Uma proposta de análise do ciclo de vida de credenciais em redes LoraWan privadas para IIoT

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. *O uso de dispositivos inteligentes para as mais diversas atividades humanas fez emergir o conceito como IoT, e de IIoT quando estes dispositivos são aplicados à indústria. A gestão de identidades e segurança em ambientes IIoT tem requisitos específicos no ciclo de vida das credenciais utilizadas. A utilização de LPWAN e RSSF em redes industriais é um assunto que merece atenção, bem como conceitos do ciclo de vida de credenciais. Neste artigo, é feita uma proposta de pesquisa centrada no problema da garantia de autenticidade de dispositivos por meio da análise do ciclo de vida das credenciais. Tendo como objetivo, fazer uma análise de segurança em relação ao ciclo de vida de credenciais no cenário proposto.*

1. Introdução

A *Internet of Things* (IoT) permite que bilhões de dispositivos como computadores, sensores e atuadores sejam conectados em rede e implantados em diversos contextos, inclusive no contexto industrial, culminando na realização de conceitos como indústrias inteligentes, Indústria 4.0, ou ainda *Industrial Internet of Things* (IIoT). Tipicamente, estes dispositivos estão conectados a redes sem fio, o que fez ressignificar a importância destas redes [Caldas et al., 2017]. A arquitetura das redes sem fio pode ter diversos tipos de arranjos, como redes públicas e privadas e diversos requisitos como baixo consumo de energia e comunicação a grandes distâncias. Redes com requisitos de baixo consumo de energia e ampla cobertura de área são denominadas *Low-power Wide-area Network* (LPWAN). Entre as LPWANs, o protocolo LoRaWAN oferece suporte aos recursos de eficiência energética e transmissão de longo alcance e possibilita a criação de redes privadas de baixo custo com alta eficiência [Lora-Alliance, 2015].

Além do contexto e dos requisitos de energia e abrangência, existem os requisitos relacionados a segurança. Neste sentido, o controle de acesso e o gerenciamento de credenciais são um importante vetor de atenção na garantia de confidencialidade [Naoui et al., 2016]. Na gestão de identidades, o gerenciamento de credenciais é composto por etapas responsáveis por disponibilizar e revogar credenciais usadas em uma entidade autenticadora no controle de acesso. Este processo tem o objetivo de conceder privilégios de acesso somente a entidades válidas e com privilégios para acesso dos serviços da rede.

Este artigo apresenta uma proposta para analisar se, em contextos LPWAN e IIoT privados, o protocolo LoRaWAN é capaz de garantir estes requisitos relativos ao gerenciamento do ciclo de vida de credenciais. Além disso, se este gerenciamento de credenciais

está de acordo com padrões e boas práticas, e se existe garantia que os dispositivos seguem o ciclo de vida de credenciais de modo a garantir a autenticidade a dispositivos integrantes de redes privadas LoraWan IIoT.

O artigo está organizado como segue. A Seção 2 fundamenta o contexto e cenário da pesquisa, bem como as peculiaridades do contexto e os principais aspectos das redes sem fio privadas para IIoT. A Seção 3 contém a definição do problema, enquanto a Seção 4 descreve a proposta de trabalho.

2. Fundamentação

A IIoT representa a nova geração de avanço industrial, visando interconectar e informatizar os processo pré e pós industriais. O objetivo da IIoT é tornar as fábricas inteligentes o suficiente em termos de adaptabilidade aprimorada, eficiência de recursos, integração aprimorada de processos de oferta e demanda entre as fábricas. A comunicação sem fios, por meio das *Redes de Sensores Sem Fio* (RSSF), possui um importante papel na habilitação desta nova era da indústria, desde a conexão de infraestrutura legada até em novos dispositivos inteligentes [Proietti Franceschilli, 2019].

