Autenticação de Oráculos em um Blockchain usando Contexto Físico como Segundo Fator de Autenticação

Wilson S. Melo Jr.[1], **Luiz F. R. C. Carmo**[1,2]

[1]Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro)
Duque de Caxias, RJ – Brasil

[2]Universidade Federal do Rio de Janeiro (UFRJ)
Programa de Pós-Graduação em Informática (PPGI) – Rio de Janeiro, RJ – Brasil

{wsjunior,lfrust}@inmetro.gov.br, rust@nce.ufrj.br

Abstract. *Oracles are entities that feed blockchains with information from the external world. In this work, we use physical context-based authentication as a second factor of authentication to oracles. This idea takes advantage of information from the physical world to identify an oracle based on its behavior. Thus this strategy does not depend on trusty third parties. We implement our proposal for a distributed measuring system describe in the literature. Our results demonstrate that our proposal makes oracles' authentication more robust, since it aggregates physical context information and so offers natural protection against attacks involving measurements tampering.*

Resumo. *Oráculos são entidades que proveem informação do mundo externo para smart contracts em um blockchain. Neste trabalho, usamos autenticação de contexto físico como segundo fator de autenticação para oráculos. Essa ideia vale-se do uso informações do mundo físico para caracterizar o comportamento do oráculo, sem a dependência de terceiras partes confiáveis. Nossa proposta é implementada de forma prática sobre um sistema distribuído de medição baseado em blockchains, descrito na literatura. Os resultados demonstram que nossa proposta torna o processo de autenticação de oráculos mais robusto, uma vez que agrega informações do seu contexto físico, e serve naturalmente como proteção contra ataques envolvendo fraude de medições.*

1. Introdução

Blockchain é uma tecnologia que tem despertado a atenção nos últimos anos em razão das diversas possibilidades de aplicação que podem ser propostas [Nakamoto 2008, Zheng et al. 2017, Dai et al. 2019]. Basicamente, uma rede *blockchain* permite a seus participantes realizarem transações associadas a bens digitais (*digital assets*), sem a necessidade de que as partes envolvidas confiem umas nas outras. Diferentemente de aplicações centralizadas, onde a confiança é provida por uma terceira parte na qual todos confiam, em uma rede *blockchain* a confiança é obtida de forma distribuída por meio de protocolos de consenso [Cachin and Vukolić 2017].

Uma questão, todavia, emerge diante da possibilidade de se usar uma rede *blockchain* para gerenciar bens físicos (*physical assets*). Por exemplo, uma aplicação envolvendo negociação de criptomoedas é significativamente distinta de uma aplicação voltada à venda de energia elétrica por microgeradores. Na primeira aplicação, uma carteira de criptomoedas pode ser mantida pelo simples histórico de registros armazenados

no *blockchain*. Em contrapartida, uma transação de compra e venda de energia requer evidências de que o bem físico, neste caso, o montante de energia negociado, está de fato disponível para entrega ao comprador. Para tanto, uma transação desta natureza requer que um dispositivo capaz de interagir com o mundo externo ateste a disponibilidade desse bem físico. Tal dispositivo pode ser, por exemplo, um medidor inteligente, que periodicamente informa à rede *blockchain* a quantidade de energia que um participante dispõe para negociação. Dispositivos que realizam essa função em uma rede *blockchain* são denominados *oráculos* [Gordon 2017, Mammadzada et al. 2020]. Eles são responsáveis por prover à rede *blockchain* informações a respeito do mundo externo, de modo confiável e sem influência das partes interessadas na transação.

Muitas das futuras aplicações de *blockchains* que hoje estão sendo propostas dependem fortemente do uso de oráculos, que são vistos inclusive como os elementos de integração entre *blockchains* e Internet das Coisas [Gordon 2017]. Todavia, mesmo sendo um tema promissor, os desafios relacionados à autenticidade e integridade das informações providas por oráculos ainda são pouco explorados na literatura científica [Zhang et al. 2016, Adler et al. 2018, Ma et al. 2019]. Grande parte das soluções de oráculos que lidam com dados de sensores (i.e., informações do mundo físico) dependem da existência de uma terceira parte confiável [Mammadzada et al. 2020], um conceito que vai na direção oposta àquele que justifica a concepção de *blockchains* como uma solução de confiança descentralizada. Assim, mecanismos de autenticação alternativos, que sejam independentes da existência de terceiras partes confiáveis, podem constituir soluções promissoras e, portanto, merecem ser investigados.

Um conceito que pode ser explorado na autenticação de oráculos é a *Autenticação baseada em Contexto Físico* (ACF) [Melo Jr. et al. 2018]. A ACF consiste no uso de informações extraídas do mundo físico de modo a caracterizar situações às quais entidades de um sistema físico estão sujeitas [Habib and Leister 2015]. O contexto físico é descrito pelas propriedades físicas de um sistema e de suas entidades, como também pelos resultados de suas múltiplas interações. A ACF pode ser associada a aplicações tais como o uso de biometria comportamental para autenticar indivíduos [Rostami et al. 2013], ou de características físicas e de variáveis ambientais para autenticar dispositivos inteligentes [Karapanos et al. 2015], ou mesmo do posicionamento espacial e temporalidade para identificar módulos de um sistema ciber físico [Juuti et al. 2017]. O trabalho de [Melo Jr. et al. 2018] apresenta uma metodologia para uso de ACF como *segundo fator de autenticação* (2FA) em sistemas que apresentam interação ciber física. Se um oráculo interage com o mundo físico (como no exemplo de venda de energia citado anteriormente), ele estará de imediato relacionado a um contexto físico que pode ser usado como evidência complementar de sua identidade e autenticidade.

