Gerência de Autenticação de Dispositivos IoT Adaptativa Aos Ambientes Urbanos Apoiada em Políticas e Confiança Social

Yan Uehara de Moraes[1], **Carlos Pedroso**[1], **José Marcos Nogueira**[2], **Aldri Santos**[1,2]

[1]Núcleo de Redes Sem-Fio e Redes Avançadas (NR2) – UFPR

[2]Depto. de Ciência da Computação – Universidade Federal de Minas Gerais (UFMG)

{yumoraes,capjunior}@inf.ufpr.br {jmarcos,aldri}@dcc.ufmg.br

Abstract. *Devices' authentication is one of the key requirements to provide security in IoT environments. However, current Adaptative Authentication Systems (AAS) employ adaptation factors in an isolated way and ignore the correlation between them, as well as the relations that the devices build in the contexts where they are located. Those AASs show themselves as rigid about the most compatible mechanisms in one given context and do not provide multi-factor adaptation. This work proposes GALENA as an adaptive authentication management system in IoT networks, based on social trust strategies, devices' context, and policies. The GALENA evaluation showed its efficiency in adapting and selecting the authentication mechanism appropriated for each interaction, achieving a compatibility rate of about 97% with 200 devices and 98% with 400 devices in all scenarios, with maximum trust accuracy of 0,45 and 0,38 respectively.*

Resumo. *A autenticação de dispositivos é um dos requisitos-chave à segurança dos ambientes IoT. Entretanto, os atuais Sistemas de Autenticação Adaptativa (SAAs) empregam fatores de adaptação de forma isolada e ignoram a correlação entre os fatores, bem como as relações constituídas pelos dispositivos nos ambientes onde eles estão inseridos. Assim, esses SAAs mostram-se ainda rígidos quanto aos mecanismos mais compatíveis num dado ambiente, e não provendo uma adaptação multi-fatorial. Este trabalho propõe o sistema GALENA para o gerenciamento adaptativo da autenticação de dispositivos nas redes IoT, apoiado em estratégias de confiança social, no ambiente de inserção e uso de políticas. Uma avaliação por simulação do GALENA no NS3 mostrou a sua eficiência na adaptação e seleção do mecanismo de autenticação adequado a cada interação, tendo uma taxa de compatibilidade de cerca de 97% com 200 dispositivos e de 98% com 400 dispositivos, em todos os cenários analisados, com acurácia máxima da confiança de 0,45 e 0,38, respectivamente.*

1. Introdução

A Internet das Coisas (IoT) está inserida nos mais variados ambientes humanos e urbanos, colaborando em diversos domínios de aplicação, a fim de aumentar a qualidade de vida de seus habitantes [Qin et al. 2020]. Para atender aos objetivos desses domínios, os dispositivos IoT trocam mensagens e disseminam informações pela rede, ações que devem ocorrer de modo seguro, visto que muitos dos dispositivos IoT estão inseridos em contextos que podem trazer risco à vida, como no ambiente de *Smart Healthcare*. Apesar

dos requisitos de segurança, como confidencialidade, integridade e autenticação diferenciarem de um ambiente para outro, a autenticação dos dispositivos é um dos requisitos chave da IoT para evitar que ações maliciosas interfiram na rede, e portanto tragam os mais diversos danos aos usuários [de Oliveira et al. 2022].

A mobilidade dos dispositivos IoT impõe restrições quanto a localização, entrada e saída de dispositivos e mudanças de ambientes, dificultando que métodos tradicionais de autenticação atuem adaptativamente nas redes IoT [El-hajj et al. 2019]. Além disso, em razões de limitações de processamento, energia e armazenamento, os dispositivos normalmente possuem restrições para empregar mecanismos de autenticação clássicos. Logo, o modo de autenticação dos dispositivos também deve levar em conta a sua inserção no ambiente a fim de ser modificado conforme eles transitam [Arias-Cabarcos et al. 2019]. Embora os Sistemas de Autenticação Adaptativa (SAAs) existentes selecionem o mecanismo cabível para um determinado ambiente ao levar em conta os aspectos mencionados, eles têm utilizado fatores de adaptação, como ambiente, risco e comportamento, de maneira isolada e não consideram a correlação entre esses fatores para a decisão do mecanismo de autenticação a ser empregado [Arias-Cabarcos et al. 2019, Patwary et al. 2020].

Os SAAs de IoT que consideram o contexto (ambiente) como fator de adaptação simplesmente alteram o mecanismo de autenticação à medida que o dispositivo se move entre ambientes [Aman and Snekkenes 2015]. E há aqueles que exploram a percepção sobre o risco como fator de adaptação, ao detectar mudanças do risco derivado da localização, do tráfego de rede e de mensagens trocadas pelo dispositivo [Sylla et al. 2020]. Logo, em ambientes de risco baixo (ou ambientes seguros) pode não ser necessária a adaptação, enquanto que em ambientes de alto risco (ou inseguros) a necessária adaptação pode demandar um mecanismo de autenticação mais custoso computacionalmente. Contudo, os SAAs ainda não exploram os benefícios das relações sociais constituídas entre os dispositivos à medida que eles percorrem diferentes partes da rede, o que acontece em ambientes abrangentes das cidades inteligentes, como, por exemplo, a vizinhança inteligente visando a tomada de serviços associados ao bem-estar e a mobilidade das pessoas.

As técnicas de adaptação normalmente aplicadas pelos SAAs em IoT compreendem o aprendizado de máquina (ML), a teoria dos jogos e uso de políticas. As estratégias de ML primeiramente determinam o comportamento padrão do dispositivo para depois detectar desvios do padrão, e assim adaptarem os mecanismos de autenticação empregados. Elas, no entanto, mostram-se inadequadas à IoT porque necessitam de poder de processamento e energia, nem sempre disponíveis [Gebrie and Abie 2017]. Já os sistemas que empregam Teoria dos Jogos modelam a mudança dos fatores como um problema matemático cuja solução indica o mecanismo de autenticação a ser empregado [Assis et al. 2017, Hamdi and Abie 2014]. Apesar dos SAAs baseados em políticas colaborarem para um gerenciamento adaptativo de sistemas por serem mais simples e facilmente configuráveis [Huertas Celdrán et al. 2019], as políticas são usualmente aplicadas de maneira centralizada, e isso impede uma operação autônoma de um grupo não correlacionado de dispositivos. Ademais, esses SAAs não escalam à medida que os dispositivos cruzam diversos ambientes, visto que a entidade centralizadora é a detentora das políticas para todos os dispositivos da rede [Sylla et al. 2020].

