Análise de mecanismos de autenticação de dispositivos em redes móveis 5G para Internet Industrial (IIoT) categorizada por mMTC, eMBB e URLLC

Sergio Henrique Silva[1], **Charles Christian Miers**[1]

[1]Programa de Pós-Graduação em Computação Aplicada (PPGCAP)
Universidade do Estado de Santa Catarina (UDESC)

sergio.hs@edu.udesc.br - charles.miers@udesc.br

Resumo. *As redes 5G possuem um aspecto inovador ao proporcionar pela primeira vez uma cobertura em larga escala para interconectar não apenas pessoas mas principalmente dispositivos em larga escala, densidade e área de cobertura. Cada geração de redes celulares sempre define pelo menos um método de autenticação, as redes 5G possuem três métodos de autenticação 5G: AKA, EAP-AKA e EAP-TLS. Este trabalho, apresenta uma análise inicial da arquitetura básica de segurança do 5G, os protocolos e mecanismos de autenticação e faz uma relação destes com o cenário de implantação em dispositivos da Internet Industrial, categorizando-os de acordo com os serviços de autenticação do 5G como Enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (uRLLC) e Massive Machine Type Communications (mMTC).*

1. Introdução

As redes celulares 5G, trazem consigo novas possibilidades de aplicação em relação às gerações anteriores de redes móveis, principalmente por características como velocidades mais altas, latência inferior e suporte a um numero superior de conexões simultâneas. Os serviços oferecidos por redes 5G [Prasad et al., 2018] podem ser classificados em três cenários principais: (i) eMBB que consiste na característica de banda larga aprimorada, garantindo maior vazão aos dispositivos ou usuários conectados; (ii) uRLLC com baixa latência e alta disponibilidade em relação às gerações anteriores; e (iii) mMTC serviço que remete a capacidade de comunicações massivas, ou seja, em larga escala [ITU-R, 2017] [TSGR, 2017]. Estes serviços [possibilitam uma oportunidade de concretização de aplicações de IoT como cidades inteligentes, agricultura inteligente e monitoramento de frota. Além disso, as redes 5G oferecem o suporte necessário para aplicações industriais da *Internet of Things* (IoT), denominadas IIoT. No contexto de IIoT, os serviços eMBB, URLLC e mMTC são decisivos na implementação de diversas aplicações. Em IIoT pode ser necessário um expressivo tráfego de dados, disponibilidade para o monitoramento de componentes críticos da produção industrial ou disponibilidade para comportar um número massivo de dispositivos conectados com alta densidade ou não.

Na utilização de dispositivos conectados em redes *Redes Móveis de Quinta Geração* (5G), como em qualquer contexto computacional, os protocolos de autenticação são componentes essenciais na garantia dos requisitos de segurança como confidencialidade, integridade e autenticidade [Jenuario, 2019]. Os padrões em redes 5G descrevem mecanismos e protocolos de segurança que visam garantir autenticação segura na comunicação segura entre dispositivos ou entre dispositivos, servidores e outros equipamentos de rede. Os

protocolos descritos têm em si especificidades e cada um tem um contexto próprio para uso, a depender da finalidade e os requisitos da implementação. A escolha do protocolo de autenticação correto na implementação de projetos envolvendo dispositivos em *Industrial Internet of Things* (IIoT), tem singular importância na garantia da segurança e funcionalidade de todo o sistema computacional.

O presente trabalho tem como objetivo identificar os principais mecanismos e protocolos de autenticação aplicados a contextos IIoT usando redes 5G. Além disso, apresenta uma análise inicial dos mecanismos de autenticação categorizando-os pelos serviços da 5G. O trabalho final consiste no emprego de mecanismo de autenticação 5G para sistema de IIoT tipo robô que está em desenvolvimento.

Na Seção 2 são definidos os conceitos de IIoT, redes 5G e autenticação de dispositivos neste cenário, além dos mecanismos de autenticação em 5G. Já a Seção 3 faz um apanhado de trabalhos relacionados, buscando comprovar a relevância desta proposta de pesquisa. A Seção 4 faz referência a uma análise preliminar sobre a aplicabilidade dos mecanismos de autenticação em dispositivos IIoT.

