Entretanto, a automação dessa garantia representa desafios adicionais na orquestração de serviços, com a alocação dinâmica de recursos e escalonamento automático. Para garantir que as fatias suportem os requisitos dos serviços, os provisores terão que implementar inteligência nos serviços e na rede, além de conhecimento do contexto por parte da fatia [23].

A implementação do 5G ainda é muito recente e introduz muitos desafios. Com o suporte de inteligência artificial, o uso de gêmeos digitais para redes 5G tem potencial de facilitar e completar a sua implementação. NFV e SDN permitem a flexibilidade de posicionamento das funções de rede, na borda ou na nuvem, implantando apenas as funções necessárias [2], [24]. Requisitos de indústrias verticais do 5G[2] muitas vezes são contraditórios, impondo latências extremamente baixas ao mesmo tempo que outros demandam taxas de banda extremamente altas, tornando difícil a definição de redes de propósito genérico [25], [26]. Podemos extrapolar o conceito de gêmeos digitais em redes até o futuro 6G, onde taxas de dados extremamente altos com baixíssima latência serão a norma. O conceito de desacoplamento será essencial para a implementação do 6G. A combinação de SDN e NFV são fundamentais para o fatiamento da rede, mas o fatiamento necessário para o 6G será diferente: gêmeos digitais enriquecidos pelo 6G usarão uma representação digital do sistema físico, utilizando aprendizado de máquina para proativamente analisar e modelar as funções de rede. Junto de NFV, o fatiamento da rede será mais granular, otimizando o acesso a recursos [27]. Um gêmeo digital do 6G irá depender diretamente do fatiamento de rede, desacoplamento de dados, análise proativa e de otimização dos recursos fornecidos pela introdução de inteligência dentro da rede, que só poderá ocorrer com a introdução de programabilidade, de forma a obter uma orquestração de rede completamente autônoma [2], [13], [26], [28], [29]. Ao mesmo tempo que o 6G pode facilitar a realização e adoção de gêmeos digitais em múltiplas industrias, provendo os níveis necessários de confiabilidade e velocidade, gêmeos digitais com seu poder de inteligência artificial podem facilitar o design, implantação e operação do 6G. Uma implementação que leva em conta esses critérios pode ter alto impacto para atingir uma rede de alta confiabilidade [30]. Gêmeos digitais também podem ser utilizados para melhor o fatiamento da rede, provendo dados organizados e customizados para as fatias, refinando a abstração das fatias para um nível maior de personalização [31].

Redes programáveis, baseadas em software através de SDN e NFV, é uma das principais tecnologias facilitadoras para o 6G. Com a virtualização, o desacoplamento de serviços e permitindo maximizar o uso da rede entre os diferentes serviços usando a mesma infraestrutura possibilita que os provedores de serviço compartilhem dinamicamente da mesma rede de física que os operadores de rede móvel. O uso de SDN permitirá a reconfiguração dinâmica da topologia de rede de acordo com a demanda e adicionar mais recursos de rede para manter a qualidade de serviço para os usuários. Para os operadores de rede, isso significa uma rede mais fácil de monitorar e manter, com redução de CapEx (*Capital Expenses*, custo capital) e OpEx (*Operational Expenses*, custo operacional), além de inovação mais rápida, pela facilidade de implantação em software ao invés de hardware [32]–[34]. Para a implantação das redes 6G, é esperado que arquiteturas de rede baseadas em software utilizando infraestrutura definida em software seja amplamente utilizada [35].

Para a implementação de gêmeos digitais, o uso de tecnologias como computação de borda e NFV praticam um papel importante para o oferecimento de baixa latência, resiliência, alta banda e escalabilidade [36], [37]. *Multi-Access Edge Computing* (MEC) é um paradigma que combina esses elementos para que operadores abram acesso à rede para serviços tirarem vantagem da grande proximidade com o usuário, facilitado por NFV pela redução de custos de hardware através da virtualização, o provisionamento flexível (escalar para cima/baixo de acordo com a demanda) de recursos e a rápida instanciação de novos serviços. O *offloading* de funções para a computação na borda introduz reduções no desperdício de computação e uso de memória [38], [39].

Introduzindo serviços de rede altamente flexíveis automatizam muito do processo manual de configuração, mas a introdução de NFV em sistemas industriais ainda apresenta alguns desafios, como a integração de protocolos legados ainda usados em comunicação de máquinas existentes, que são consideravelmente diferentes de protocolos mais recentes, como REST, além da dificuldade de lidar com a complexidade de diferentes serviços virtualizados [40]. Além disso, implementar um gêmeo digital pode não ser a solução mais eficiente para muitos provedores, pois gera computação extra e um ponto adicional de ameaça para a segurança do sistema. Um cenário de aprendizado distribuído, como é o caso, causa custos de

[2]Um vertical da indústria é um termo utilizado para definir grupos de empresas com foco em um nicho específico ou com mercado especializado que abrange várias indústrias. Mais informações em "https://web.archive.org/web/20220311194057/https://pitchbook.com/what-are-industry-verticals".

armazenamento adicionais para a etapa de treinamento [41].