Como em qualquer contexto computacional, na garantia de requisitos de segurança como confidencialidade, integridade e autenticidade são importantes pontos de preocupação. Para a garantia destes requisitos o controle de acesso de usuários e dispositivos é fundamental. O controle de acesso por sua vez faz uso de credenciais, que tem um ciclo de vida que compreende: o registro, validação, utilização, expiração/revogação, arquivamento e eventual destruição das credenciais usadas nesse processo de controle de acesso. Este ciclo de vida independe do tipo de credencial. A análise presente neste trabalho visa entender como o aperfeiçoamento do gerenciamento de identidades em contextos de redes RSSF e LPWAN industriais pode melhorar garantia de segurança em tais contextos.

2.1. Redes sem fio para IIoT

As RSSF são definidas como uma rede de sensores que se utilizam de comunicação sem fio como meio de transmissão [Loureiro et al., 2003]. O potencial das RSSF compara-se ao da internet, pois enquanto a *web* permite o acesso remoto a informações, as RSSFs permitem a interação remota com o mundo físico por meio de sensores. Deste modo concretizando o cenário da computação pervasiva [Cirilo, 2008].

Na atividade industrial demanda-se uma troca contínua de informação entre equipamentos, a implantação de RSSFs são uma opção interessante neste cenário por propiciar essa troca coordenada de informação entre dispositivos. Assim, a opção por redes sem fio em ambientes industriais são interessantes em relação ao potencial de economia de recursos em lançamento e manutenção de redes guiadas em redes que podem contabilizar mais de dez mil dispositivos num alcance de um quilômetro quadrado [Brown et al., 2018].

2.2. Identidade e Ciclo de vida de credenciais

Em controle de acesso, a identidade pode ser definida como uma reapresentação de uma entidade física ativa. Esta entidade pode ser um ser humano, um sistema, um dispositivo, sensor ou atuador [Benantar, 2006]. A identidade ainda pode ser definida como uma base para atribuição de privilégios em um sistema [Pfitzmann and Hansen, 2010]. A identidade é comprovada por meio de credenciais, e o conceito de credencial pode

ser definido genericamente como um dado, ou conjunto de dados, para verificar a identidade e também como informações que fornecem evidências de autenticidade de uma entidade [Bertino and Takahashi, 2010]. Em controle de acesso, é vital que a identificação das entidades utilizem apenas credenciais registradas e válidas para autenticação. Para isso, são atribuídos estados para as credenciais. Segundo a literatura [Rodriguez, 2009, Eludiora et al., 2011] estes estados do ciclo de vida são: Registro, Armazenamento, Uso, Atualização, Revogação (e/ou expiração), Arquivamento e possível Destruição (Figura 1).

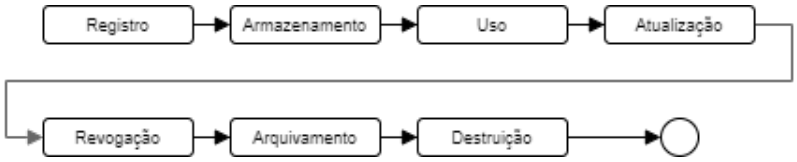

Figura 1. Ciclo de vida de credenciais.

O ciclo de vida de credenciais (Figura 1) obedece um fluxo que depende dos requisitos de um determinado cenário, podendo haver variações como o re-uso de credenciais que embora não recomendado pode ser necessário. Em contextos de redes privadas IIoT os dispositivos como sensores e atuadores são as principais entidades envolvidas no processo de controle de acesso. Portanto, as credenciais envolvidas neste contexto são majoritariamente relativas a dispositivos e usuários não humanos.

2.3. LoRaWan

A LoRaWAN é uma LPWAN com padrão de arquitetura de rede aberto definido pelo grupo LoRa Alliance. Esta utiliza o padrão de modulação LoRa (Figura 2) e seu objetivo é padronizar a implantação das LPWANs no cenário de IoT. Existem diversos casos de uso de LoraWan no contexto industrial [Lora-Alliance, 2021]. Neste trabalho, especificamente, o cenário problema é de uma indústria do ramo de aço e siderurgia. No contexto de redes IIoT, características das LPWAN LoraWan são relevantes por conta com a utilização de um espectro aberto o que torna desnecessária qualquer autorização regulatória. Outros atributos das LoraWan são um protocolo aberto, a possibilidade da criação de redes privadas e o baixo custo [Silva, 2019].