Neste trabalho, apresentamos uma proposta de como a ACF pode ser aplicada como 2FA em oráculos que proveem informação do mundo físico para uma rede *blockchain*. A principal vantagem dessa abordagem é tornar mais robusto um mecanismo de autenticação pré-existente, sem a necessidade de se recorrer a soluções envolvendo uma terceira parte confiável. Além disso, o uso da ACF acrescenta à autenticação informações de contexto do mundo físico, que são por definição difíceis de serem estimadas por um ataque cibernético [Melo Jr. et al. 2018], como por exemplo as evidências de coalocação e simultaneidade. Nossa proposta é implementada de forma prática, usando como objeto

de estudo um Sistema Distribuído de Medição (SDM) de velocidade de veículos baseado em *blockchains*, onde sensores indutivos funcionam como oráculos para *smart contracts* que implementam funções de medição [Melo Jr. et al. 2019]. Os resultados obtidos demonstram que nossa proposta é funcional, permitindo a correta autenticação de oráculos em aproximadamente 80% dos casos, de modo a proteger a integridade das informações e ao mesmo tempo prevenir fraudes relacionadas à medição de velocidade.

2. Preliminares

2.1. Blockchains

Conceitualmente, um *blockchain* pode ser descrito como uma estrutura de dados imutável (denominada *ledger*), onde novos registros podem apenas ser adicionados, e jamais removidos. Esta estrutura de dados é replicada e compartilhada entre os nodos (também chamados *peers*) de uma rede, o que explica o termo *rede blockchain* [Christidis and Devetsikiotis 2016]. O *ledger* consiste em uma sequência de blocos de informação onde o bloco n é cripotograficamente ligado ao bloco $n-1$ por meio de uma função de dispersão (*hash*). Consequentemente, o bloco n não pode ser modificado sem que todos os blocos subsequentes $n+i, ..., n+k$ também o sejam [Nakamoto 2008].

Por ser um modelo descentralizado, a disponibilidade de uma rede *blockchain* não depende de uma entidade central de controle, o que significativamente reduz custos na oferta de serviços [Zheng et al. 2017]. Por sua vez, a integridade do *ledger* é garantida por *consenso* entre os *peers*, o que previne qualquer modificação na cadeia de blocos, e ao mesmo tempo impõe a necessidade um acordo entre as partes a respeito de cada novo bloco adicionado ao *ledger* [Vukolić 2016, Sousa et al. 2018]. Virtualmente, um *blockchain* pode armazenar qualquer ativo digital (*digital asset*), desde dados simples até conjuntos de instruções autoexecutáveis, definidos como *contratos inteligentes* (*smart contracts*). Tal aspecto torna um *blockchain* não apenas um repositório de dados, mas também uma plataforma distribuída para execução de fluxos de trabalho automatizados [Christidis and Devetsikiotis 2016]. Uma vez que os *smart contracts* são executados de forma independente e automática por cada um dos *peers* que compõem a rede *blockchain*, tanto a integridade dos dados como também do *smart contract* é garantida pelas propriedades intrínsecas do ledger.

2.2. Autenticação baseada em Contexto Físico

Em computação, define-se *contexto* como *"qualquer informação útil para caracterizar a situação de uma entidade"* [Dey and Abowd 1999]. Assim, o *contexto físico* remete à ideia de que informações extraídas do mundo físico podem ser úteis para caracterizar situações às quais as entidades de um sistema físico estão sujeitas [Habib and Leister 2015]. Tais informações podem ser aplicadas em problemas clássicos de segurança ciber física, em especial na identificação e autenticação de entidades, em uma metodologia denominada *Autenticação baseada em Contexto Físico* (ACF) [Melo Jr. et al. 2018]. É o caso, por exemplo, de soluções que exploram a biometria comportamental [Rostami et al. 2013] como fator de autenticação de usuários de um sistema, ou ainda o uso de propriedades construtivas de dispositivos eletrônicos para a criação de identificadores fortes, e.g. *Physical Unclonable Functions* [Mauw and Piramuthu 2013]. É possível mencionar também propostas de autenticação de entidades com base em

variáveis que descrevem o ambiente onde elas se encontram [Karapanos et al. 2015], ou ainda o uso de posicionamento espacial e temporalidade, em uma abordagem denominada *autenticação transparente* [Juuti et al. 2017].

No trabalho de [Melo Jr. et al. 2018], os autores propõem o uso de ACF como um segundo fator de autenticação (2FA) em cenários onde as entidades apresentam interação ciber física. É o caso de diversos sistemas envolvendo sensores, controladores, componentes IoT e outros dispositivos inteligentes (*smart*), incluindo instrumentos de medição. Os autores desenvolvem uma metodologia completa para implementação de ACF como 2FA, a qual provê duas propriedades de autenticação que protegem as entidades contra ataques do tipo *replay* e *relay*. Estas propriedades são:

- **Coalocação**: quando duas entidades autenticam-se usando ACF, tem-se que ambas encontram-se em uma mesma localização física, dentro do escopo de observação delimitado por seu contexto físico;
- **Simultaneidade**: quando duas entidades autenticam-se usando ACF, tem-se que ambas capturam ao mesmo tempo os mesmos eventos que descrevem o contexto físico.

2.3. Blockchains e Oráculos

Conforme mencionado, o conceito de oráculo no contexto de redes *blockchain* é ainda recente, e pouco explorado na literatura científica [Zhang et al. 2016, Adler et al. 2018, Ma et al. 2019, Mammadzada et al. 2020]. Oráculos são entidades confiáveis e aptas a prover informações do mundo externo para dentro do *blockchain*. Geralmente, *smart contracts* utilizam oráculos como provedores de informação do mundo externo, e tomam decisões com base nessas informações. Entretanto, as premissas de segurança assumidas para dados e *smart contracts* internos ao *blockchain* não se aplicam aos oráculos. Assim, são necessários mecanismos adicionais para se garantir que tanto um oráculo quanto as informações por ele providas são confiáveis.