Uma proposta híbrida de SDN, adicionando um gêmeo digital, é proposta por Taylor [42] para adicionar mais funcionalidades para suportar grandes quantidades de nodos. O controlador centraliza a configuração de dispositivos de rede e monitoramento, e o gêmeo digital virtualiza os elementos na borda, recomendando configurações para o plano de controle. Para redes *wireless*, o plano de controle é um híbrido entre os planos de controle e dados, pois os dados de controle do *gateway* e do ponto de acesso podem ser transmitidos sem-fio junto com os pacotes de dados. Um gerenciador de topologia é implementado dentro do sistema, coletando dados de geolocalização dos nodos da rede, afim de se autoconfigurar, pela modificação dos nodos.

C. Internet das Coisas

Virtualização é um conceito diretamente ligado com a implementação de gêmeos digitais. Em redes, virtualização é baseado em melhor explorar o hardware disponível, executando diferentes aplicações utilizando o mesmo hardware genérico. Esse processo está normalmente acoplado com SDNs, efetuando o desacoplamento do hardware da rede do seu software controlador. Orquestração é fundamental para coordenar a alocação dos recursos, ou seja, computação, armazenamento e recursos de rede dentro da infraestrutura virtualizada. Virtualização da rede oferece a capacidade de lidar com a virtualização de funções, sua orquestração e o encadeamento entre diferentes serviços à infraestrutura do gêmeo digital [43].

A combinação de IoT com o ecossistema industrial é uma possibilidade de implementação de gêmeos digitais, permitindo redução de custos em equipamentos e manutenção, monitoramento de recursos, otimização de manutenção, economia de energia, além de possibilitar a conexão entre dispositivos inteligentes. SDN podem dinamicamente refletir os requisitos de comunicação necessários, levando em consideração as condições de rede, sendo um mecanismo de controle da importância das mensagens e do estado geral da rede, de forma a proporcionar a melhor qualidade de serviço possível definindo as regras de encaminhamento de cada elemento da rede. O controle efetuado define o caminho para as mensagens do gêmeo digital para garantir as condições de tempo-real necessárias [44]–[46]. A integração de tecnologia industrial, gêmeos digitais, SDN e NFV são habilitadoras para mover o processamento para a computação em borda. Fusão, aquisição e mineração de dados serão essenciais para essa implementação nos espaços industriais, mas apresentam desafios pela escala massiva de sistemas e tipos de dados a serem modelados até a integração com sistemas de aprendizado [47].

O uso de SDN para dinamicamente modificar como os nodos na borda administram os fluxos de tráfego, lidar com configurações e requisitos dinâmicos de QoS, como tolerância de latência, com capacidade de adaptação da rede. Metadados podem ser analisados pelo controlador para priorização de mensagens. SDN emergiu primariamente para administrar *switches* em *datacenters* fechados e centralizados, mas sua adoção provou seus benefícios em cenários com poder computacional e de capacidade de rede mais limitados. SDNs podem ser usados para manter os requisitos de latência e garantir QoS na troca de dados em tempo real, atingindo melhor sincronização e confiabilidade entre sistemas [48].

Focando em ambientes industriais, SDN em IIoT é primariamente usado em ambientes fechados, utilizando OpenFlow. SDN pode ser adotado para dinamicamente explorar os mecanismos de comunicação mais adequados para os requisitos da aplicação, como utilizando dados sobre o contexto do pacote para mais eficientemente definir regras de fluxo de tráfego [49]. Um gêmeo digital interligado com a rede pode efetuar o gerenciamento da rede internamente ao sistema, com o controlador da rede softwarizada conectando o gêmeo digital de cada parte do sistema industrial com o seu parceiro físico [14]. A precisão e tempo de reação de gêmeos digitais permitem o controle remoto por operadores humanos de robôs industriais a longas distâncias [50].

Para lidar com dispositivos em movimento, Santa et al [51] propõem que para a continuidade de processamento seja o objetivo, a transferência dos recursos de processamento e o estado da tarefa sendo processada deve ser efetuada para manter o serviço. A sua solução utiliza o conceito de *virtual mobile devices* (vMDs) como funções virtualizadas representando dispositivos físicos, instanciados na borda da rede, utilizando SDN para migrar os dispositivos ao longo da rede, sem perda de computação, através da transferência de estados de gêmeos digitais com capacidade de processar dados para dispositivos em movimento de forma transparente.

Redes Sensíveis ao Tempo (TSN, *Time Sensitive Networking*) é um tecnologia criada para a implementação de redes determinísticas com requisitos de tempo real, o que inclui aumento de confiabilidade, controle de latência, sincronização de relógio e gerenciamento de recurso, necessários para manufatura avançada assistida por robótica. Ter esses bens industriais virtualizados dependem do fatiamento de rede e assistência fornecidas por SDN e um controlador centralizado para configuração da rede. Gêmeos digitais podem ser usados nesse contexto para otimizar a imprecisão da rede, com seus requisitos dinâmicos, calculando as configurações de roteamento e agendamento, além de manter um modelo atualizado da rede, com constante atualização vinda pelos dados de telemetria [52], [53].