2. Contexto: IIoT, Redes 5G e autenticação

O uso de redes celulares móveis para aplicações IIoT era limitado antes do surgimento do 5G por conta dos requisitos de desempenho (Tabela 1). Contudo, as especificações do 5G e a possibilidade de redes privadas possibilitaram a sua aplicação a cenários industriais [TSGS, 2019].

Tabela 1. Principais requisitos de desempenho em IIoT [Brown et al., 2018].

Caso de Uso (alto nível)		Disponibilidade	Ciclos de tempo	Tamanho típico do *payload*	Número de dispositivos	Área típica de serviço
Controle de movimento	Impressora industrial	>99,9999%	<2ms	20 bytes	>100	100m x 100m x 30m
	Máquina-ferramenta	>99,9999%	<0,5ms	50 bytes	∼20	15m x 15m x 3m
	Máquina de embalagem	>99,9999%	<1ms	40 bytes	∼50	10m x 5m x 3m
Robôs móveis	Controle de movimento cooperativo	>99,9999%	1ms	40-250 bytes	100	<1 km^2
	Controle remoto operado por vídeo	>99,9999%	10-100ms	15-150 bytes	100	<1 km^2
Painéis de controles móveis e com funções de segurança	Robôs de montagem ou fresadoras	>99,9999%	4-8ms	40-250 bytes	4	10m x 10m
	Guindastes móveis	>99,9999%	12ms	40-250 bytes	2	4m x 60m
Automação / Monitoramento de processos		>99,99%	>50ms	vários	10.000 dispositivos por km^2	

Os padrões gerais das redes 5G são desenvolvidos pelo consórcio *3rd Generation Partnership Project* (3GPP). Estes padrões descrevem protocolos que tem como objetivo fornecer garantias de segurança aos assinantes, usuários e prestadores de serviço das redes móveis. A Figura 1 ilustra a arquitetura em redes móveis em geral e as principais entidades envolvidas no processo de autenticação [TSGS, 2019]. O *User Equipament* (UE), que se trata do equipamento que deseja autenticar na rede, seja este um usuário ou dispositivo IoT. A *Service Network* (SN) que representa a infraestrutura de conectividade como antenas, roteadores e demais componentes da rede de serviço. A *Home Network* (HN) é responsável pelo registro e autenticação dos assinantes, recebendo o papel de uma rede doméstica.

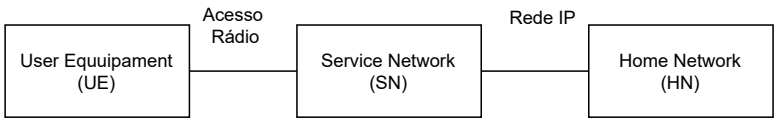

Figura 1. Arquitetura básica 5G. Adaptado de [TSGS, 2019]

Analisando a Figura 1, o escopo desta pesquisa concentra-se na autenticação do UE que é listada na Figura 2.

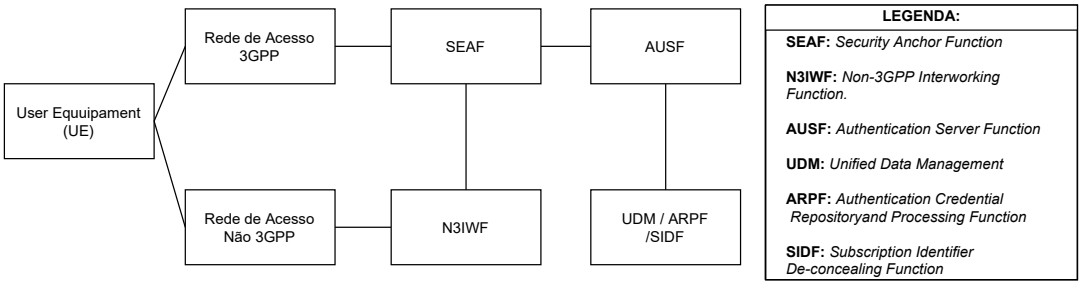

Figura 2. Fluxo de autenticação em 5G. Adaptado de [TSGS, 2019]