Por definição, oráculos são entidades identificáveis e autenticadas por algum mecanismo de segurança conhecido. O recente trabalho de [Mammadzada et al. 2020] apresenta uma revisão sistemática descrevendo as principais propostas de implementação de oráculos para *blockchains*. Chama a atenção que, dos 23 trabalhos selecionados na literatura, mais da metade das soluções envolvendo oráculos dependem de uma terceira parte confiável (*Trusted Third Party* - TTP) para validação dos dados providos. Em complemento, um número significativo dessas soluções propõem o uso de Infraestruturas de Chave Publica (ICPs) como mecanismo de autenticação, que por sua vez também dependem de TTPs (no caso, as Autoridades Certificadoras). Embora TTPs e ICPs sejam soluções crassas em problemas que requerem identificação e autenticação de entidades e mensagens, elas geralmente implicam em soluções centralizadas. Tal conceito segue na direção oposta à filosofia base de uso de um *blockchain*, que propõe obter-se confiança entre as partes por meio de uma solução distribuída e descentralizada, e não dependente de uma TTP.

Quanto à sua arquitetura, oráculos podem ser classificados em *centralizados* e *descentralizados* [Ma et al. 2019]. Uma arquitetura centralizada se baseia em entidades confiáveis que obtém informações do mundo externo quando requisitadas por um *smart contract*. Embora conceitualmente mais simples, arquiteturas centralizadas inevitavelmente introduzem pontos únicos de falha (*Single Point of Failure* - SPOF), que facilmente

se tornam alvos de ataques de segurança. Uma arquitetura descentralizada, por sua vez, estabelece oráculos como entidades redundantes, que tem a função de prover informações e também validá-las, por meio de protocolos envolvendo voto e verificação. Isso elimina a existência de SPOFs, mas por outro introduz complexidade ao processo desempenhado pelos oráculos.

Town Crier [Zhang et al. 2016] e *Astraea* [Adler et al. 2018] são as duas soluções de oráculos mais citadas na literatura. O primeiro é uma solução centralizada, implementada para a plataforma Ethereum[1], que utiliza a tecnologia Intel SGX[2] para prover verificação confiável de valores vindos do mundo externo. Por sua vez, o Astraea é uma solução descentralizada, que distribui a tarefa de prover informações do mundo externo a diferentes entidades, por meio de funções específicas de voto e verificação, atribuindo incentivos à realização das mesmas, de forma integrada à plataforma *blockchain* adotada.

3. Autenticação de oráculos usando contexto físico como 2FA

3.1. Premissas iniciais

Neste trabalho, desenvolvemos uma proposta de uso de ACF como 2FA para o problema de autenticação de oráculos em um *blockchain*. Ela consiste de uma arquitetura descentralizada, que utiliza dispositivos seguros como entidades provedoras de informação do mundo real. O uso de ACF como 2FA fortalece o mecanismo de autenticação por prover evidências de coalocação e simultaneidade. Deste modo, tem-se uma estratégia de autenticação que faz uso de informações que estão naturalmente disponíveis em um sistema que apresenta interação ciber física, ao mesmo tempo que independe de soluções centralizadas, tais como ICPs e TTPs.

Para tanto, nossa proposta estabelece um cenário de aplicação que satisfaz, por premissa, os seguintes requisitos:

1. As entidades que desempenham o papel de oráculos possuem um componente criptográfico de chaves assimétricas, capaz de produzir assinaturas de chave pública, e cuja chave privada é armazenada de forma segura. Essa solução dispensa a necessidade de uma ICP, uma vez que não requer a existência de um certificado digital, mas tão somente de diretivas criptográficas que evidenciem integridade e autenticidade;
2. As entidades-oráculo redundantes (i.e., que autenticam uma a outra para prover informações do mundo externo) compartilham um mesmo contexto físico, e são protegidas contra ataques internos, satisfazendo as condições estabelecidas em [Melo Jr. et al. 2018] para aplicação da metodologia de ACF.

Para ilustrar o cenário de aplicação, foi escolhida uma arquitetura de medição distribuída baseada em *blockchains*, desenvolvida em [Melo Jr. et al. 2019]. Esta arquitetura consiste de um Sistema Distribuído de Medição (SDM) que integra medidores de velocidade de veículos, usualmente conhecidos no Brasil como *radares*. Medidores de velocidade são uma solução eficiente para estimar o uso de vias públicas, obter estatísticas de tráfego de veículos e também fiscalizar limites de velocidade [Ki and Baik 2006, Ali et al. 2011]. Sensores indutivos detectam o veículo em função do