Este trabalho propõe um sistema para a gerência adaptativa sobre os mecanismos de autenticação de dispositivos IoT aplicados a diversos ambientes, apoiado em confi-

ança social e políticas de configuração de segurança. O sistema, chamado GALENA (*mana**G**ement of **A**daptive authentication based on po**L**ici**E**s a**N**d soci**A**l trust*), determina o mecanismo de autenticação mais adequado para realizar o procedimento de autenticação entre os dispositivos IoT. Ele emprega três fatores de confiança social, SOR, $C-LOR$ e $C-WOR$, calculados a partir da sociabilidade estabelecida entre os dispositivos, para guiar a configuração dos mecanismos de segurança aplicados na autenticação. As políticas de configuração estabelecidas determinam o mecanismo de autenticação a ser empregado em um dispositivo de acordo com a confiança social percebida e o ambiente. Simulações no NS3 avaliaram o desempenho do GALENA a partir de comportamentos realísticos a fim de analisar a sua efetividade em selecionar os melhores mecanismos. Os resultados mostram que o GALENA configurou o mecanismo de autenticação compatível em cerca de 97% das interações em cenários com 200 dispositivos e 98% das interações com 400 dispositivos, com acurácia da confiança em 0,45 e 0,38 respectivamente.

O restante do artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados. A Seção 3 descreve os modelos das infraestruturas de redes IoT e a arquitetura do sistema GALENA proposto com seus algoritmos. A Seção 4 detalha a avaliação e os resultados obtidos. A Seção 5 apresenta a conclusão e os trabalhos futuros.

2. Trabalhos Relacionados

Embora a literatura possua trabalhos de autenticação adaptativa em IoT envolvendo diferentes técnicas, tais como Aprendizado de Máquina [Gebrie and Abie 2017, Hayashi et al. 2013], Teoria dos Jogos [Assis et al. 2017, Hamdi and Abie 2014], Políticas [Sylla et al. 2020], eles possuem limitações arquiteturais, sendo muitas delas centralizadas. Além disso, normalmente elas ignoram fatores presentes nos ambientes onde atuam, como a percepção social, largamente empregada em redes IoT [Chen et al. 2018, Jafarian et al. 2020] para a seleção e a composição de serviços.

Em [Gebrie and Abie 2017], os autores propõem um SAA baseado em ML e na percepção de risco como um fator de adaptação. Esse SAA trata da autenticação do dispositivo ao *gateway*, onde ocorre a avaliação devido à sua capacidade computacional para lidar com a tarefa de ML. Ele treina o classificador *Naive-Bayes* com os padrões de uso do usuário e dos dispositivos, classificando as atividades como *normais*, *suspeitas*, *anormais* e *críticas*. À medida que o comportamento desvia do normal e o risco aumenta, o SAA exige que o usuário ou dispositivo aplique um método de autenticação mais complexo e/ou diferente. Entretanto, ele desconsidera a autenticação par-a-par de maneira distribuída entre os dispositivos, ignora as capacidades dos dispositivos e a percepção do ambiente como fatores de adaptação. Em [Hayashi et al. 2013], os autores propõem o sistema CASA (*Context-Aware Scalable Authentication*) que usa três fatores passivos dos dispositivos do usuário, localização, características comportamentais e proximidade com outros dispositivos, a fim de modular o mecanismo de autenticação no contexto de proximidade com outros dispositivos. Um classificador *Naive-Bayes* escolhe entre a senha e a impressão digital do usuário como fator ativo com base no risco calculado. O CASA, porém, exige um pré-treinamento das amostras, o que para redes com dispositivos móveis é inadequado devido ao tempo de resposta e a um custo computacional elevado.

Em [Assis et al. 2017], os autores empregaram a teoria dos jogos para mitigar ataques DDoS em redes SDN. O módulo de mitigação baseado em teoria dos jogos recebe

o comportamento esperado e as conexões suspeitas da rede que são aglutinadas com as possíveis contramedidas. Essas informações são modeladas matematicamente e emprega-se o equilíbrio de Nash para determinar a contramedida recomendada, de tal forma que o controlador SDN ou o *firewall* de rede possa aplicá-la. Visto que a arquitetura é centralizada (devido à arquitetura SDN), esse sistema mostra-se inadequado a um cenário com dispositivos IoT autônomos e com múltiplos proprietários. Em [Hamdi and Abie 2014], os autores apresentaram um SAA baseado na teoria do jogos que considera a quantidade de energia e de memória, bem como o padrão de comunicação para modelar o comportamento do dispositivo. A intrusão é representada por um modelo matemático de como ela se propaga pela rede através da comunicação entre nós comprometidos e sadios, bem como a velocidade com que os nós se recuperam. O SAA emprega o equilíbrio de Nash para maximizar a segurança tanto quanto o gasto energético permitir para estender a vida dos dispositivos. Entretanto, essa solução se aplicaria apenas a dispositivos IoT sobre a mesma administração/propriedade, impedindo a operação autônoma em vários ambientes.

Em [Sylla et al. 2020], os autores propõem um SAA baseado em políticas para as redes SDN-IoT a fim de oferecer segurança ciente do contexto. Este SAA avalia o risco associado de cada contexto baseado no modelo de atacante existente no ambiente e seleciona as políticas conforme o nível de segurança estabelecido e as envia ao agente para ser aplicada. Entretanto, além de ser centralizado, ele depende de uma fase de pré-registro e emprega chaves simétricas na sua comunicação com os dispositivos, dificultando uma operação autônoma da autenticação dos dispositivos em qualquer ambiente. Além disso, considera apenas o contexto onde o dispositivo se encontra como o fator de adaptação. Em [Aman and Snekkenes 2015], os autores propõem o sistema EDAS (*Autonomic Event-Driven Adaptive Security*) que adapta o modo de autenticação dos dispositivos supervisionados ao levar em conta o risco derivado de eventos reportados por eles. O EDAS emprega políticas associadas às preferências do usuário, capacidades dos dispositivos e métricas de segurança. Assim, ao receber uma métrica de risco associada a um evento, ele analisa as suas políticas a fim de adaptar-se aos riscos percebidos. Todavia, devido à sua centralidade, em ambientes densos ele enfrenta problemas de escalabilidade por exigir o armazenamento das politicas da rede num único local.

A confiança social entre os dispositivos, por sua vez, tem sido aplicada na seleção e na composição de serviços em redes IoT. Em [Chen et al. 2018], desenvolveu-se um sistema de gerência de confiança a partir da Amizade, Comunidades de Interesse e do Contato Social, como um serviço em rede chamado de TaaS (***T**rust **A**s **A** **S**ervice*). O TaaS opera na nuvem e armazena dados sobre a reputação dos dispositivos. Ele emprega a confiança social para avaliar a reputação dos dispositivos, além de compor e solicitar serviços desses dispositivos. A confiança social permite ao dispositivo determinar o prestador de serviço mais confiável dentro da rede; por exemplo, o serviço sobre a qualidade do ar em regiões da cidade. No entanto, o TaaS, além de ser centralizado, não permite uma operação autônoma. Em [Jafarian et al. 2020], os autores propuseram o sistema DATM (***D**iscrimination-**A**ware **T**rust **M**anagement*), que emprega confiança social baseada no contexto para a seleção de serviços. Eles empregam as relações de Comunidades de Interesse para compartimentalizar o comportamento do dispositivo e compará-lo em ambientes de *Smart City*. O DATM não permite operação autônoma e depende de um provedor central para armazenar os valores de confiança. O uso de amostras aleatórias do *dataset* de avaliação compromete a análise de funcionamento em múltiplos ambientes.