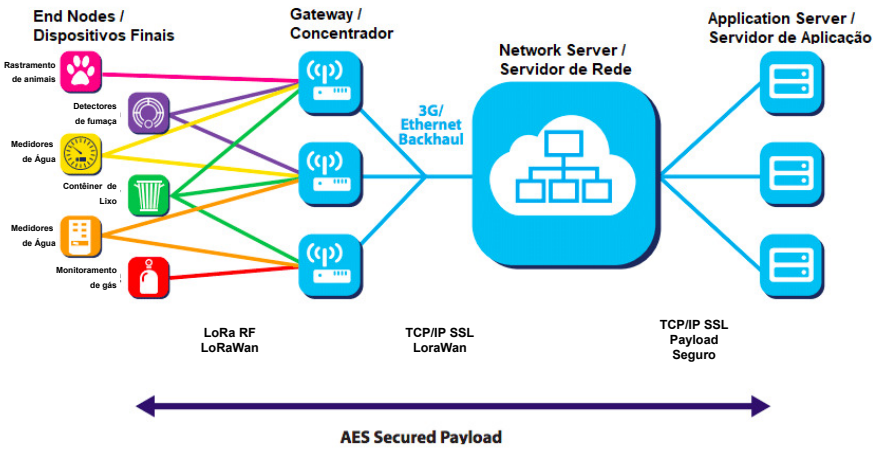

Figura 2. Arquitetura de rede LoRa. Adaptado de: [Lora-Alliance, 2021].

As redes em LoraWan podem oferecer serviços como monitoramento, rastreamento entre outros. As redes LoraWan possuem capilaridade em densos ambientes internos ou urbanos o que favorece a aplicação em cenários como o monitoramento industrial

como proposto neste trabalho. Conforme a Figura 2, pode-se observar que a arquitetura da rede do LoRaWAN funciona em formato de estrela. Tipicamente, a topologia é composta por dispositivos finais, *gateways*, servidores de rede e servidores de aplicação. Os dispositivos finais são os elementos mais básicos da rede, são sensores, atuadores e outros dispositivos. Neste trabalho os dispositivos finais de IIoT são voltados ao sensoriamento industrial. Outros elementos da arquitetura LoraWan são os *gateways*, que intermedeiam e retransmitem mensagens entre os dispositivos finais e os servidores de rede. Os servidores de rede por sua vez são responsáveis por receber as informações dos *gateways* e enviá-las para a aplicação, nesse caso é a central de monitoramento fabril. Os servidores de aplicação podem disparar ações com base nos dados de sensoriamento, armazenar e disponibilizar as informações via Web [Bonaldi and Peroni, 2019].

No contexto de IIoT, uma rede industrial pode atingir rapidamente uma quantidade expressiva de dispositivos finais que precisam estar conectados seguramente para exercer seu sensoriamento ou atuação. Tipicamente, para conectar-se a uma rede é necessário inserir credenciais as quais são geralmente vinculadas a uma ou mais pessoas. Neste sentido, percebe-se que cada vez mais há um necessidade de vincular credenciais a dispositivos que não sejam diretamente vinculadas a credenciais de pessoas e sim aos dispositivos e consequentemente alinhadas ao novo paradigma de IIoT.

3. Problema

Em contextos LPWAN e IIoT privados, a utilização de protocolos de redes sem fio deve obedecer a critérios de produtividade mas também de segurança. Em sensoriamento em atividades industriais, cenário desta pesquisa, o protocolo LoraWan é amplamente utilizado. De modo geral, o problema deste trabalho se concentra na análise da garantia destes requisitos de segurança. De maneira específica, a proposta de trabalho visa analisar a implementação do processo de controle de acesso em redes LoraWan especialmente no que se refere ao ciclo de vida de dispositivos finais em uma rede privada industrial. Desta maneira, o objetivo específico é fazer uma análise de segurança em relação ao ciclo de vida de credenciais no cenário proposto.