A aplicação de SDN para redes de sensores IoT tem o desafio de lidar com a baixa capacidade dos dispositivos conectados, tanto computacional quanto de comunicação. O uso de virtualização das funções de rede e para criar a representação virtual dos sensores dependem de NFV, possibilitando o enriquecimento dos dispositivos com mais recursos, como capacidade adicional de computação através do pré-processamento de dados, de comunicação através de maior variedade de protocolos de transmissão, diferentes dependendo de cada aplicação ou de armazenamento com dados coletados pelos sensores sendo pré-processamento localmente antes de serem transportados para um coletor de dados, pendente a disponibilidade de conectividade [2].

D. Redes Veiculares

Essa seção se trata da combinação de SDNs e gêmeos digitais no contexto de redes veiculares, que oferecem conectividade entre veículos e infraestrutura em rede, oferecendo aplicações e serviços. VANETs (*Vehicular Ad-hoc NETworks*) tradicionais possuem o desafio de como possibilitar uma rede inteligente com seu formato descentralizado, onde um veículo não possui capacidade de coletar e computar grandes quantidades de dados. A implementação de SDN para redes veiculares introduz com o controlador o poder computacional não presente em veículos individuais, tendo a visão global da rede e podendo adaptar de forma inteligente o roteamento para a demanda dinâmica desse ambiente [54].

Gêmeos digitais também são essenciais para a implementação de veículos autônomos. A transformação para veículos com operação baseada em dados torna necessária a adoção de novas regras para aumentar a resiliência e segurança dos veículos, essenciais para a redução de acidentes e para manter o cuidado num ambiente volátil, que envolve motoristas de outros veículos e pedestres. Veículos autônomos estão sujeitos a múltiplos tipos de falhas: por falha do sistema, sendo de origens mecânicas, eletroeletrônicas, ou falhas por ataques, tanto física quanto por ciberataques [55].

Redes VEC (Vehicular Edge Computing), criadas para melhor prover aplicações e serviços em proximidade de veículos, reduzem a latência de transmissão e o congestionamento da rede. Entretanto, desafios para implementação de redes como essa são a alta mobilidade de veículos, num ambiente dinâmico, necessitando administração de alta complexidade. Auxiliadas por gêmeos digitais, redes VEC podem adaptativamente administrar os recursos da rede e o cronograma de políticas de encaminhamento. Em tempo real, o gêmeo digital pode monitor os estados dos veículos e os recursos de rede, obtendo uma análise precisa da rede. Além disso, ele criará a camada virtual entre as entidades físicas da VEC e as aplicações veiculares, criando a ponte entre aplicações e usuários. Por ser responsável por essa comunicação, todo o fluxo de dados passa pelo gêmeo, sendo que dessa forma a rede VEC pode se adaptar para mudanças dinâmicas na topologia da rede, se adaptar a mudança de localização dos veículos e se adaptar para situações de emergência, alterando o cronograma de políticas e efetuando *offloading* de tarefas [56].

Zaid [57] argumenta que SDN, NFV e gêmeos são tecnologias habilitadoras para a implementação de eVTOLS (de *electric Vertical Take-off and Landing*, veículos urbanos para transporte aéreo), afim de ser uma alternativa ao trânsito terrestre tanto para o transporte de bens e produtos quanto para locomoção de passageiros. Ainda se tratando de uma tecnologia futuro, é possível especular alguns aspectos básicos necessários para o seu funcionamento e sua implementação, como comunicação confiável de alta velocidade e de baixa latência, com coordenação colaborativa entre os veículos, pela importância da carga carregada e para dirigir de forma autônoma. Para redes alcançarem esses objetivos, é essencial a introdução de reprogramabilidade da rede, dependência de um controlador centralizado para coordenação dos veículos e virtualização de componentes para serem escalados dentro da rede. Gêmeos digitais de eVTOLS serão utilizados nesse contexto, obtendo uma visão geral do sistema, afim de garantir a segurança e o planejamento de rotas [57].

E. Redes Ópticas

Uma rede óptica é uma tecnologia de rede altamente adotada por prover alta taxa de dados com baixo custo de operação comparada com outras tecnologias, mas possui a desvantagem de alto consumo de energia. O design de uma rede eficiente e inteligente pode levar em conta o comportamento de uso da rede pelos consumidores, utilizando aprendizado de máquina para ser mais eficiente no consumo de energia. Uma rede baseada em SDN tem o benefício do monitoramento de dados fornecido pelo controlador, regularmente coletando dados de toda infraestrutura, como estatísticas do tráfego e *logs* de eventos. Como conservação de energia e manter o maior QoS possível são dois objetivos contraditórios, o poder de decisão e o monitoramento próximo das operações devem ser executados de forma reativa e proativa em ordem para minimizar o consumo sem deteriorar o QoS [58].