3. O sistema GALENA

Esta seção apresenta o sistema GALENA (*mana**G**ement of **A**daptive authentication based on po**L**ici**E**s a**N**d soci**A**l trust*) para o gerenciamento adaptativo da autenticação de dispositivos em redes IoT, apoiado em estratégias de confiança social, no ambiente de inserção e uso de políticas; a arquitetura do sistema e seus componentes são detalhados. É também apresentada uma visão geral do modelo dos ambientes da rede IoT, da comunicação e do comportamento social dos dispositivos pressuposto pelo GALENA.

3.1. Ambientes de Redes IoT Urbanas

Numa visão geral, os vários ambientes urbanos de uma cidade compõem uma infraestrutura de rede IoT na qual os dispositivos atuam e estabelecem comunicação entre si. Além do mais, os modelos de comportamento social exibidos pelos dispositivos IoT determinam como são construídas as relações sociais entre eles. A Figura 1 ilustra a representação de uma rede IoT com múltiplos domínios de aplicação, e que apresentam diferentes relações sociais entre os dispositivos.

Modelo físico da rede: a rede IoT é composta por um conjunto de dispositivos IoT identificados por $D = \{d_1, d_2, d_3, ..., d_n\}$, onde $d_n \in D$. Cada dispositivo d_n possui um identificador (Id) único e oferta e demanda um subconjunto de serviços $s \subseteq S = \{s_1, s_2, s_3, ..., s_i\}$ entre eles de maneira autônoma. Os dispositivos suportam um subconjunto dos mecanismos de autenticação $M = \{m_1, m_2, m_3, ..., m_k\}$ a ser aplicado de acordo com a sua capacidade de comunicação e processamento. Assim, um perfil $P_i^{m_k}$ corresponde as configurações específicas de um mecanismo (m_k) de autenticação agrupando sequencialmente suas opções disponíveis (i).

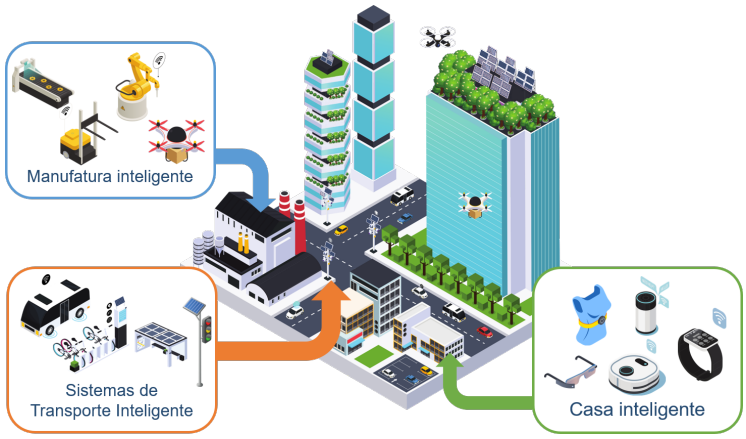

Figura 1. Representação das Rede IoT com múltiplos domínios de aplicação

Modelo de comunicação: a comunicação entre os dispositivos ocorre através de um meio sem fio em um canal assíncrono e compartilhado. Os dispositivos trocam mensagens utilizando o protocolo 6LoWPAN sobre o padrão IEEE 802.15.4 ou o padrão Wi-Fi, protocolos adequados para interligar entre si os dispositivos com restrição e com a Internet convencional para formar a IoT [Morabito and Jimenez 2020]. Além disso, a comunicação está sujeita a perdas de pacotes devido à mobilidade dos dispositivos e o raio de transmissão considera a dimensão do ambiente onde os dispositivos estão inseridos.

Modelo de mensagens: compreende cinco tipos de mensagens trocadas entre os dispositivos: mensagens *Beacon* para anúncio de presença; *ServiceInquiry* e *ServiceAnswer*

para descoberta de serviços e dos mecanismos de autenticação suportados; *TrustRequest* e *TrustAnswer* para troca de valores de confiança social; e *ServiceExchange* no estabelecimento do mecanismo de autenticação a ser aplicado pelos dispositivos.

Comportamento social: os dispositivos possuem capacidade para estabelecerem autonomamente três comportamentos sociais do paradigma da Internet das Coisas Sociais (SIoT): *Social object relationship* (SOR), *Co-location object relationship* (C-LOR), e *Co-work object relationship* (C-WOR), este último caracterizando os relacionamentos comuns aos ambientes urbano da rede. O SOR é o atributo mais comum e os dispositivos o estabelecem quando entram em contato entre si, de maneira esporádica ou contínua. A C-LOR ocorre entre os dispositivos no mesmo ambiente (contexto), provendo ou não um mesmo serviço. Os dispositivos estabelecem a relação C-WOR quando se encontram no mesmo contexto e colaboram para prover um serviço em comum [Marche et al. 2018].

3.2. A Arquitetura

A arquitetura do sistema GALENA compreende os módulos Gerência de Descoberta (**SDM**) e Gerência de Autenticação (**SGAUTH**). O **SDM** reúne os serviços relacionados a descoberta de dispositivos e disseminação de informações; o **SGAUTH** reúne os serviços de interação social, de políticas e de gerenciamento de adaptação do mecanismo de autenticação. A Figura 2 ilustra um ambiente urbano IoT e apresenta a arquitetura e os componentes do GALENA. Ambos os módulos apoiam-se num serviço de localização (**SLOC**) que provê o posicionamento e o contexto dos dispositivos IoT. Ele determina o contexto do dispositivo utilizando, por exemplo, sistemas GNSS (Global Navigation Satellite System), triangulação, trilateração, e outros meios. O contexto pode também ser definido de forma semântica, automaticamente por de serviços de localização online ou manualmente pela interação com o usuário. Desta forma, O SLOC consegue identificar e gerar contextos semânticos, como “trabalho” ou “escola”, e repassá-los ao GALENA e a outros sistemas.