Na Figura 2, cada dispositivo da UE é equipado com um *Universal Integrated Circuit Card* (UICC) que leva pelo menos um *Universal Subscriber Identity Module* (USIM) que por sua vez armazena uma chave criptográfica que é compartilhada com a rede do usuário. A SN consiste em equipamentos de acesso de rádio como estações base entre outros itens de infraestrutura. A comunicação entre as redes de serviço e uma rede doméstica é baseada em IP, sendo as entidades centrais conectadas em uma rede IP coletivamente chamadas de EPS. Já, especificamente em 5G propôs-se uma arquitetura baseada em serviço, denominada *Service Based Architecture* (SBA). Nesta arquitetura novas entidades e requisições foram definidas no processo de autenticação [Ivezic, 2020], A *Security Anchor Function* (SEAF), funciona como um intermediário no processo de autenticação entre o UE e sua rede doméstica. Este pode rejeitar a autenticação, mas depende da rede doméstica para aceitá-la. A *Authentication Server Function* (AUSF) localizada na rede doméstica executa a autenticação do UE. Esta entidade toma a decisão sobre a autenticação, mas depende dos serviços de *back-end* para realizar a autenticação. A entidade *Unified Data Management* (UDM) é uma entidade que hospeda funções relativas ao gerenciamento dos dados da autenticação, por sua vez definido como *Authentication Credential Repository and Processing Function* (ARPF). [TSGS, 2019] O ARPF também é responsável por selecionar o método de autenticação com base na identidade do assinante. Já a *Subscription Identifier De-concealing Function* (SIDF) é uma entidade que tem como função descriptografar a identidade fornecida através do *Subscription Concealed Identifier* (SUCI) para obter a identidade de longa duração, ou seja, o *Subscription Permanent Identifier* (SUPI) que pode ser o *International Mobile Subscriber Identity* (IMSI).

Em redes 5G, diferentemente das gerações de redes móveis anteriores, as identidades de longa duração são transmitidas pelas interfaces de rádio, sempre de maneira cifrada. Portanto, apenas o SIDF tem acesso a chave privada, associada a uma chave pública distribuída aos UE para cifrar seus SUPIs. A estrutura de autenticação foi definida para que a autenticação seja aberta, com suporte ao *Extensible Authentication Protocol* (EAP). Além disso, agnóstica em relação a rede de acesso, ou seja é compatível com redes 3GPP e redes de acesso não 3GPP como redes sem fio (e.g., IEEE 802.11) e guiadas (e.g., Ethernet). Quando o EAP é usado, a autenticação é entre o UE, que é um ponto EAP e o

AUSF que é um servidor EAP através do SEAF que funciona como um atravessador EAP para o autenticador. A autenticação do UE pode ter origem em redes confiáveis 3GPP e não 3GPP. Quando a autenticação é em redes não confiáveis é necessário que seja feita uma N3IWF que opera como uma nova entidade funcionando como uma *Virtual Private Network* (VPN) para garantir acesso ao núcleo 5G através de túneis IPSec.

Nos padrões 5G foram descritos protocolos que podem, através de seus mecanismos de autenticação garantir a segurança na autenticação. O protocolo padrão extensível para redes 5G é o 5G *Authentication and Key Agreement* (AKA) [Flynn, 2018]. Para implementar a arquitetura aberta foi proposta pelo 3GPP uma extensão deste protocolo com a utilização conjunta do EAP, denominado EAP-AKA. Tanto o protocolo original e esta extensão empregam criptografia simétrica. Contudo, nem todas as UE ou dispositivos podem utilizar os protocolos baseados em 5G AKA. Para estes casos foi definido o protocolo *Extensible Authentication Protocol – Transport Layer Security* (EAP-TLS) [Simon et al., 2008], possibilitando o uso de EAP com certificados padrão X.509. O 5G EAP-TLS, não exige que necessariamente o UE ou dispositivo esteja equipado com um USIM, abrindo espaço para estas redes abarcarem dispositivos que não foram desenhados especificamente para redes móveis como o 5G.