Alabarce et al [59] discute o uso de gêmeos digitais como habilitador de redes sem toque (*Zero Touch Networking*), redes com a capacidade de atualização, provisionamento e *upgrade* das capacidades da rede por meio de automação com o mínimo de intervenção humana, reduzindo custos de manutenção. Isso é possível através de diagnósticos automáticos e validação de corretude das configurações de rede antes de sua implementação em campo, ou seja, no contexto de um gêmeo digital de redes, simular o funcionamento da rede modificada no ambiente digital antes de sua implantação no ambiente físico [59]. Gêmeos digitais podem ser utilizados para prover flexibilidade experimental, antes da implementação da rede [60], e seu uso de aprendizado de máquina e mecanismos de inteligência artificial é essencial para a existência de redes sem toque.

F. Segurança

A introdução de sistemas como gêmeos digitais introduz o potencial de ataques por meios digitais. Gêmeos digitais serão utilizados na crescente digitalização de indústrias de manufatura, construção, cidades, saúde, logística e energia. Apesar de todos os benefícios gerados para esses sistemas, altamente ligados à tomada de decisões de sistemas inteligentes. Devido à escala de comunicação e a interação com os seus parceiros reais, manter a segurança desse tipo de tecnologia é ainda mais essencial, pois pode causar efeitos diretos no mundo físico, vulnerável ao uso malicioso. A implementação segura de gêmeos digitais para infraestruturas heterogêneas é essencial. Infraestruturas inteligentes baseadas em SDN podem ser utilizadas para que redes de comunicação se tornem mais resilientes a ataques. Caminhos redundantes permitem o aumento da resiliência da rede e estratégias para mitigar ataques a comunicação de dados podem ser explorados, como

técnicas de criptografia, que torna a comunicação mais segura contra muitos tipos de ataques [61].

Ameaças a segurança de gêmeos digitais são variadas, podendo ser ataques a comunicação do sistema e à forma de armazenamento de dados. Desafios de segurança, como modificação não autorizada de informação do gêmeo, interfaces de comunicação mal configuradas, autenticação vulnerável são algumas possibilidades [4]. Outro tópico de interesse é confidencialidade, pois vazamentos de dados podem ser críticos ao funcionamento de sistemas, contendo problemas como propriedade intelectual e segredos comerciais. Karaarslan [61] classifica para gêmeos digitais sete grupos de ameaças à segurança:

- Ameaças físicas: segurança dos dispositivos físicos, que podem ser danificados, destruídos ou modificados.
- Ameaças de modificação de dados: modificação de dados irá passar informação incorreta para o gêmeo, gerando problemas para as previsões do sistema. Devido à comunicação direta com esses dispositivos, é necessário cuidado extra com o ambiente físico, pois um dispositivo infectado poderá afetar o comportamento de todo o sistema.
- Ameaças sistêmicas: ataques ao sistema operacional do gêmeo, que podem tomar controle sobre a sua operação, gerando problemas como negação de serviço, além de ataques maliciosos direcionados a atacar sistemas industriais.
- Ameaças de software: permitir acesso não autorizado ao gêmeo irá informar um atacante sobre o estado geral do sistema, que poderá analisar e buscar por vulnerabilidades. Um acesso dessa forma poderia ser obtido por violações de segurança por terceiros, inserindo código malicioso dentro do sistema.
- Ameaças de comunicação de dados: gêmeos digitais dependem de uma grande quantia de componentes heterogêneos serem integrados. Ameaças sobre comunicação, como *Denial of Service*, *Eavesdropping*, *Spoofing* e *Man-in-the-middle* são alguns cenários possíveis.
- Ameaças de armazenamento de dados: dados de operações para gêmeos digitais normalmente são armazenados em um cenário de nuvem. A centralização de armazenamento em uma nuvem pública pode gerar o vazamento desses dados.
- Ameaças de aprendizado de máquina: processos de aprendizado de máquina são vulneráveis a ataques de segurança, com ataques podendo influenciar o seu treinamento e diminuindo a performance e confiabilidade do sistema.

Ambientes virtualizados são vantajosos para a construção de sistemas de controle industriais (ICS, *Industrial Control Systems*), que necessitam manter o sistema se comportando dentro de valores esperados. ICS podem ser virtualizados e executados na nuvem, executando funções virtualizadas para efetuar o controle das operações de comunicação e segurança. Gêmeos digitais podem ser utilizados em sistemas como esse para servirem de mesas de teste para experimentação, geração de cenários de otimização, análise forense para identificar causas de mal funcionamento ou incidentes de segurança, tudo para garantir uma interoperabilidade segura nos sistemas controlados efetuando uma avaliação dinâmica dos eventos críticos do sistema [37], [62]. Dai et al [63] propõe o uso de gêmeos digitais para criar um sistema de defesa baseado em defesa através de mímica criando uma estrutura dinâmica de redundância, o que significa que os resultados de processamento são comparados vindos de múltiplas entidades diferentes, sendo fácil identificar um membro que não está operando da forma correta, ou seja, que foi atacado e modificado.