Em redes LoraWan privadas, especialmente no cenário proposto neste trabalho, os dispositivos podem estar em lugares de difícil acesso. Portanto, esta gestão das identidades muitas vezes deve ser feita sem o acesso físico ao dispositivo, o que facilita a comprovação de sua autenticidade no registro. Deste modo, identifica-se um problema de como gerenciar seguramente uma quantidade expressiva de dispositivos IIoT que necessitam possuir credenciais seguras que demandem o mínimo de interação humana e possam ter seus atributos de segurança gerenciados em grupo e de maneira ordenada e dinâmica. Nota-se que a configuração manual não representa uma opção viável dentro deste conceito. Por outro lado, as empresas não precisam apenas autorizar os dispositivos IIoT legítimos, mas também mitigar que dispositivos indevidos (maliciosos ou não) se conectem em *gateways* da estrutura.

4. Proposta de pesquisa

Em consonância com a questão de pesquisa deste trabalho, a pesquisa tem como proposta fazer uma análise do ciclo de vida de credenciais de dispositivos IIoT em redes privadas LoraWan. Esta análise é centrada nas complexidades relativas ao ciclo de vida quando

aplicado a variáveis de contexto e de aplicação no cenário descrito neste artigo. Para tanto o trabalho coloca como proposta de arquitetura, um esquema de autenticação que podem utilizar recursos (e.g., LDAP, identidades federadas, TPM, etc.) com atributos que possam garantir a correta identificação de dispositivos e os privilégios que estes podem ter na rede privada da organização (Figura 3).

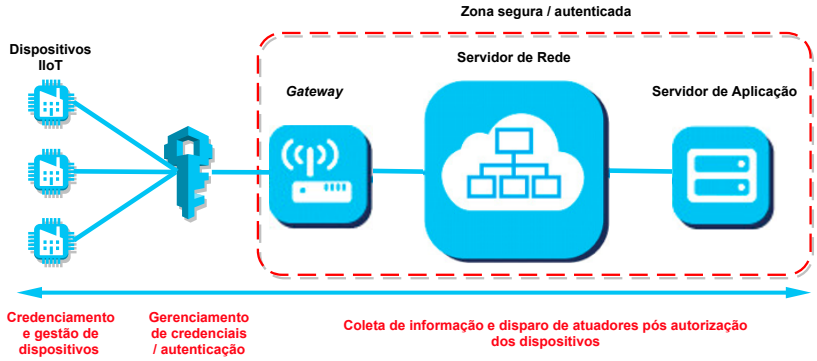

Figura 3. Proposta de arquitetura com gerenciamento de credenciais.

Conforme a Figura 3, na arquitetura proposta os dispositivos finais que neste caso serão dispositivos de sensoriamento ambiental fabril, após o registro na rede, passam por uma instância de autenticação na qual é implementado o gerenciamento de credenciais para que os dados obtidos por estes passem pelo *gateway* seguindo o fluxo de dados na rede. Além do processo de registro e autenticação, os demais processos de gerenciamento de credenciais serão implementados.

A proposta consiste em criar um novo esquema com todos os atributos possíveis que garantam a identificação única do dispositivo, bem como seus recursos, em uma abordagem centrada nos dispositivos e suas funcionalidades (não nas pessoas que os utilizam). Processos como o armazenamento, revogação e destruição de credenciais, como parte do processo geral do ciclo de vida de credenciais também serão implementados de modo a garantir a atualidade e autenticidade das credenciais. A partir do desenvolvimento da proposta será eleito o método de gerenciamento de autenticação, podendo ter configurações de autenticação distribuída, autenticação federada ou outra arquitetura de autenticação.