É perceptível em 5G, apesar da estrutura de autenticação ser unificada, a escolha do protocolo de autenticação pode variar em relação ao contexto de utilização. Os contextos eMBB, uRLLC e mMTC tem requisitos diferentes em relação a sua implementação e podem impactar diretamente na implementação destas redes. Em contextos de IIoT como por exemplo uma rede privada com sensores e atuadores, que não possuem cartões de telefonia móvel a implementação deve valer-se do protocolo 5G EAP-TLS.

3. Trabalhos Relacionados

Este trabalho, além de analisar a autenticação em redes 5G de maneira geral, propõe a análise dos mecanismos quanto a sua aplicação nos cenários propostos pelos padrões. Ademais, dentro desta análise privilegiar os cenários de aplicabilidade no cenário de IIoT. Assim, são analisados trabalhos que tratam sobre autenticação em redes móveis 5G, quando possível direcionados ao ambiente IIoT e categorizados pela fatia de rede (*network slice*), e observando a similaridade com o presente trabalho (Tabela 2).

Tabela 2. Trabalhos relacionados identificados.

Referência	Autenticação IIoT	Categorizado por cenário (mMTC, eMBB e uRLLC)
[Fan et al., 2016]	Aborda Indiretamente	Não aborda
[Ferrag et al., 2018]	Aborda Indiretamente	Não aborda
[Behrad et al., 2019]	Aborda indiretamente	Aborda indiretamente
[Chen et al., 2018]	Aborda Indiretamente	Aborda Indiretamente
[Al-Aqrabi et al., 2019]	Aborda	Aborda indiretamente
[Cao et al., 2018]	Aborda Indiretamente	mMTC
[Weinand et al., 2019]	Aborda indiretamente	URLLC
[Seok et al., 2020]	Aborda indiretamente	URLLC e mMTC
[Ni et al., 2018]	Aborda Indiretamente	mMTC, e MBBe URLLC
[Qiu et al., 2020]	Aborda Indiretamente	mMTC, eMBB e URLLC

Destacam-se na Tabela 2 os trabalhos [Ni et al., 2018] e [Qiu et al., 2020], porque tratam o tema da autenticação em redes 5G categorizadas pelos serviços além de relatar a autenticação de dispositivo. Entretanto, não tratam exatamente do contexto IIoT, o qual possui especificidades que são determinantes na escolha do mecanismo de autenticação.

4. Análise preliminar

A possibilidade de uso de diversos mecanismos de autenticação no 5G reforça que é possível implementar a conectividade de pessoas e dispositivos. Neste contexto, os mecanismos de autenticação do 5G categorizados pelos serviços IIoT são listados na Tabela 3.

Tabela 3. Categorização dos mecanismos de autenticação *vs.* dispositivos IIoT.

	Cenário e dispositivos IIoT					
	Controle de movimento cooperativo			**Controle remoto operado por vídeo**		
	Disponibilidade exigida	**Número típico de dispositivos**	**Área típica de Serviço**	**Disponibilidade exigida**	**Número típico de dispositivos**	**Área típica de Serviço**
5G AKA	Atende	Atende parcialmente	Atende	Atende	Atende parcialmente	Atende
EAP-AKA	Atende	Atende parcialmente	Atende	Atende	Atende Parcialmente	Atende
EAP-TLS	Atende	Atende	Atende	Atende	Atende	Atende

A Tabela 3 relaciona os protocolos de autenticação com o cenário de dispositivos IIoT, especialmente os dispositivos de tipo robô no que se refere a aplicabilidade destes mecanismos em relação aos requisitos dos dispositivos. Ainda na Tabela 3, analisam-se os requisitos relativos a disponibilidade, ao número de dispositivos e a área típica de uso destes dispositivos conforme descrito na Tabela 1. Na análise, observa-se que os protocolos 5G-AKA e EAP-AKA atendem parcialmente os requisitos e disponibilidade número típico e área típica dos dispositivos. Por outro lado, o protocolo EAP-TLS atende integralmente a estes requisitos nos dispositivos elencados. É importante ressaltar que existem diversas iniciativas na comunidade acadêmica em aprimorar ou até criar extensões dos protocolos para melhor funcionamento nos cenários de implantação.