Com o acoplamento direto entre o mundo real e digital, mecanismos mais eficientes para defesa dos sistemas são necessários. Liu [64] sugere a introdução de um plano de segurança, dedicado ao suporte nativo de segurança na rede, composto por três partes: (1) Operação e Manutenção de segurança inteligente, (2) motor inteligente de políticas de segurança e (3) uma biblioteca habilitadora de segurança. (1) conduz as operações de operação e manutenção (O&M) baseados em inteligência artificial e informações obtidas no plano de dados; (2) o motor dinamicamente ajusta e melhora as políticas de segurança da rede e os mecanismos de segurança utilizados pelos componentes da rede; e (3) planeja as funções de segurança que serão requisitadas pela rede. Pelo uso de inteligência artificial, redes terão segurança nativa implementada, através de interação e colaboração entre as entidades conectadas, criando imunidade proativa de ameaças de forma ubíqua na rede [64].

Devido aos limites computacionais, capacidades de segurança, armazenamento e recursos de rede da computação em borda, além da grande quantidade de pontos de acesso, é difícil de ela estar equipada com medidas de proteção efetivas. Sun et al [65] apresenta uma arquitetura de proteção especificamente para computação em borda, com recomendações para camada de aplicação, dados, rede, nodo e de recurso, criando um sistema de proteção e mecanismos de segurança que levam em consideração a flexibilidade de gêmeos digitais na borda.

Provisionamento de políticas de acesso em setores industriais requer pré-análise, definição de papéis, permissões e regras para acessar recursos e efetuar ações, considerando restrições precisas e consistentes, o que é uma atividade complexa de administrar, devido a decentralização dos sistemas. Logo, administração de sistemas de autorização devem se tornar automatizados, com miníma intervenção manual, com o uso de inteligência artificial para duas atividades: **Alteração Automática de Política**, criando compreensão de acessos anteriores e o seu efeito no sistema, para refinar regras existentes. Mineração de dados e algoritmos de classificação podem ser usados para identificar falhas em especificações de políticas; e **Aprendizado de Regras**, onde algoritmos são treinados partindo de dados e inferindo novas políticas, através de aprendizado por reforço [66].

Para ambientes industriais, Krishnan et al [67] propõe um

TABLE I
CLASSIFICAÇÃO DE TRABALHOS

Categorias	Trabalhos	Total
5G, 6G e Sistemas *Wireless*	[2], [4], [13], [15]–[20], [22]–[37], [39]–[42], [47], [64], [66]	27
Detecção de Anomalias	[10], [11]	2
Escalonamento de VNF	[20]	1
Gêmeos Digitais para Redes	[1], [3]–[10], [12], [21], [30], [31], [46], [52], [59]	16
Internet das Coisas	[2], [14], [25], [31], [39], [43]–[52], [62], [67]	17
P4	[19], [21]	2
Redes Ópticas	[58]–[60]	3
Redes Veiculares	[54]–[57]	4
Segurança	[4], [37], [61]–[67]	9

sistema de detecção de intrusos utilizando a descrição de uso do fabricante (*manufacturer usage description*, MUD) dos dispositivos para melhorar o monitoramento de redes, explorando se dispositivos IoT apresentam padrões previsíveis, que podem ser definidos formal e sucintamente, utilizando gêmeos digitais e redes definidas por software para aumentar a segurança de ambientes industriais.

IV. CONCLUSÃO

A lista de artigos lidos gerou um total de 9 categorias de interesse, com base nos assuntos que cada trabalha apresentava, e podem ser visualizados na tabela I. Alguns trabalhos se encaixaram em mais de uma categoria, então a classificação não é exclusiva. Para quem tem interesse em um assunto específico, esta pesquisa serve como um breve resumo de contribuições e relações dos três assuntos-chave (SDN, NFV e gêmeos digitais) com as categorias originadas.

Uma classificação dentro de cada categoria seria uma próxima etapa dentro desse trabalho, para diferenciar as contribuições dentro de cada disciplina por cada um dos trabalhos.

Gêmeos digitais (e seus muitos outros nomes e subclassificações) representam a integração do mundo físico com o mundo digital. Através da obtenção de grandes quantidades de dados e com estudo de padrões por aprendizado de máquina, torna possível sistemas realmente autônomos, que aprendem e se tornam mais eficientes sem necessidade de intervenção humana. Sua inserção tecnológica torna possível a ubiquidade da computação, com dispositivos conectados em todos os lugares, transparente ao ser humano. Para a indústria, ela representa mais estabilidade, eficiência e redução de custos em todas esferas, tornando possível níveis de precisão sem limites humanos.

No contexto de redes de computadores, gêmeos digitais, implementados com o auxílio de SDN e NFV, auxiliam na solução de problemas na rede, predição do estado futuro da rede e melhora na sua confiabilidade por eliminar riscos conhecidos antes de acontecerem, além de poderem ser ferramentas úteis para automação e aumento de segurança de sistemas.

REFERENCES

[1] M. Alja'Afreh, "A qoe model for digital twin systems in the era of the tactile internet," Ph.D. dissertation, Université d'Ottawa/University of Ottawa, 2021.

[2] C. Nguyen and D. Hoang, "Software-defined virtual sensors for provisioning iot services on demand," in *2020 5th International Conference on Computer and Communication Systems (ICCCS)*. IEEE, 2020, pp. 796–802.