Através de técnicas de pesquisa-ação serão documentados os cenários de aplicação em um empresa parceira, na área de tratamento de aço laminado, que já dispões de diversos sistemas de sensoriamento e busca aprimorar seu processo através de IIoT. Assim planos e cenários de testes serão desenvolvidos e divulgados de acordo com a política de privacidade (cfme.a LGPD e outras normas internacionais que a empresa segue).

5. Considerações & Trabalhos futuros

O uso de IIoT de forma prática, com uma mudança de paradigma de credenciais centradas em dispositivos e não pessoas, é um desafio relevante. Percebe-se a necessidade em IIoT em gerenciar credenciais de um forma segura e dinâmica para não incorrer em erros já ocorridos com IoT em redes domésticas ou casos de grande corporações que tiverem seus dispositivos IIoT manipulados indevidamente. Os próximos passos são o detalhamento da análise de requisitos, definição do plano de testes, descrição de um esquema LDAP (ou outro) e versão inicial do protótipo. A parte final da pesquisa incluirá em melhorias do protótipo até a sua implantação e testes no cenário real controlado na empresa parceira.

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

Referências

Benantar, M. (2006). *Access control systems: security, identity management and trust models*. 1 edition. ISBN: 978-0-387-00445-7, 262 pages, Springer US.

Bertino, E. and Takahashi, K. (2010). *Identity management: Concepts, technologies, and systems*. 1 edition. ISBN: 9781608070398, 196 pages, Artech House.

Bonaldi, G. T. and Peroni, J. V. d. A. (2019). Rede lora® e protocolo lorawan aplicados na agricultura de precisÃo no brasil. Disponível em: http://repositorio.ufsm.br/handle/1/19446.

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

Caldas, A., Degelo, R., Mota, E., and Carvalho, C. B. (2017). Compressão de dados sem perdas para dispositivos iot. Disponível em: https://repositorio.ufsc.br/handle/123456789/216077.

Cirilo, C. E. (2008). Computação ubíqua: definição, princípios e tecnologias. *São Carlos: UFSCar*, Volume 9. Disponível em: https://docit.tips/download/computacao-ubaquadefiniaao-principios-e-tecnologias-carlos.pdf.

Eludiora, S., Abiona, O., Oluwatope, A., Oluwaranti, A., Onime, C., Kehinde, L., et al. (2011). A user identity management protocol for cloud computing paradigm. *Int'l J. of Communications, Network and System Sciences*, 4(03):152.

Lora-Alliance (2015). A technical overview of LoRa and LoRaWAN. Technical report. Disponível em: https://lora-alliance.org/wp-content/uploads/2020/11/what-is-lorawan.pdf. Acesso em: 11 ago 2021.

Lora-Alliance (2021). a digital revolution for oil & gas from scada to industrial iot. Technical report. Disponível em: https://lora-alliance.org/wp-content/uploads/2021/04/LoRaWAN-OIl-Gas.pdf. Acesso em: 11 ago 2021.

Loureiro, A. A., Nogueira, J. M. S., Ruiz, L. B., Mini, R. A. d. F., Nakamura, E. F., and Figueiredo, C. M. S. (2003). Redes de sensores sem fio. In *Simpósio Brasileiro de Redes de Computadores (SBRC)*, pages 179–226. sn.

Naoui, S., Elhdhili, M. E., and Saidane, L. (2016). Enhancing the security of the iot lorawan architecture. *2016 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, pages 1–7.

Pfitzmann, A. and Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. Disponível em: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.

Proietti Franceschilli, C. (2019). Beyond the gdpr: data protection in the context of industry 4.0.

Rodriguez, U. F. (2009). *Privacy model for federated identity architectures*. PhD thesis, Institut National des Télécommunications; Instituto tecnológico autónomo ....

Silva, F. E. S. e. (2019). Lorawan para comunicações de redes elétricas inteligentes em áreas suburbanas e rurais. Disponível em: http://repositorio.ufsm.br/handle/1/19446.