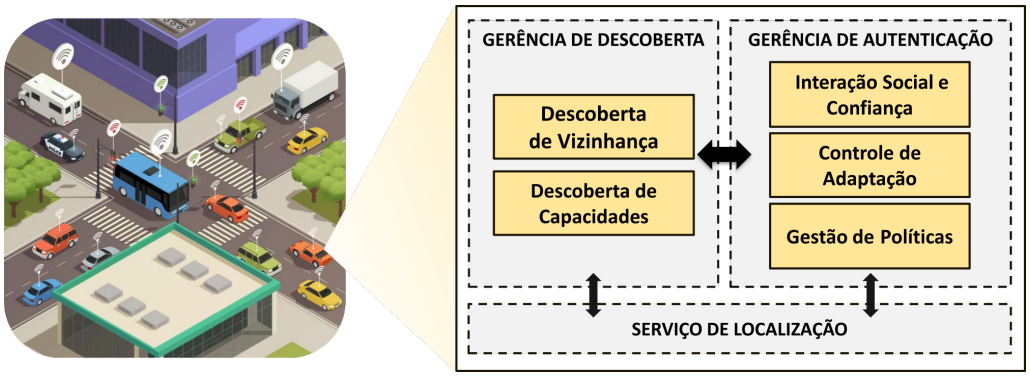

Figura 2. Ambiente IoT e componentes do sistema GALENA

O módulo Gerência de Descoberta (**SDM**) controla a descoberta de dispositivos vizinhos e mapeia a conexão entre ambientes, serviços e dispositivos. O SDM compõe-se do serviço de Descoberta de Vizinhança (SDES) e do serviço de Descoberta de Capacidade (SDCAP). O SDES anuncia a presença do dispositivo em intervalos periódicos configuráveis e também recebe anúncios da presença de dispositivos próximos. O SDCAP recebe e responde as solicitações em relação aos serviços oferecidos e os mecanismos de autenticação suportados. O Algoritmo 1 descreve como o SDM anuncia a

presença do dispositivo e como ele descobre as capacidades de autenticação dos vizinhos. Periodicamente, os dispositivos, através do procedimento `AnnouncePresence` (*l*.1-*l*.7), anunciam sua presença aos outros dispositivos a fim de manter atualizadas as informações sobre a sua vizinhança. Ao receber um anúncio, o receptor registra o dispositivo emissor como seu vizinho no ambiente onde eles estão inseridos (procedimento `ReceiveAnnounce` (*l*.8-*l*.12)). Em seguida, o serviço de descoberta de capacidades (SDCAP) requisita informações aos dispositivos vizinhos sobre os mecanismos de autenticação suportados por eles e os serviços ofertados, e atualiza essas informações na sua lista de vizinhos, procedimento `RequireCapabilities` (*l*.1-*l*.3) do Algoritmo 2. Por sua vez, os dispositivos disseminam suas capacidades de autenticação e serviços através do procedimento `AnswerCapabilitiesRequest` (*l*.4-*l*.6). Além disso, periodicamente, SDES e SDCAP refazem as suas listas de vizinhos para evitar inconsistência de informação sobre os ambientes recentemente frequentados pelos dispositivos (procedimento `PeriodicSDESCleanUp` (*l*.13-*l*.15) do Algoritmo 1) e sobre os serviços atualmente suportados pelos dispositivos (procedimento `PeriodicSDCAPCleanUp` (*l*.7-*l*.9) do Algoritmo 2).

Algoritmo 1: Serviço de Descoberta de Vizinhança

```
1  procedure AnnouncePresence(MyId)
2      NeighborList ← 0
3      while True do
4          SendAnnounce(MyId)
5          WaitInterval (TimeInterval)    // Espera um intervalo de tempo para
             não ocupar o meio
6      end
7  end procedure
8  procedure ReceiveAnnounce()
9      NeighborId ← GetId()
10     NeighborList ← NeighborList ∪ NeighborId
11     RequireCapabilities(NeighborId)              // Interface com o SDCAP
12 end procedure
13 procedure PeriodicSDESCleanUp()
14     NeighborList ← 0
15 end procedure
```

Algoritmo 2: Serviço de Descoberta de Capacidades

```
1  procedure RequireCapabilities(NeighborId)
2      NeighborCapabilities[NeighborId] ← RequireNeighborCapabilities(NeighborId)
3  end procedure
4  procedure AnswerCapabilitiesRequest()
5      SendServicesAndAuthenticationMechanisms()
6  end procedure
7  procedure PeriodicSDCAPCleanUp()
8      NeighborCapabilitites ← 0
9  end procedure
```

O módulo **SGAUTH** estabelece as relações sociais com outros dispositivos IoT, gerencia e aplica as políticas de adaptação estabelecidas para o dispositivo, e controla a configuração da autenticação adaptativa. O SGAUTH compõe-se de: Serviço de Interação Social e Confiança (SISCO), que coleta e dissemina os dados sociais a respeito dos outros dispositivos; Serviço de Gestão de Políticas (SPOL), que gerencia as políticas

armazenadas no dispositivo; Serviço de Controle de Adaptação (SADPT) que aplica a política selecionada pelo SPOL e configura o mecanismo de autenticação derivado dela.

À medida que os dispositivos interagem uns com os outros, eles estabelecem as relações sociais descritas anteriormente, isto é, LOR, SOR e WOR. A relação WOR é calculada a partir da similaridade dos serviços ofertados. A LOR é calculada pela distância normalizada entre esses dispositivos; e eles estabelecem a relação SOR ao oferecerem serviços uns para os outros. O serviço SISCO calcula o valor da confiança social a parir da Equação 1, onde LOR e WOR correspondem aos valores dessas relações. Os valores de confiança variam entre 0 e 1 e os termos α, β, γ configuram uma restrição cuja soma deve se manter unitária.

$$\mathcal{ST}(Id) = \alpha * LOR_{Id} + \beta * WOR_{Id} + \gamma * SOR_{Id} \tag{1}$$

O SISCO computa o valor SOR a partir da Equação 2, que leva em conta as interações com sucesso (μ_{Id}) e o total de interações (τ_{Id}). O valor μ_{Id} representa a quantidade de serviços requisitados e atendidos. O termo $e^{-\lambda_d(t_{now}-t_{-1})}$ exprime o decaimento como uma função exponencial decrescente dependente do termo $-\lambda_d$, taxa de decaimento, e do termo $(t_{now} - t_{-1})$, a variação do tempo observada entre a última interação e a interação atual entre os dispositivos. O valor R_{Id} representa a média das recomendações de outros dispositivos, i.e. a confiança que eles têm, sobre o dispositivo com o qual se quer interagir. Desta forma, quando um dispositivo requisita o valor de confiança sobre um terceiro, a resposta do emissor pode ser um valor neutro, indicando que não há confiança preestabelecida sobre o terceiro, ou simplesmente nenhuma recomendação. Já o valor δ pondera entre a confiança direta, representada pelo primeiro termo da soma, e a confiança indireta (recomendação), representada pelo segundo termo.

$$SOR_{Id} = \delta * \left(\frac{\mu_{Id}}{\tau_{Id}}\right) * e^{-\lambda_d(t_{now}-t_{-1})} + (1-\delta) * R_{Id} \tag{2}$$

No GALENA, as políticas codificam as regras das formas de autenticação definidas previamente pelo usuário ou administrador do dispositivo. Assim, para determinar o mecanismo de autenticação a ser aplicado com um dispositivo na vizinhança em um dado ambiente, o SADPT reconhece o ambiente através do SLOC (*l*.2) e consulta o serviço SPOL para conhecer as políticas estabelecidas para aquele ambiente (*l*.3). Em seguida, ele obtém os valores de confiança do SISCO (*l*.5) e então executa essas políticas a fim de determinar o mecanismo a ser empregado no processo de autenticação do dispositivo, procedimentos `DecidePolicy` e `ApplyAuthMechanism` (*l*.6-*l*.7) do Algoritmo 3.