[3] C. Zhou, H. Yang, X. Duan, D. Lopez, A. Pastor, Q. Wu, M. Boucadair, and C. Jacquenet, "Digital Twin Network: Concepts and Reference Architecture," Internet Engineering Task Force, Internet-Draft draft-zhou-nmrg-digitaltwin-network-concepts-07, Mar. 2022, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-zhou-nmrg-digitaltwin-network-concepts-07

[4] L. U. Khan, Z. Han, W. Saad, E. Hossain, M. Guizani, and C. S. Hong, "Digital twin of wireless systems: Overview, taxonomy, challenges, and opportunities," *arXiv preprint arXiv:2202.02559*, 2022.

[5] J. Jagannath, K. Ramezanpour, and A. Jagannath, "Digital twin virtualization with machine learning for iot and beyond 5g networks: Research directions for security and optimal control," *arXiv preprint arXiv:2204.01950*, 2022.

[6] M. Ferriol-Galmés, J. Suárez-Varela, J. Paillise, X. Shi, S. Xiao, X. Cheng, P. Barlet-Ros, and A. Cabellos-Aparicio, "Building a digital twin for network optimization using graph neural networks," *Available at SSRN 3995236*, 2021.

[7] S. Vakaruk, A. Mozo, A. Pastor, and D. R. López, "A digital twin network for security training in 5g industrial environments," in *2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI)*. IEEE, 2021, pp. 395–398.

[8] C. Güemes-Palau, P. Almasan, S. Xiao, X. Cheng, X. Shi, P. Barlet-Ros, and A. Cabellos-Aparicio, "Accelerating deep reinforcement learning for digital twin network optimization with evolutionary strategies," *arXiv preprint arXiv:2202.00360*, 2022.

[9] P. Almasan, M. Ferriol-Galmés, J. Paillisse, J. Suárez-Varela, D. Perino, D. López, A. A. P. Perales, P. Harvey, L. Ciavaglia, L. Wong *et al.*, "Digital twin network: Opportunities and challenges," *arXiv preprint arXiv:2201.01144*, 2022.

[10] W. Wang, L. Tang, C. Wang, and Q. Chen, "Real-time analysis of multiple root causes for anomalies assisted by digital twin in nfv environment," *IEEE Transactions on Network and Service Management*, 2022.

[11] W. Wang, Q. Chen, T. Liu, and L. Tang, "Digital-twin assisted root cause analysis of anomalies in nfv environment," in *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021, pp. 1–6.

[12] X. Sun, C. Zhou, X. Duan, and T. Sun, "A digital twin network solution for end-to-end network service level agreement (sla) assurance," *Digital Twin*, vol. 1, no. 5, p. 5, 2021.

[13] L. U. Khan, W. Saad, D. Niyato, Z. Han, and C. S. Hong, "Digital-twin-enabled 6g: Vision, architectural trends, and future directions," *arXiv preprint arXiv:2102.12169*, 2021.

[14] M. Kherbache, M. Maimour, and E. Rondeau, "When digital twin meets network softwarization in the industrial iot: Real-time requirements case study," *Sensors*, vol. 21, no. 24, p. 8194, 2021.

[15] S. Schneider, M. Peuster, K. Hannemann, D. Behnke, M. Müller, P.-B. Bøk, and H. Karl, ""producing cloud-native": Smart manufacturing use cases on kubernetes," in *2019 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*. IEEE, 2019, pp. 1–2.

[16] F. Granelli, R. Capraro, M. Lorandi, and P. Casari, "Evaluating a digital twin of an iot resource slice: an emulation study using the eliot platform," *IEEE Networking Letters*, vol. 3, no. 3, pp. 147–151, 2021.

[17] F. Naeem, G. Kaddoum, and M. Tariq, "Digital twin-empowered network slicing in b5g networks: Experience-driven approach," in *2021 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2021, pp. 1–5.

[18] A. Fellan, C. Schellenberger, M. Zimmermann, and H. D. Schotten, "Enabling communication technologies for automated unmanned vehicles in industry 4.0," in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2018, pp. 171–176.

[19] C.-Y. Chang, T. G. Ruiz, F. Paolucci, M. A. Jiménez, J. Sacido, C. Papagianni, F. Ubaldi, D. Scano, M. Gharbaoui, A. Giorgetti *et al.*, "Performance isolation for network slices in industry 4.0: The 5growth approach," *IEEE Access*, vol. 9, pp. 166 990–167 003, 2021.

[20] E. Zeydan, J. Mangues-Bafalluy, J. Baranda, R. Martínez, and L. Vettori, "A multi-criteria decision making approach for scaling and placement of virtual network functions," *Journal of Network and Systems Management*, vol. 30, no. 2, pp. 1–36, 2022.

[21] R. Larsson, "Creating digital twin distributed networks using switches with programmable data plane," 2021.

[22] H. Wang, Y. Wu, G. Min, and W. Miao, "A graph neural network-based digital twin for network slicing management," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 2, pp. 1367–1376, 2020.

[23] D. de Vleeschauwer, J. Baranda, J. Mangues-Bafalluy, C. F. Chiasserini, M. Malinverno, C. Puligheddu, L. Magoula, J. Martín-Pérez, S. Barmpounakis, K. Kondepu *et al.*, "5growth data-driven ai-based scaling," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2021, pp. 383–388.