[1]https://ethereum.org

[2]https://software.intel.com/sgx

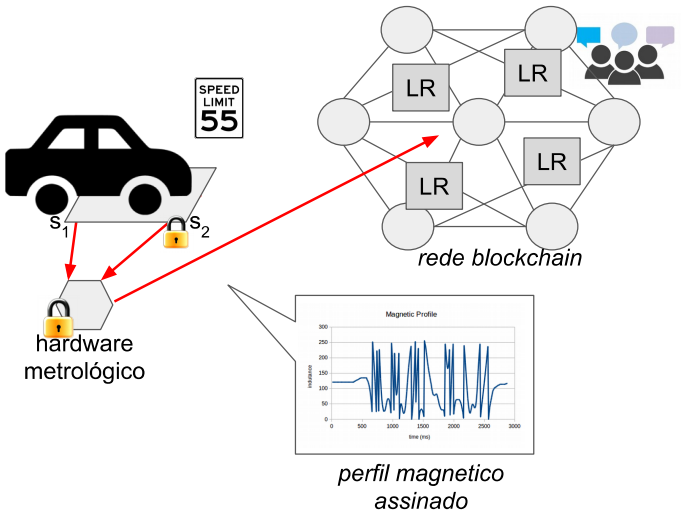

Figura 1. SDM para medição de velocidade de veículos usando *blockchains*

deslocamento de sua massa metálica, determinam sua velocidade e capturam uma ou mais imagens, identificando a placa de licenciamento do veículo. A medição de velocidade e as imagens obtidas constituem o *registro legalmente relevante*, o qual deve ser confiável e protegido contra fraudes de medição. Por implementar uma funcionalidade sensível, que é a geração de autos de infração, os medidores de velocidade são frequentemente colocados sob suspeita por motoristas e mesmo entidades civis. Alguns especulam a existência de uma "indústria da multa", responsável por fraudar deliberadamente o cálculo da velocidade do veículo, ou ainda por atribuir infrações a veículos que sequer trafegaram pela via onde o medidor de velocidade é instalado. Assim, quaisquer medidas e iniciativas associadas ao aumento da confiabilidade na medição realizada por esses instrumentos são sempre bem vindas e incentivadas.

3.2. Descrição do SDM de velocidade

Medidores de velocidade são geralmente construídos como um *instrumento de medição tipo U* [WELMEC 2015], o que significa que seu software executa em um computador universal. Isso acontece porque medidores de velocidade modernos implementam uma extensa lista de requisitos e agregam um conjunto significativo de funcionalidades ditas *não legalmente relevantes* (NLR). Consequentemente, o software desses medidores é complexo e de difícil avaliação, validação e verificação por parte da autoridade metrológica responsável pela regulação desses instrumentos. Além disso, os fabricantes de medidores de velocidade usualmente se queixam da necessidade de se disponibilizar o código fonte do software de medição para avaliação, alegando questões pertinentes à propriedade intelectual. Um terceiro aspecto é o fato que tais instrumentos são instalados ao longo de vias públicas, sendo muitas vezes espalhados em extensas áreas geográficas, o que dificulta a realização de inspeções regulares por parte de agentes de metrologia.

Em razão dos desafios descritos, [Melo Jr. et al. 2019] propõe um SDM para medição de velocidade de veículos que funciona conforme apresentado na Figura 1. Neste modelo, o medidor instalado em uma via pública é projetado como um dispositivo de *hardware* simples, à prova de adulteração (*tamper proofing*), que consiste de dois sensores indutivos que capturam o *perfil magnético* do veículo. O perfil magnético consiste da

variação de corrente induzida sobre o sensor em função da variação de massa metálica resultante do movimento realizado pelo veículo. O *hardware* de medição faz uso de uma chave privada para assinar digitalmente o perfil magnético, e por fim envia o perfil assinado para o SDM, constituído por uma rede *blockchain*. Por sua vez, a rede *blockchain* executa o *software legalmente relevante* (LR) como um *smart contract*, determinando a velocidade do veículo em função do perfil magnético recebido.

3.3. Autenticação de oráculos usando ACF como 2FA

No sistema SDM descrito na subseção anterior, os sensores indutivos do *hardware* de detecção de veículos funcionam como oráculos, provendo informações do mundo físico para uma rede *blockchain* que armazena transações digitais (i.e., o registro LR). A autenticação do *hardware* de medição pela rede *blockchain* é feita por meio da verificação da assinatura de chave pública no registro LR. Como o medidor é constituído por um *hardware* protegido, tal procedimento pode ser dito como seguro, uma vez que a chave privada do hardware não pode ser exposta. Entretanto, tal mecanismo garante apenas a integridade do *hardware* de aquisição de sinais, sem garantir que este é usado corretamente para detecção de um veículo em uma respectiva via pública. Evidentemente, esse mecanismo de autenticação não acrescenta qualquer evidência física associada à detecção de um veículo especifico em determinado local, nem mesmo ao instante de detecção deste veículo no tempo. Assim, o que propomos é o uso da ACF como segundo fator de autenticação, de modo a exigir que o oráculo apresente evidências e coalocação e simultaneidade, e deste modo tornando o mecanismo de autenticação mais robusto.

Nossa proposta de autenticação adota a seguinte estratégia. Define-se que um dos sensores indutivos usados na medição (na Figura 1 esse sensor corresponde a S_2) está sob controle da autoridade metrológica e possui sua própria chave privada, de forma que o *hardware* de medição recebe as informações desse sensor já assinadas. De posse dos sinais de S_1 e S_2, o *hardware* de medição submete uma transação de envio de registro LR para o SDM (i.e., *blockchain*), que além de autenticar S_1 e S_2 por meio de suas assinaturas digitais, implementa também a ACF de S_1. A ideia consiste em correlacionar o *perfil magnético* do veículo obtido pelo sensor S_1 àquele informado pelo sensor S_2. Se os perfis são correspondentes, entende-se que a detecção do veículo por S_1 e S_2 descreve um mesmo contexto físico decorrente da passagem do veículo por eles. Isso também evidencia que os sensores satisfazem as condições de coalocação e simultaneidade.