Algoritmo 3: Controle da Autenticação Adaptativa

```
1 procedure DecideAndApplyPolicy(NeighborId)
2     Context ← GetContext() ;                          // Interface com SLOC
3     Policies ← GetPolicies(Context) ;                 // Interface com SPOL
4     Capabilities ← NeighborCapabilities[NeighborId]   // Obtido pelo Alg. 2
5     Trust ← S(NeighborId) ;                           // Obtido pela Eq. 1
6     M ← DecidePolicy(NeighborId, Capabilities, Trust, Context, Policies)
7     ApplyAuthMechanism(M) ;   // Aplica o mecanismo de autenticação no
        dispositivo
8 end procedure
```

As políticas são denotadas como $\mathcal{P}_j : \langle Id, AuthCapabilities, \mathcal{ST}_{Id}, context\rangle = P_i^m$, onde os campos da tupla podem ser valores únicos, conjuntos ou funções específicas, ou ainda o símbolo * para denotar a opção *qualquer*. A função $\mathcal{F}(value)$ filtra o campo Id com o valor *value*. O conjunto $AuthCapabilities$ indica os mecanismos de autenticação suportados. O campo $\mathcal{ST}_{Id}$ utiliza comparadores matemáticos ($=$, $>$, $<$ e $!=$) para limitar os valores de confiança. Já a função $\mathcal{C}(value)$ restringe os valores do campo $context$ a $value$. Portanto, uma política $\mathcal{P}_j$ emprega o Id do dispositivo, os mecanismos de autenticação suportados, e o valor da confiança social, além do contexto, para determinar o perfil de autenticação a ser aplicado. Por exemplo, a notação de uma política que configura uma autenticação baseada em PUF and RSA seria da seguinte forma:

$$\mathcal{P}_1 : \langle \mathcal{F}(*), \{PUF, RSA\}, \mathcal{ST}_{Id} > 0,5, \mathcal{C}(\text{“}escola''\rangle = P_1^{RSA}$$

Essa política então seria aplicada a todos os dispositivos ($\mathcal{F}(*)$), com os mecanismos de autenticação PUF e RSA. No entanto, ela se aplicaria apenas no contexto *escola*. Ademais, ela exige que os dispositivos possuam um valor de confiança social ($\mathcal{ST}_{Id}$) maior do que *0,5*, e logo o uso de um perfil de autenticação que empregue RSA. Um exemplo do funcionamento do GALENA em uma rede IoT num ambiente urbano de vias públicas com Sistemas de Transporte Inteligente (STI) e de Iluminação Pública Inteligente (IPI) é descrito em detalhes em um trabalho dos autores[1].

4. Avaliação

Esta seção descreve uma avaliação do desempenho do GALENA na gestão adaptativa dos mecanismos de autenticação de dispositivos IoT de acordo com o ambiente e suas relações sociais. Implementou-se o GALENA[2] no simulador NS3, versão 3.29. As simulações levam em conta o ambiente de um centro urbano de uma cidade, sendo a rede IoT composta de dispositivos smartphones portados por seus donos. Os dispositivos oferecem o conjunto de serviços: *Localização, Data e horário, Presença, Ambiente, Consumo de Energia e Movimento* provenientes do dataset de [Marche et al. 2018], voltado especialmente para simulações de redes de Internet das Coisas Sociais (SIoT). Além disso, esses dispositivos suportam os seguintes mecanismos de autenticação: RSA, ECC, autenticação simétrica (identificado por SIM) e sem senha (NOPASS). Não houve uma comparação com outras estratégias, pois o trabalho mais próximo, de [Chen et al. 2018], que considera as relações de Amizade (friendship) e as Comunidades de Interesse (CoI), apresenta relações que dependem de características do proprietário do dispositivo, as quais não foram tratadas neste trabalho, visto que essas relações não são construídas autonomamente.

Os dois cenários avaliados contêm 200 e 400 dispositivos que se aleatoriamente durante 360s dentro de um espaço urbano de *1,6km x 1,6km* correspondente a uma subárea dos traços do dataset de [Marche et al. 2018]. A comunicação entre os dispositivos ocorre empregando o protocolo UDP sobre IPv6, sendo estabelecida uma rede *ad-hoc* no padrão IEEE 802.11 (WiFi). Os cenários diferenciam-se pela configuração dos pesos das recomendações (δ na Equação 2) que variam entre $0,5$, $0,2$ e $0,8$ e pelos valores de α, β e γ da Equação 1, que variam entre $0,2$, $0,3$ e $0,5$, perfazendo 21 combinações no total. No Cenário 1, os dispositivos interagiram 3.932 vezes e, no Cenário 2, 11.542 vezes. Cada configuração foi simulada apenas uma vez, dado a constância dos valores devido

[1] `https://yanuehara.dev/project/galena/func-STI-IPI.pdf`

[2] Disponível em `https://github.com/yanuehara/galena/`

ao uso de semente (*seed*) fixa de simulação, portanto levando a uma estacionariedade das métricas agregadas.

Para todas as simulações, configurou-se nos dispositivos as três políticas:

$$\mathcal{P}_1 : \langle \mathcal{F}(*), \{ECC, RSA, SIM, NOPASS\}, \mathcal{ST}(Id) > 0,5 \,\&\mathcal{ST}(Id) < 0,9, \mathcal{C}(*) \rangle = P_1^{ECC}$$
$$\mathcal{P}_2 : \langle \mathcal{F}(*), \{ECC, RSA, SIM, NOPASS\}, \mathcal{ST}(Id) > 0,0 \,\&\mathcal{ST}(Id) < 0,5, \mathcal{C}(*) \rangle = P_1^{RSA}$$
$$\mathcal{P}_3 : \langle \mathcal{F}(*), \{ECC, RSA, SIM, NOPASS\}, \mathcal{ST}(Id) > 0,9, \mathcal{C}(*) \rangle = P_1^{NOPASS}$$

Na avaliação do GALENA empregaram-se as seguinte métricas: **Evolução da Confiança** (EC) – baseado em [Chen et al. 2018], **Acurácia da Confiança** (AC) – obtida a partir de [Tan et al. 2016], **Taxa de Aplicação de Políticas** (TAP) e **Taxa de Compatibilidade de Autenticação** (TCA) – baseadas em [Gwak et al. 2018].