[24] B. Han, W. Jiang, M. A. Habibi, and H. D. Schotten, "An abstracted survey on 6g: Drivers, requirements, efforts, and enablers," *arXiv preprint arXiv:2101.01062*, 2021.

[25] M. Peuster, S. Schneider, D. Behnke, M. Müller, P.-B. Bøk, and H. Karl, "Prototyping and demonstrating 5g verticals: the smart manufacturing case," in *2019 IEEE Conference on Network Softwarization (NetSoft)*. IEEE, 2019, pp. 236–238.

[26] G. Liu, N. Li, J. Deng, Y. Wang, J. Sun, and Y. Huang, "6g mobile network architecture-solids: Driving forces, features, and functional topology," *Engineering*, 2021.

[27] J. T. Penttinen, "On 6g visions and requirements," *Journal of ICT Standardization*, pp. 311–326, 2021.

[28] M. Tariq, F. Naeem, and H. V. Poor, "Toward experience-driven traffic management and orchestration in digital-twin-enabled 6g networks," *arXiv preprint arXiv:2201.04259*, 2022.

[29] S. Yrjölä *et al.*, "Decentralized 6g business models," *Proceedings of the 6G Wirel. Summit, Levi, Finland*, pp. 5–7, 2019.

[30] H. Ahmadi, A. Nag, Z. Khan, K. Sayrafian, and S. Rahadrja, "Networked twins and twins of networks: an overview on the relationship between digital twins and 6g," *arXiv preprint arXiv:2108.05781*, 2021.

[31] X. Shen, J. Gao, W. Wu, M. Li, C. Zhou, and W. Zhuang, "Holistic network virtualization and pervasive network intelligence for 6g," *IEEE Communications Surveys & Tutorials*, 2021.

[32] S. Kumar, "6g mobile communication networks: Key services and enabling technologies," *Journal of ICT Standardization*, pp. 1–10, 2022.

[33] D. Stock, M. Schneider, and T. Bauernhansl, "Towards asset administration shell-based resource virtualization in 5g architecture-enabled cyber-physical production systems," *Procedia CIRP*, vol. 104, pp. 945–950, 2021.

[34] N. S. Kumar, U. Kaur, T. Anuradha, S. Majji, S. R. Karanam, and R. G. Deshmukh, "5g network virtualization for the remote driving enhancement," in *2021 4th International Conference on Computing and Communications Technologies (ICCCT)*. IEEE, 2021, pp. 458–463.

[35] E.-K. Hong, I. Lee, B. Shim, Y.-C. Ko, S.-H. Kim, S. Pack, K. Lee, S. Kim, J.-H. Kim, Y. Shin *et al.*, "6g r&d vision: Requirements and candidate technologies," *Journal of Communications and Networks*, NA.

[36] J. Cheng, Y. Yang, X. Zou, and Y. Zuo, "5g in manufacturing: a literature review and future research," *The International Journal of Advanced Manufacturing Technology*, pp. 1–23, 2022.

[37] A. Narayan, C. Krueger, A. Goering, D. Babazadeh, M.-C. Harre, B. Wortelen, A. Luedtke, and S. Lehnhoff, "Towards future scada systems for ict-reliant energy systems," in *International ETG-Congress 2019; ETG Symposium*. VDE, 2019, pp. 1–7.

[38] A. Filali, A. Abouaomar, S. Cherkaoui, A. Kobbane, and M. Guizani, "Multi-access edge computing: A survey," *IEEE Access*, vol. 8, pp. 197 017–197 046, 2020.

[39] M. Groshev, C. Guimarães, A. De La Oliva, and R. Gazda, "Dissecting the impact of information and communication technologies on digital twins as a service," *IEEE Access*, vol. 9, pp. 102 862–102 876, 2021.

[40] S. Schneider, M. Peuster, D. Behnke, M. Müller, P.-B. Bøk, and H. Karl, "Putting 5g into production: Realizing a smart manufacturing vertical scenario," in *2019 European Conference on Networks and Communications (EuCNC)*. IEEE, 2019, pp. 305–309.

[41] D. Roy, A. S. Rao, T. Alpcan, G. Das, and M. Palaniswami, "Achieving ai-enabled robust end-to-end quality of experience over radio access networks," *arXiv preprint arXiv:2201.05184*, 2022.

[42] J. M. Taylor and H. R. Sharif, "Leveraging digital twins to enhance performance of iot in disadvantaged networks," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2020, pp. 1303–1308.

[43] R. Minerva, G. M. Lee, and N. Crespi, "Digital twin in the iot context: a survey on technical features, scenarios, and architectural models," *Proceedings of the IEEE*, vol. 108, no. 10, pp. 1785–1824, 2020.

[44] S. Yun, J.-h. Park, H.-s. Kim, and W.-T. Kim, "Importance-aware sdn control mechanism for real-time data distribution services," in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2018, pp. 1113–1118.

[45] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-iiotset: A new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40 281–40 306, 2022.