O procedimento de ACF é executado na rede *blockchain* pelo mesmo *smart contract* responsável por coletar o registro LR. Isso implica que uma transação composta pelos perfis magnéticos dados por S_1 e S_2 invoca o código autoexecutável de um *smart contract* para comparar os perfis e decidir se eles descrevem o mesmo contexto físico de detecção de veículo. Pode-se aplicar assim a metodologia proposta em [Melo Jr. et al. 2018], definindo-se uma função de comparação C entre os contextos físicos descritos por S_1 e S_2, e um limiar de aceitação Th. Caso a comparação não satisfaça a condição de limiar definida, o oráculo S_1 não é autenticado, e o registro LR informado pode ser considerado pendente de verificação por parte da autoridade metrológica.

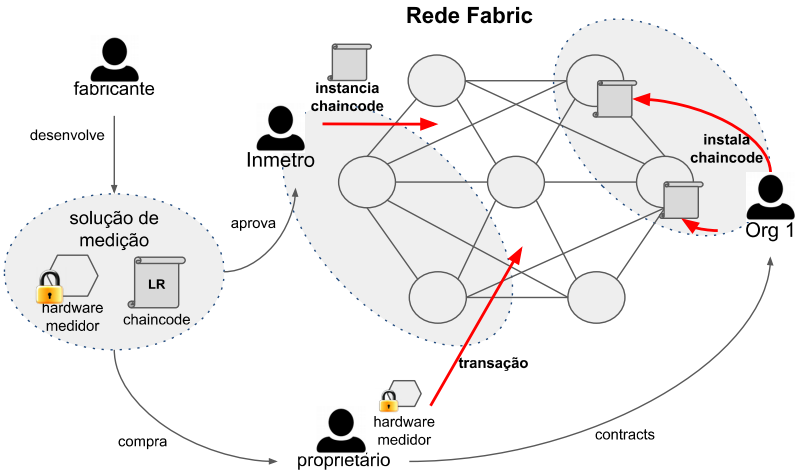

Figura 2. Implementação do SDM usando *Hyperledger Fabric*

4. Experimento prático e Resultados

4.1. Descrição da Arquitetura Utilizada

O experimento criado para se avaliar nossa proposta faz uso do *Hyperledger Fabric*[3] [Androulaki et al. 2018], uma plataforma *blockchain* completa de código aberto, para implementar uma rede *blockchain* permissionada onde os *peers* cooperam entre si para armazenar medições de velocidade e executar *software* legalmente relevante (LR) a partir de *smart contracts*. Os *peers*, neste caso, são providos por entidades que querem oferecer recursos computacionais para execução de *software* de medição, podendo ser recompensados por isso, ou ainda por entidades que têm interesse em fiscalizar a medição de velocidade nesses instrumentos, e que decidem participar da rede *blockchain* de forma voluntária.

Uma visão geral do cenário prático envolvendo nossa proposta é descrita na Figura 2. Fabricantes desenvolvem soluções metrológicas constituídas basicamente pelo *hardware* de medição e pelo *software* LR que processa os perfis magnéticos e determina a velocidade do veículo. O *software* LR é, neste caso, um *smart contract*, ou ainda um *chaincode*, nome dado ao *smart contract* no contexto do *Fabric*. Cada solução desenvolvida é previamente verificada e aprovada pela autoridade metrológica, aqui representada pelo Inmetro[4]. Uma vez aprovadas, as soluções de medição podem ser adquiridas por proprietários (i.e., entidades que gerenciam ou fiscalizam o trânsito em vias públicas) e postas em operação. Além de instalar o *hardware* de medição, o proprietário faz uso dos serviços oferecidos por organizações independentes (representadas na Figura 2 como Org1) que possuem acordos com os fabricantes para execução do respectivo *chaincode* associado ao processamento do perfil magnético. Basicamente, cada organização participante da rede *blockchain* (incluindo o Inmetro e qualquer outra organização interessada em fiscalizar as medições) disponibiliza *peers* que se integram por meio das ferramentas da plataforma *Fabric*.

O *Fabric* inclui dois conceitos interessantes para construção de um SDM: *endorsers* e políticas de segurança. *Endorsers* são *peers* que efetivamente executam o *chain-*

[3] `https://www.hyperledger.org/projects/fabric`
[4] Instituto Nacional de Metrologia, Qualidade e Tecnologia - www.inmetro.gov.br

code. Os demais *peers* apenas validam essa execução. Tal estratégia tem um impacto significativo em questões de propriedade intelectual e desempenho. Primeiramente, ela permite que o fabricante revele seu *software* LR apenas aos *peers* escolhidos por ele. Deste modo, conflitos associados a propriedade intelectual são resolvidos diretamente entre o fabricante e a entidade que provê o *peer*. Por sua vez, a quantidade de *peers* autorizados a executar um determinado *chaincode* pode ser dimensionada em função da demanda de medições, ou mais especificamente em função do número de medidores de velocidade contemplados. Isso implica que um fabricante que possui muitos equipamentos pode igualmente disponibilizar seu *chaincode* LR a um número maior de *peers*, implementando assim uma solução escalável. Já as políticas de segurança permitem especificar quais organizações estão habilitadas a prover *peers* para trabalharem como *endorsers*. Ao mesmo tempo, é possível especificar que um dado *chaincode* seja executado por *endorsers* de diferentes organizações simultaneamente e determinar a comparação da resposta das diferentes execuções durante a validação de uma transação, que é realizada por todos os demais *peers* da rede *blockchain*. Tal flexibilidade impõe restrições que aumentam significativamente o custo associado a ataques de conluio.