Tabela 1. Métricas de avaliação de desempenho

Descrição	Equação
Evolução da Confiança (EC): mensura a média da confiança de todos dispositivos a cada momento da operação da rede, onde t representa o momento do tempo, $C_{i,j}^t$ indica a confiança de i para j no instante t, e N o total de dispositivos.	$EC^t = \frac{\sum_{i,j} C_{i,j}^t}{\lvert N \rvert}$
Acurácia da Confiança (AC): mensura a diferença entre a média da confiança calculada em relação ao dispositivo i e a média das recomendações sobre ele, em que C_i indica a média de confiança em relação ao dispositivo i, R_i representa todas as recomendações a respeito de i, e N_i a quantidade de dispositivos que recomendaram i.	$AC = \frac{\sum_1^N C_i - \frac{R_i}{\lvert N_i \rvert}}{\lvert N \rvert}$
Taxa de Aplicação de Políticas (TAP): mensura a percentagem de vezes que uma política $\mathcal{P}_j$ foi aplicada na rede, onde int representa o total de interações e $int_{\mathcal{P}_j}$ o número de vezes da aplicação da politica.	$TAP = \frac{int}{int_{\mathcal{P}_j}}$
Taxa de Compatibilidade de Autenticação (TCA): mensura a quantidade de interações nas quais dois dispositivos na rede concordaram sobre o mecanismo de autenticação a ser utilizado, onde $I_{i,j}$ representa um valor binário em que 1 significa uma interação com sucesso entre i e j e 0 uma interação sem acordo, T representa o tempo total de simulação, e int representa o total de interações.	$TCA = \frac{\sum_0^T \sum_{i,j} I_{i,j}}{\lvert int \rvert}$

4.1. Análise da Eficiência e da Adaptação

A Evolução da Confiança (EC) para as várias combinações de pesos dos parâmetros α, β, γ e δ no Cenário 1 (200 dispositivos) pode ser vista nos gráficos Figura 3. Cada linha de um gráfico representa uma combinação específica dos parâmetros α, β, γ, como indicado à esquerda; cada coluna representa um dos valores possíveis de δ. Nesse cenário, a confiança indireta (Recomendações) manteve-se, com poucas variações, em torno de $0,5$ em todas as configurações e durante toda a simulação. Isso deve-se porque a simulação conta com poucos dispositivos em um grande espaço. Assim, como não existe recomendação a ser enviada devido a baixa interação, o GALENA assume o valor $0,5$ como recomendação neutra nessas situações.

O comportamento do SOR em todos os gráficos mostrou-se característico, isto é, para configurações com γ médio ou alto, percebe-se que o valor do δ influencia o SOR, com a curva deste último atingindo valores maiores à medida que os gráficos são visualizados da esquerda para direita. Porém, para algumas configurações, o SOR mantém-se

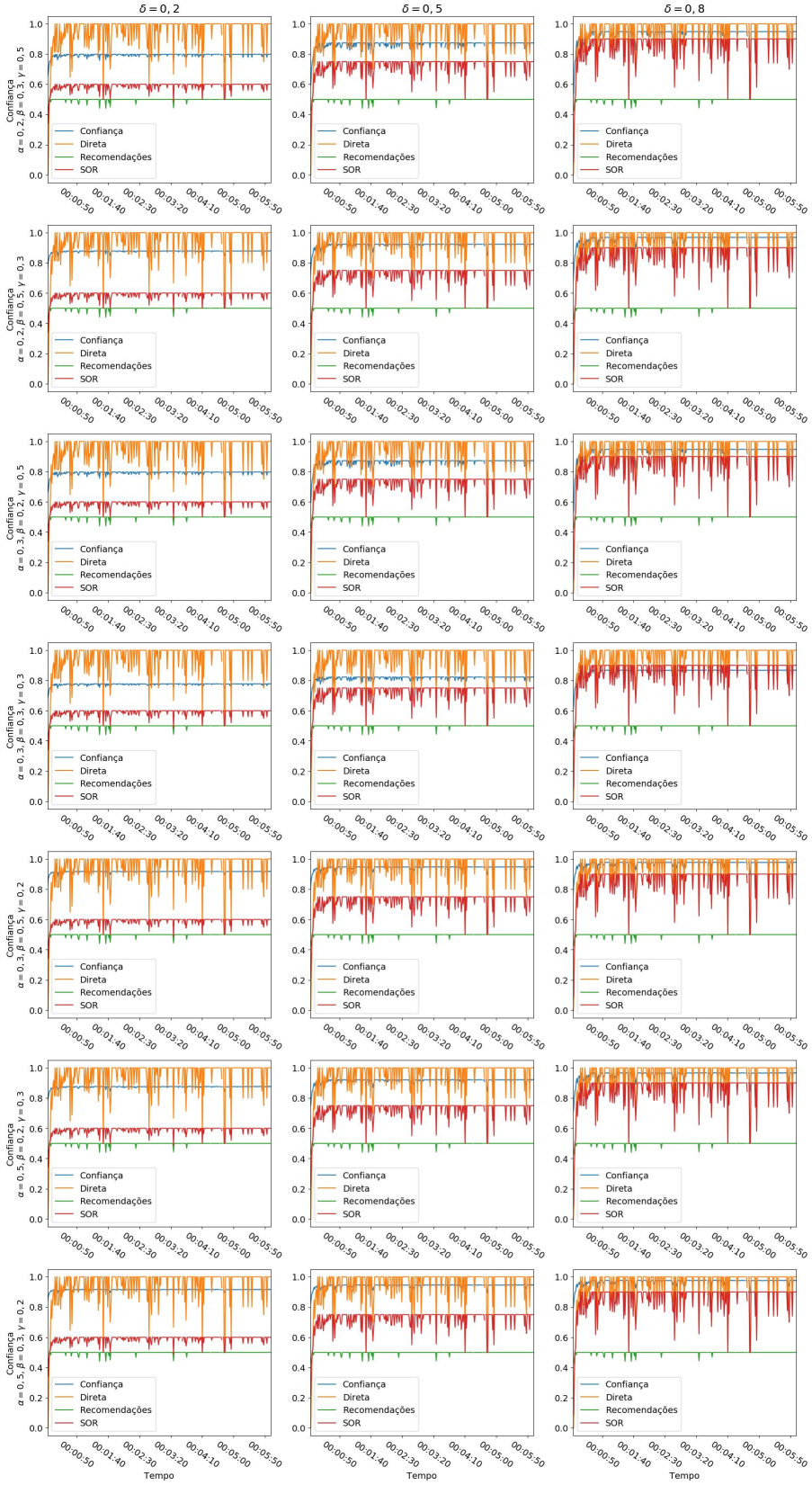

Figura 3. Evolução da Confiança (EC) - Cenário 1

praticamente estável por causa do baixo valor de γ. Assim, a confiança direta influencia pouco no SOR e seu comportamento não muda entre uma simulação e outra. Neste Cenário 1, percebe-se que a confiança restringe-se ao intervalo entre $0,8$ e $1,0$, devido ao modo como o GALENA compõe a confiança; ou seja, além do SOR, ele utiliza o LOR, com valores perto de 1, e o WOR, com valor igual a 1 porque os dispositivos são homogêneos. Assim, espera-se que a confiança não exceda 1 e atinja valores altos. Por razões de espaço não foram incluídos aqui o gráfico e a análise da EC no Cenário 2[3].