[46] T. Yang, J. Chen, and N. Zhang, "Ai-empowered maritime internet of things: a parallel-network-driven approach," *IEEE Network*, vol. 34, no. 5, pp. 54–59, 2020.

[47] S. Zeb, A. Mahmood, S. A. Hassan, M. J. Piran, M. Gidlund, and M. Guizani, "Industrial digital twins at the nexus of nextg wireless networks and computational intelligence: A survey," *Journal of Network and Computer Applications*, p. 103309, 2022.

[48] A. K. Ghosh, A. S. Ullah, R. Teti, and A. Kubo, "Developing sensor signal-based digital twins for intelligent machine tools," *Journal of Industrial Information Integration*, vol. 24, p. 100242, 2021.

[49] P. Bellavista, C. Giannelli, M. Mamei, M. Mendula, and M. Picone, "Application-driven network-aware digital twin management in industrial edge environments," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7791–7801, 2021.

[50] I. A. Tsokalo, D. Kuss, I. Kharabet, F. H. Fitzek, and M. Reisslein, "Remote robot control with human-in-the-loop over long distances using digital twins," in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[51] J. Santa, J. Ortiz, P. J. Fernandez, M. Luis, C. Gomes, J. Oliveira, D. Gomes, R. Sanchez-Iborra, S. Sargento, and A. F. Skarmeta, "Migrate: Mobile device virtualisation through state transfer," *IEEE Access*, vol. 8, pp. 25 848–25 862, 2020.

[52] H. Chahed and A. J. Kassler, "Software-defined time sensitive networks configuration and management," in *2021 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*. IEEE, 2021, pp. 124–128.

[53] H. Kim, H. Shin, H.-s. Kim, and W.-T. Kim, "Vr-cpes: A novel cyber-physical education systems for interactive vr services based on a mobile platform," *Mobile Information Systems*, vol. 2018, 2018.

[54] L. Zhao, G. Han, Z. Li, and L. Shu, "Intelligent digital twin-based software-defined vehicular networks," *IEEE Network*, vol. 34, no. 5, pp. 178–184, 2020.

[55] S. Almeaibed, S. Al-Rubaye, A. Tsourdos, and N. P. Avdelidis, "Digital twin analysis to promote safety and security in autonomous vehicles," *IEEE Communications Standards Magazine*, vol. 5, no. 1, pp. 40–46, 2021.

[56] Y. Dai and Y. Zhang, "Adaptive digital twin for vehicular edge computing and networks," *Journal of Communications and Information Networks*, vol. 7, no. 1, pp. 48–59, 2022.

[57] A. A. Zaid, B. E. Y. Belmekki, and M.-S. Alouini, "Technological trends and key communication enablers for evtols," *arXiv preprint arXiv:2110.08830*, 2021.

[58] D. S. N. A. B. Pg, S. S. Newaz, F. H. Rahman, T.-W. Au, N. S. Nafi, R. K. Patchmuthu, F. Al-Hazemi *et al.*, "Digital-twin-assisted software-defined pon: A cognition-driven framework for energy conservation," in *2021 31st International Telecommunication Networks and Applications Conference (ITNAC)*. IEEE, 2021, pp. 166–177.

[59] M. G. Alabarce and P. P. Mariño, "Optical network design and analysis tools: A test of time," *Optical Switching and Networking*, vol. 44, p. 100651, 2022.

[60] D. Kilper, J. Yu, and S. Santaniello, "Optical networking in smart city and wireless future networks platforms," in *2021 European Conference on Optical Communication (ECOC)*. IEEE, 2021, pp. 1–4.

[61] E. Karaarslan and M. Babiker, "Digital twin security threats and countermeasures: An introduction," in *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*. IEEE, 2021, pp. 7–11.

[62] A. F. Murillo and S. Rueda, "Access control policies for network function virtualization environments in industrial control systems," in *2020 4th Conference on Cloud and Internet of Things (CIoT)*. IEEE, 2020, pp. 17–24.

[63] W. Dai, S. Li, L. Lu, Y. Ye, F. Meng, and D. Zhang, "Research on application of mimic defense in industrial control system security," in *2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA)*, vol. 2. IEEE, 2021, pp. 573–577.

[64] G. Liu, Y. Huang, N. Li, J. Dong, J. Jin, Q. Wang, and N. Li, "Vision, requirements and network architecture of 6g mobile network beyond 2030," *China Communications*, vol. 17, no. 9, pp. 92–104, 2020.

[65] Y. Sun, X. Xu, R. Qiang, and Q. Yuan, "Research on security management and control of power grid digital twin based on edge computing," in *2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)*. IEEE, 2021, pp. 606–610.

[66] J. Lopez, J. E. Rubio, and C. Alcaraz, "Digital twins for intelligent authorization in the b5g-enabled smart grid," *IEEE Wireless Communications*, vol. 28, no. 2, pp. 48–55, 2021.

[67] P. Krishnan, K. Jain, R. Buyya, P. Vijayakumar, A. Nayyar, M. Bilal, and H. Song, "Mud-based behavioral profiling security framework for software-defined iot networks," *IEEE Internet of Things Journal*, 2021.