O fato de apenas os *endorsers* conhecerem um *chaincode* não implica que este possa ser modificado facilmente. Isso porque, antes de poder ser executado, o *chaincode* deve ser *instanciado* na rede *blockchain* por uma autoridade metrológica. Na prática, isso significa enviar uma transação à rede *blockchain* contendo o resumo criptográfico do *chaincode* instanciado, a qual é escrito no *ledger* e tornar-se, assim, imutável. Só a partir desse ponto é que os *endorsers* podem *instalar* o *chaincode*. A Figura 2 descreve como esse processo funciona. Um *endorser* confiável sempre se recusa a instalar um *chaincode* inválido. Por sua vez, se um atacante obtém sucesso em subverter um *endorser* para que este execute um *chaincode* adulterado, tal resultado será inócuo se as políticas de segurança explicitarem que a medição deve ser confrontada com aquela obtida por *endorsers* de diferentes organizações. Têm-se assim que qualquer ataque envolvendo adulteração do *software* LR requer um conluio entre os *endorsers*, o que é essencialmente uma premissa de segurança de uma rede *blockchain* que eleva significativamente o custo de um ataque bem sucedido.

4.2. Descrição dos Testes

O ambiente utilizado para executar a rede *blockchain* consistiu de 3 nodos físicos de um cluster Dell PowerEdge R410. Cada nodo possui duas CPUs Intel® Xeon® Processor E5520 com 2.27 GHz e 32 GB de memória RAM. As máquinas físicas são usadas para virtualizar os *peers* que compõem a rede *blockchain*. A rede foi configurada com um total de oito *peers*, quatro deles pertencentes à organização Inmetro e quatro deles pertencentes à Org1, e mais um serviço de ordenação usando a biblioteca BFT-SMaRt [Sousa et al. 2018], que suporta falhas bizantinas. Foi utilizada a distribuição padrão do Fabric, na versão 1.1[5]. Por sua vez, as transações representando o envio de perfis magnéticos por diferentes módulos do *hardware* de medição foram simuladas usando 4 nodos físicos de um cluster Dell PowerEdge R300, cada um deles com CPU Intel® Xeon® Processor L5410 com 2.33 GHz e 8 GB de memória RAM. O ambiente foi configurado nas dependências do LaSIGE (Laboratório de Sistemas de Grande Escala) da Faculdade de Ciências da Universidade de Lisboa.

[5]`http://hyperledger-fabric.readthedocs.io/en/release-1.1`

A simulação de transações geradas por detecção de veículos foi feita a partir de dados reais obtidos de medidores de velocidade instalados em campo. Para tal, foi utilizada uma massa de dados de 600 veículos, cedida especificamente para esse experimento pela empresa Perkons SA[6]. Os dados incluem diferentes categorias de veículos, desde carros de passeio até veículos de carga e passageiros (i.e., caminhões e ônibus).

A demanda de transações para o experimento também foi determinada em função de dados reais de tráfego de veículos. Foi considerada como referência a cidade de São Paulo, dada a existência de dados de tráfego disponibilizados pela Companhia de Engenharia de Tráfego de São Paulo (CET-SP). Segundo a CET-SP [Companhia de Engenharia de Tráfego - CET 2017], havia em 2016 aproximadamente mil medidores de velocidade distribuídos ao longo de vias públicas da cidade. O mesmo relatório aponta o fluxo médio das principais ruas do município em torno de 2.772 veículos/hora (ou $0,76$ veículos/segundo) em horários de pico. Assumindo-se essa demanda para um total de mil medidores de velocidade, foi projetada uma simulação da ordem de 800 transações/segundo.

4.3. Definição de identificadores de contexto e da função de comparação

O experimento desenvolvido utiliza o próprio perfil magnético como o identificador de contexto físico gerado pelos sensores S_1 e S_2. O conjunto de dados utilizado já disponibiliza o perfil indutivo com a aplicação de filtros digitais que limitam cada ponto a um valor inteiro sem sinal de 8 *bits*.

Quando um veículo passa sobre um laço indutivo, sua velocidade, trajetória e propriedades físicas são retratadas pelo sinal observado no perfil magnético. A velocidade do veículo geralmente é calculada a partir do perfil fornecido pelos dois sensores, cuja distância entre eles é conhecida [Ki and Baik 2006]. No experimento em questão, os sensores capturam a variação de indutância de forma sincronizada, amostrando o sinal em intervalos de tempo regulares. A ativação do primeiro sensor indica que o veículo foi detectado por ele. Quando o segundo sensor é ativado, computa-se em função do número de amostras coletadas qual foi o tempo decorrido desde a detecção do veículo pelo primeiro sensor. Uma vez que a distância entre os dois sensores é conhecida, a velocidade do veículo pode ser computada de forma trivial. Todavia, a distância entre os sensores indutivos faz com que os sinais de S_1 e S_2 apresentem-se defasados um em relação ao outro (Figura 3).

Em razão disso, foi utilizada uma função de comparação C que desloca o espectro do sinal de S_2 à esquerda (operação *shift*), na tentativa de o sobrepor ao sinal de S_1 e assim determinar a melhor correspondência entre os dois sinais, usando a *Correlação de Pearson*. A Figura 3 ilustra esse processo, aplicando um *shift* de 300 milissegundos ao sinal de S_2. Deste modo, a função de comparação C é dada pela seguinte equação:

$$C(S_1, S_2) = (1 - max(correl(S_1, bestshift(S_2)), 0) \quad (1)$$

onde $correl(...)$ é a *Correlação de Pearson* e $bestshift(...)$ é a função que avalia S_2 e determina o melhor deslocamento de modo a se obter a maior correlação com S_1. Ainda sobre a correlação, os valores negativos são considerados como zero.