5. Considerações & Trabalhos futuros

Como o 5G se trata de uma tecnologia em implantação relativamente recente, é importante que ao definir os protocolos autenticação seja identificado qual o cenário de uso mais adequado. Nos contextos da IIoT, a utilização de redes 5G tem que acontecer dentro de critérios de desempenho e garantia da segurança. A escolha do protocolo de autenticação é vital para garantir tais atributos. Com esta análise preliminar, categorizada pelos mecanismos de autenticação, pode-se obter algumas informações sobre as particularidades dos cenários colocados em relação ao cenário de aplicação de dispositivos industriais.

A continuidade deste trabalho focará em mecanismo de autenticação para cenários de IIoT de robôs no qual é necessário levar em consideração sistemas legados como sistemas já compatíveis com os mecanismos de autenticação presentes no 5G.

Agradecimentos: Os autores agradecem o apoio do LabP2D/UDESC e FAPESC.

Referências

Al-Aqrabi, H., Johnson, A. P., Hill, R., Lane, P., and Liu, L. (2019). A multi-layer security model for 5g-enabled industrial internet of things. In *Communications in Computer and Information Science*, volume 1122 CCIS, pages 279–292. Springer.

Behrad, S., Bertin, E., Tuffin, S., and Crespi, N. (2019). 5G-SSAAC: Slice-specific Authentication and Access Control in 5G. In *Proceedings IEEE NetSoft 2019*, pages 281–285. IEEE.

Brown, G. et al. (2018). Ultra-reliable low-latency 5g for industrial automation. *Technol. Rep. Qualcomm*, 2:52065394.

Cao, J., Ma, M., Li, H., Fu, Y., and Liu, X. (2018). EGHR: Efficient group-based handover authentication protocols for mMTC in 5G wireless networks. *Journal of Network and Computer Applications*, 102:1–16.

Chen, Z., Chen, S., Xu, H., and Hu, B. (2018). A security authentication scheme of 5G ultra-dense network based on block chain. *IEEE Access*, 6:55372–55379.

Fan, K., Gong, Y., Liang, C., Li, H., and Yang, Y. (2016). Lightweight and ultra-lightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. *Security and Communication Networks*, 9(16):3095–3104.

Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., and Janicke, H. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes.

Flynn, K. (2018). 3gpp 5g security. *3gpp.org*.

ITU-R (2017). Minimum requirements related to technical performance for IMT-2020 radio interface(s) M Series Mobile, radiodetermination, amateur and related satellite services.

Ivezic, M. (2020). Introduction to 5g core service-based architecture (sba) components. *5G Security - 5G, mIoT, CPSSEC, Security blog by Marin Ivezic*.

Jenuario, Tadeu, C. J. O. P. G. K. D. (2019). Verificação Automática de Protocolos de Segurança com a ferramenta Scyther. pages 172–177.

Ni, J., Lin, X., and Shen, X. S. (2018). Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT. *IEEE Journal on Selected Areas in Communications*, 36(3):644–657.

Prasad, A. R., Arumugam, S., B, S., and Zugenmaier, A. (2018). 3gpp 5g security. *Journal of ICT Standardization*, 6(1):137–158.

Qiu, Q., Liu, S., Xu, S., and Yu, S. (2020). Study on Security and Privacy in 5G-Enabled Applications. *Wireless Communications and Mobile Computing*, 2020.

Seok, B., Sicato, J. C. S., Erzhena, T., Xuan, C., Pan, Y., and Park, J. H. (2020). Secure D2D communication for 5G IoT network based on lightweight cryptography. *Applied Sciences (Switzerland)*, 10(1).

Simon, D., Hurst, R., and Aboba, D. B. D. (2008). The EAP-TLS Authentication Protocol. RFC 5216.

TSGR (2017). TR 138 912 - V14.0.0 - 5G; Study on New Radio (NR) access technology (3GPP TR 38.912 version 14.0.0 Release 14).

TSGS (2019). TS 133 501 - V15.5.0 - 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.5.0 Release 15). Technical report.

Weinand, A., Sattiraju, R., Karrenbauer, M., and Schotten, H. D. (2019). Supervised learning for physical layer based message authentication in URLLC scenarios. In *IEEE Vehicular Technology Conference*, volume 2019-September. IEEE.