Apesar da Evolução da Confiança (EC) oferecer um panorama da confiança durante a simulação, a métrica Acurácia da Confiança (AC) nos permite analisar a qualidade dessa confiança, sumarizada na Tabela 2. No Cenário 1, percebe-se que a confiança apresenta valores de AC entre $0,27$ e $0,45$. Como as recomendações concentraram-se perto do valor $0,5$, a AC demonstra que a confiança distanciou-se do valor das recomendações. No Cenário 2 os valores de AC mantiveram-se entre $0,27$ e $0,38$, mostrando que a confiança também distanciou-se das recomendações. Ao contrário da conjectura de [Tan et al. 2016], nos dois cenários o distanciamento mostra-se benéfico, pois as recomendações foram neutras em sua maioria, e, portanto, a confiança exibida traduz as relações sociais criadas entre os dispositivos.

As taxas de aplicação de políticas (TAP) e de compatibilidade de autenticação (TCA) indicam a influência da variação da confiança na aplicação de políticas e na seleção do mecanismo de autenticação. No Cenário 1, o GALENA decidiu pela aplicação da política $\mathcal{P}_3$ em 12 das 21 combinações com TAPs em torno de 91%. A $\mathcal{P}_2$ foi aplicada apenas em seis combinações, com uma TAP de somente 0,07% do total de interações. A política $\mathcal{P}_1$ foi aplicada em todas as combinações com TAPs entre 4,7% (quando a $\mathcal{P}_3$ foi a mais aplicada) a 99,4% das interações nas combinações. Com baixa densidade de dispositivos (menos interações), a TCA atingiu valores entre 96% e 99%, mostrando que o GALENA conseguiu negociar autonomamente um mecanismo de autenticação adequado a um nível de confiança social do dispositivo num dado momento. Os valores de TAP e TCA encontram-se sumarizados na Tabela 3. No Cenário 2, em 17 das 21 combinações foi aplicada unicamente a política $\mathcal{P}_1$, mas em 12 deles foram aplicadas conjuntamente as políticas $\mathcal{P}_2$ e $\mathcal{P}_3$, indicando que o GALENA é capaz de alterar a política a medida que altera-se a confiança. Nas simulações em que somente $\mathcal{P}_1$ foi empregada, ela atingiu uma TAP e uma TCA de 99%. Nas simulações em que $\mathcal{P}_1$ e $\mathcal{P}_2$ foram aplicadas, $TAP_{\mathcal{P}_1} \approx 98{,}70\%$ e $TAP_{\mathcal{P}_2} = 0{,}01\%$. Por fim, nas simulações em que todas as políticas foram aplicadas, $TAP_{\mathcal{P}_1} \approx 4\%$ e $TAP_{\mathcal{P}_2}$

Pesos Par. Sociais				Cenários	
α	β	γ	δ	**1**	**2**
2	3	5	2	0,28	0,28
2	3	5	5	0,33	0,33
2	3	5	8	0,38	0,38
2	5	3	2	0,37	0,37
2	5	3	5	0,40	0,40
2	5	3	8	0,43	0,43
3	2	5	2	0,28	0,28
3	2	5	5	0,33	0,33
3	2	5	8	0,38	**0,38**
3	3	3	2	**0,27**	**0,27**
3	3	3	5	0,30	0,30
3	3	3	8	0,33	0,33
3	5	2	2	0,41	0,28
3	5	2	5	0,43	0,33
3	5	2	8	**0,45**	**0,38**
5	2	3	2	0,37	0,28
5	2	3	5	0,40	0,33
5	2	3	8	0,43	**0,38**
5	3	2	2	0,41	0,28
5	3	2	5	0,43	0,33
5	3	2	8	**0,45**	**0,38**

Tabela 2. Acurácia da Confiança

[3]Disponíveis em: `https://yanuehara.dev/project/galena/EC-cenario2.pdf`

= 0,01% e $TAP_{\mathcal{P}_3}$ = 88,90%. Para o Cenário 2, em todas as simulações, o GALENA atingiu uma TCA acima de 93%, chegando a 99% em algumas combinações. Os valores de TAP e de TCA para o Cenário 2 estão sumarizados na Tabela 4. Nos dois cenários, em todas as combinações, a política $\mathcal{P}_2$ apresentou um TAP baixo devido a sua definição e o comportamento da Confiança na simulação. O GALENA emprega essa política quando a confiança é menor do que $0,5$, o que ocorre somente nos primeiros momentos da simulação, de acordo com o gráfico da Figura 3 e o gráfico do Cenário 2[3]. Ainda, o gráfico do Cenário 2 também mostra que a confiança ficou abaixo de $0,9$, que é o valor de confiança definido para aplicação da política $\mathcal{P}_3$. Esses comportamentos demonstram a capacidade do GALENA na adaptação do mecanismo de autenticação empregado pelo dispositivo.

Pesos Sociais				Tx. Ap. de Políticas (TAP)			TCA
α	β	γ	δ	$\mathcal{P}_1$	$\mathcal{P}_2$	$\mathcal{P}_3$	
2	3	5	2	99,00%	0,07%	00,00%	99,10%
2	3	5	5	99,00%	0,07%	00,00%	99,10%
2	3	5	8	04,30%	0,07%	91,60%	96,00%
2	5	3	2	99,40%	0,00%	00,00%	99,40%
2	5	3	5	04,70%	0,00%	91,60%	96,30%
2	5	3	8	04,60%	0,00%	91,80%	96,50%
3	2	5	2	99,00%	0,07%	00,00%	99,10%
3	2	5	5	99,00%	0,07%	00,00%	99,10%
3	2	5	8	04,30%	0,07%	91,60%	96,00%
3	3	3	2	99,40%	0,00%	00,00%	99,40%
3	3	3	5	99,40%	0,00%	00,00%	99,40%
3	3	3	8	99,40%	0,00%	00,00%	99,40%
3	5	2	2	04,70%	0,00%	91,60%	96,30%
3	5	2	5	04,70%	0,00%	91,60%	96,30%
3	5	2	8	04,60%	0,00%	91,80%	96,50%
5	2	3	2	99,70%	0,00%	00,00%	99,70%
5	2	3	5	04,90%	0,00%	91,60%	96,60%
5	2	3	8	04,90%	0,00%	91,80%	96,80%
5	3	2	2	04,90%	0,00%	91,60%	96,60%
5	3	2	5	04,90%	0,00%	91,60%	96,60%
5	3	2	8	04,90%	0,00%	91,80%	96,80%