[6] `http://www.perkons.com`

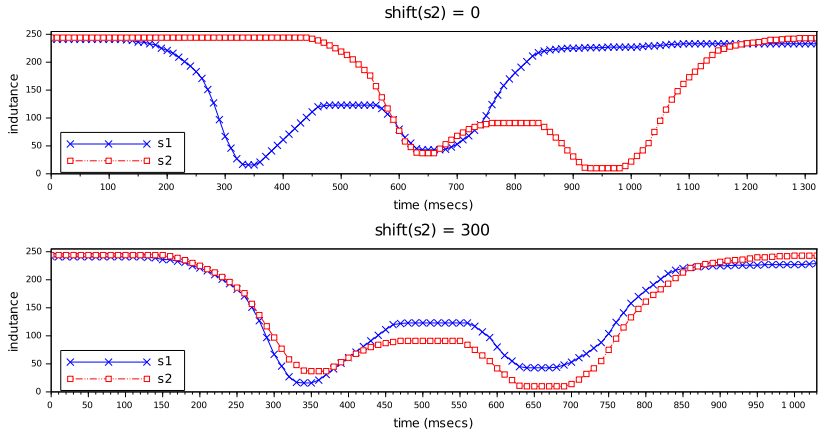

Figura 3. Defasagem do sinal de sensores indutivos e cálculo do *bestfit()*

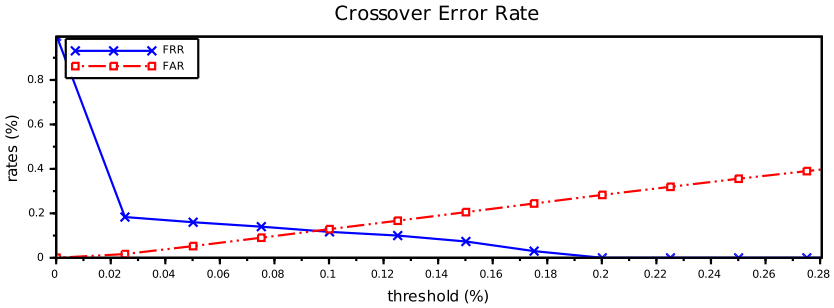

Figura 4. Variação de FRR e FAR - Autenticação de sensores indutivos

4.4. Resultados Obtidos

Os resultados do experimento foram obtidos seguindo-se a metodologia proposta por [Melo Jr. et al. 2018]. Primeiramente, um total de 600 pares de perfis magnéticos foram selecionados como massa de dados para estudo. Estes foram divididos em dois grupos com 300 amostras cada um: o primeiro para sintonia do valor de limiar Th; e o segundo para validação do valor de limiar obtido.

A Figura 4 mostra a variação das taxas FRR (*False Rejection Rate*) e FAR (*False Accept Rate*), determinando assim a *Crossover Error Rate* (CER). Como pode ser observado, o melhor ajuste para CER ocorre quando $Th \approx 0,095$. Essa é a condição que minimiza os valores de FRR e FAR. Todavia, aplica-se aqui o princípio de que um mecanismo de autenticação deve privilegiar um menor valor de FAR, ainda que se obtenha um maior valor de FRR [Melo Jr. et al. 2018]. Para um valor de $Th = 0,025$, por exemplo, o FAR fica abaixo de $0,01$ enquanto FRR se mantém em torno de $0,17$. Isso aponta que, embora o mecanismo de autenticação previna falhas e fraudes de medição (falsos negativos), um em cada 5 medições de velocidade legítimas podem ser tratadas como suspeitas (falsos positivos), em razão do elevado valor de FRR.

Os valores sugeridos para Th com a análise de CER usando os dados de teste são em seguida verificados usando os dados de validação. O resultado é sintetizado na Tabela 1. Foi obtida a matriz de confusão e os valores de FRR, FAR e FMeasure para três valores distintos de Th, a saber $0,025$, $0,05$ e $0,075$. A validação confirma o desempenho

Tabela 1. Taxas de desempenho da autenticação dos sensores indutivos

	$Th = 0,025$		$Th = 0,05$		$Th = 0,075$	
	OK	**NOK**	**OK**	**NOK**	**OK**	**NOK**
Sensores legítimos	232	68	240	60	248	52
Sensores sob ataque	681	44169	2124	42726	3621	41229
FRR	22%		20%		17%	
FAR	1,5%		4,7%		8%	
FMeasure	0,38		0,18		0,11	

estimado para o mecanismo de autenticação durante a etapa de testes. Para os valores de Th analisados, tem-se o FRR em torno de 20%, uma taxa que enfraquece o desempenho do mecanismo de autenticação, conforme já discutido. O FRR elevado afeta inclusive o valor de FMeasure, uma vez que este depende de um bom ajuste entre FRR e FAR. Em contrapartida, o valor de FAR se mantém em torno de $1,5\%$ quando é adotado um limiar $Th = 0,025$, mostrando-se um método eficiente para detectar situações onde os perfis magnéticos não são correspondentes.

Em conclusão, o desempenho do mecanismo de autenticação como um todo mostra-se eficaz para prevenir falhas e fraudes de medição associadas aos sensores indutivos. Isso é importante pois aumenta a confiabilidade das informações providas pelo medidor de velocidade. Todavia, o mecanismo resulta em uma proporção elevada de falsos negativos. Isso constitui uma limitação, uma vez que a detecção de um veículo é um evento físico único, não sendo assim possível se repetir a autenticação. Tal procedimento requer que um outro sistema, ou ainda um agente humano, proceda com a verificação de autenticidade de cada registro legalmente relevante considerado suspeito. Ainda assim, tal ônus pode ser justificado em função da eficácia do mecanismo em detectar eventuais tentativas de fraude metrológicas.