Tabela 3. TAP e TCA - Cenário 1

Pesos Sociais				Tx. Ap. de Políticas (TAP)			TCA
α	β	γ	δ	$\mathcal{P}_1$	$\mathcal{P}_2$	$\mathcal{P}_3$	
2	3	5	2	99,60%	0,00%	0,00%	99,60%
2	3	5	5	99,60%	0,00%	0,00%	99,60%
2	3	5	8	99,60%	0,00%	0,00%	99,60%
2	5	3	2	99,60%	0,00%	0,00%	99,60%
2	5	3	5	99,60%	0,00%	0,00%	99,60%
2	5	3	8	99,60%	0,00%	0,00%	99,60%
3	2	5	2	98,70%	0,01%	0,00%	98,70%
3	2	5	5	98,70%	0,01%	0,00%	98,70%
3	2	5	8	04,60%	0,01%	88,9%	93,60%
3	3	3	2	99,60%	0,00%	0,00%	99,60%
3	3	3	5	99,60%	0,00%	0,00%	99,60%
3	3	3	8	99,60%	0,00%	0,00%	99,60%
3	5	2	2	98,70%	0,01%	0,00%	98,70%
3	5	2	5	98,70%	0,01%	0,00%	98,70%
3	5	2	8	04,60%	0,01%	88,9%	93,60%
5	2	3	2	98,70%	0,01%	0,00%	98,70%
5	2	3	5	98,70%	0,01%	0,00%	98,70%
5	2	3	8	04,60%	0,01%	88,9%	93,60%
5	3	2	2	98,70%	0,01%	0,00%	98,70%
5	3	2	5	98,70%	0,01%	0,00%	98,70%
5	3	2	8	04,60%	0,01%	88,9%	93,60%

Tabela 4. TAP e TCA - Cenário 2

5. Conclusão

Este trabalho apresentou o sistema GALENA para a gestão da autenticação adaptativa de dispositivos em redes IoT de acordo com os riscos do contexto e do nível da confiança social estabelecida entre os dispositivos nos vários domínios de aplicações. Ao levar em conta os fatores *C-LOR* e *C-WOR*, o GALENA coordena via políticas pré-estabelecidas a configuração dos mecanismos de segurança aplicados na autenticação, tal que os dispositivos transitem entre ambientes tomando e disponibilizando serviços de forma segura. Os resultados obtidos mostram a sua eficiência para aplicar mecanismos de autenticação respeitando as características de cada dispositivo e os riscos nos ambientes IoT. Como trabalhos futuros pretende-se avaliar a eficiência do GALENA utilizando métricas agregadas e também o funcionamento do sistema diante de ataques de difamação.

Agradecimentos

O presente trabalho foi realizado com apoio do CNPq através dos projetos No. 436649/2018-7 e 313641/2020-0 e bolsas de pesquisa CNPq e CAPES do PPGInf/UFPR.

Referências

Aman, W. and Snekkenes, E. (2015). EDAS: An evaluation prototype for autonomic event-driven adaptive security in the internet of things. *Future Internet*, 7(4):225–256.

Arias-Cabarcos, P., Krupitzer, C., and Becker, C. (2019). A survey on adaptive authentication. *ACM Computing Surveys*, 52(4):1–30.

Assis, M. V. O. D., Hamamoto, A. H., Abrao, T., and Proenca, M. L. (2017). A game theoretical based system using holt-winters and genetic algorithm with fuzzy logic for DoS/DDoS mitigation on SDN networks. *IEEE Access*, 5:9485–9496.

Chen, I.-R., Guo, J., Wang, D.-C., Tsai, J. J., Al-Hamadi, H., and You, I. (2018). Trust as a Service for IoT Service Management in Smart Cities. In *2018 IEEE 20th International Conference on High Performance Computing and Communications.*, pages 1358–1365. IEEE.

de Oliveira, G. H., de Souza Batista, A., Nogueira, M., and dos Santos, A. L. (2022). An access control for iot based on network community perception and social trust against sybil attacks. *International Journal of Network Management*, 32(1):e2181.

El-hajj, M., Fadlallah, A., Chamoun, M., and Serhrouchni, A. (2019). A survey of internet of things (IoT) authentication schemes. *Sensors*, 19(5):1141.

Gebrie, M. T. and Abie, H. (2017). Risk-based adaptive authentication for internet of things in smart home ehealth. In *Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings*, pages 102–108.

Gwak, B., Cho, J. H., Lee, D., and Son, H. (2018). TARAS: Trust-Aware Role-Based Access Control System in Public Internet-of-Things. *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pages 74–85.

Hamdi, M. and Abie, H. (2014). Game-based adaptive security in the internet of things for eHealth. In *2014 IEEE International Conference on Communications (ICC)*. IEEE.

Hayashi, E., Das, S., Amini, S., Hong, J., and Oakley, I. (2013). Casa: context-aware scalable authentication. In *Proc. of the Ninth Symposium on Usable Privacy and Security*, pages 1–10.

Huertas Celdrán, A., Gil Pérez, M., García Clemente, F. J., and Martínez Pérez, G. (2019). Towards the autonomous provision of self-protection capabilities in 5G networks. *Journal of Ambient Intelligence and Humanized Computing*, 10(12):4707–4720.

Jafarian, B., Yazdani, N., and Haghighi, M. S. (2020). Discrimination-aware trust management for social internet of things. *Computer Networks*, 178:107254.

Marche, C., Atzori, L., and Nitti, M. (2018). A dataset for performance analysis of the social internet of things. In *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pages 1–5. IEEE.

Morabito, R. and Jimenez, J. (2020). IETF protocol suite for the internet of things: Overview and recent advancements. *IEEE Communications Standards Magazine*, 4(2):41–49.

Patwary, A. A.-N., Fu, A., Naha, R. K., Battula, S. K., Garg, S., Patwary, M. A. K., and Aghasian, E. (2020). Authentication, access control, privacy, threats and trust management towards securing fog computing environments: A review. *arXiv preprint arXiv:2003.00395*.

Qin, W., Chen, S., and Peng, M. (2020). Recent advances in industrial internet: insights and challenges. *Digital Communications and Networks*, 6(1):1–13.

Sylla, T., Chalouf, M. A., Krief, F., and Samaké, K. (2020). Towards a context-aware security and privacy as a service in the internet of things. In *IFIP Info Security Theory and Practice*.

Tan, S., Liu, Y., Li, X., and Dong, Q. (2016). A similarity-based indirect trust model with anti-spoofing capability. *Security and Communication Networks*, 9(18):5868–5881.