5. Conclusão

Neste trabalho, apresentamos uma proposta de uso de ACF como 2FA no problema de autenticação de oráculos de um *blockchain*. Aplicamos uma metodologia de autenticação já disponível na literatura em um SDM baseado em *blockchains*, obtendo resultados relevantes que demonstram que mecanismos de autenticação já existentes tornam-se mais robustos, de modo a prevenir ataques maliciosos envolvendo fraudes de medição. O uso de ACF nesse contexto constitui, assim, uma alternativa promissora. Em especial, quando se considera a perspectiva de criação de uma diversidade de soluções integrando *blockchains* e IoT, fica evidente uma demanda por diferentes mecanismos de autenticação para aumentar a confiabilidade das informações do mundo físico fornecidas em cada transação.

Os próximos passos deste trabalho devem incluir um estudo mais aprofundado sobre o uso de medidores inteligentes para constituir soluções descentralizadas de autenticação de oráculos. Uma vez que instrumentos de medição já lidam com problemas de autenticação há muitos anos, seu uso em soluções envolvendo oráculos é promissor e pode constituir uma alternativa bastante atraente para sistemas industriais baseados em *blockchain*.

Referências

Adler, J., Berryhill, R., Veneris, A., Poulos, Z., Veira, N., and Kastania, A. (2018). Astraea: A decentralized blockchain oracle. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1145–1152. IEEE.

Ali, S. S. M., George, B., Vanajakshi, L., and Venkatraman, J. (2011). A Multiple Loop Vehicle Detection System for Heterogeneous and Lane-less Traffic. *IEEE Transactions on Instrumentation and Measurement*, 61(5):1413–1417.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S. W., and Yellick, J. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, Porto, Portugal.

Cachin, C. and Vukolić, M. (2017). Blockchain Consensus Protocols in the Wild. In *31 International Symposium on Distributed Computing*, pages 1–16.

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4:2292–2303.

Companhia de Engenharia de Tráfego - CET (2017). Pesquisa de monitoramento da mobilidade: mobilidade no sistema viário principal: volume e velocidade - 2015. Technical report, Governo do Estado de São Paulo.

Dai, H.-N., Zheng, Z., and Zhang, Y. (2019). Blockchain for Internet of Things: A Survey. *IEEE Internet of Things Journal*, 6(5):8076—-8094.

Dey, A. K. and Abowd, G. D. (1999). Towards a Better Understanding of Context and Context-Awareness. *Computing Systems*, 40(3):304–307.

Gordon, G. (2017). *Provenance and Authentication of Oracle Sensor Data with Block Chain Lightweight Wireless Network Authentication Scheme for Constrained Oracle Sensors*. Master thesis, Saint Mary's University, Halifax, Nova Scotia.

Habib, K. and Leister, W. (2015). Context-Aware Authentication for the Internet of Things. In *International Conference on Autonomic and Autonomous Systems Context-Aware*, pages 134–139.

Juuti, M., Vaas, C., Sluganovic, I., Liljestrand, H., Asokan, N., and Martinovic, I. (2017). STASH: Securing transparent authentication schemes using prover-side proximity verification. In *14th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*.

Karapanos, N., Marforio, C., Soriente, C., and Čapkun, S. (2015). Sound-proof: usable two-factor authentication based on ambient sound. *Proceedings of the 24th USENIX Conference on Security Symposium (SEC '15)*, pages 483–498.

Ki, Y. K. and Baik, D. K. (2006). Model for accurate speed measurement using double-loop detectors. *IEEE Transactions on Vehicular Technology*, 55(4):1094–1101.

Ma, L., Kaneko, K., Sharma, S., and Sakurai, K. (2019). Reliable decentralized oracle with mechanisms for verification and disputation. *Proceedings - 2019 7th International Symposium on Computing and Networking Workshops, CANDARW 2019*, pages 346–352.

Mammadzada, K., Iqbal, M., Payman Milani, F., García-Bañuelos, L., and Matulevičius, R. (2020). Blockchain Oracles: A Framework for Blockchain-Based Applications (SLR Protocol and Results).

Mauw, S. and Piramuthu, S. (2013). A PUF-based authentication protocol to address ticket-switching of RFID-tagged items. *Lecture Notes in Computer Science, 8th International Workshop on Security and Trust Management*, 7783:209–224.

Melo Jr., W. S., Bessani, A., Neves, N., Santin, A. O., and Carmo, L. F. R. C. (2019). Using Blockchains to Implement Distributed Measuring Systems. *IEEE Transactions on Instrumentation and Measurement*, 68(5):1503–1512.

Melo Jr., W. S., Machado, R. C. S., and Carmo, L. F. (2018). Using Physical Context-Based Authentication against External Attacks: Models and Protocols. *Security and Communication Networks*, 2018:1–15.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at https://bitcoin.org/bitcoin.pdf.

Rostami, M., Juels, A., and Koushanfar, F. (2013). Heart-to-Heart (H2H): Authentication for Implanted Medical Devices. *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13*, pages 1099–1112.

Sousa, J., Bessani, A., and Vukolić, M. (2018). A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform. In *DSN'18: The IEEE/IFIP International Conference on Dependable Systems and Networks*.

Vukolić, M. (2016). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9591:112–125.

WELMEC (2015). European Cooperation in Legal Metrology - WELMEC 7.2, 2015: Software Guide.

Zhang, F., Cecchetti, E., Croman, K., Juels, A., and Shi, E. (2016). Town Crier: An authenticated data feed for smart contracts. In *23rd ACM Conference on Computer and Communications Security, CCS 2016*, pages 270–282.

Zheng, Z., Xie, S., Dai, H.-N., and Wang, H. (2017). Blockchain Challenges and Opportunities : A Survey. *International Journal of Web and Grid Services*, pages 1–24.