

UNIVERSIDADE FEDERAL DO PARANÁ

YAN UEHARA DE MORAES

GERENCIAMENTO E PROTEÇÃO DO SERVIÇO DE AUTENTICAÇÃO ADAPTATIVA
SOCIAL PARA AMBIENTES IOT CONTRA ATAQUES DE DIFAMAÇÃO

CURITIBA PR

2022

YAN UEHARA DE MORAES

GERENCIAMENTO E PROTEÇÃO DO SERVIÇO DE AUTENTICAÇÃO ADAPTATIVA
SOCIAL PARA AMBIENTES IOT CONTRA ATAQUES DE DIFAMAÇÃO

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre em Informática no Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, da Universidade Federal do Paraná.

Área de concentração: *Ciência da Computação*.

Orientador: Aldri Luiz dos Santos.

CURITIBA PR

2022

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)
UNIVERSIDADE FEDERAL DO PARANÁ
SISTEMA DE BIBLIOTECAS – BIBLIOTECA CIÊNCIA E TECNOLOGIA

Moraes, Yan Uehara de

Gerenciamento e proteção do serviço de autenticação adaptativa social para ambientes IoT contra ataques de difamação / Yan Uehara de Moraes– Curitiba, 2022.

1 recurso on-line : PDF.

Dissertação (mestrado) - Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-graduação em Informática.

Orientador: Aldri Luiz dos Santos.

Acesso dados abertos BDC/UFPR:

[Doi.org/10.5281/zenodo.6654128](https://doi.org/10.5281/zenodo.6654128)

1. Internet. 2. Tecnologia da informação - Sistemas de segurança. 3. Internet das coisas. 4. Autenticação. I. Santos, Aldri Luiz dos. II. Universidade Federal do Paraná. Programa de pós-Graduação em Ciências Exatas. III. Título.

Bibliotecária: Roseny Rivelini Morciani CRB-9/1585

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação INFORMÁTICA da Universidade Federal do Paraná foram convocados para realizar a arguição da Dissertação de Mestrado de **YAN UEHARA DE MORAES** intitulada: **Gerenciamento e Proteção do Serviço de Autenticação Adaptativa Social para Ambientes IoT Contra Ataques de Difamação**, sob orientação do Prof. Dr. ALDRI LUIZ DOS SANTOS, que após terem inquirido o aluno e realizada a avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito de defesa.

A outorga do título de mestre está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

CURITIBA, 31 de Março de 2022.

Assinatura Eletrônica

05/04/2022 16:45:02.0

ALDRI LUIZ DOS SANTOS

Presidente da Banca Examinadora

Assinatura Eletrônica

19/04/2022 10:00:47.0

EDUARDO LUZEIRO FEITOSA

Avaliador Externo (UNIVERSIDADE FEDERAL DO AMAZONAS)

Assinatura Eletrônica

05/04/2022 15:53:13.0

MICHELE NOGUEIRA LIMA

Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

*Para a minha família, que me mesmo
de longe, me apoiou até aqui*

AGRADECIMENTOS

Ao meu pai, Ronny Machado, e minha mãe, Kenia Uehara, pela educação proporcionada até agora que possibilitou essa conquista. Ao meu irmão, Kevyan Uehara, pela parceria nesses anos, paciência e apoio no dia-a-dia. À todos da minha família, que me apoiaram e torceram por mim nessa caminhada, mesmo estando longe.

Aos meus amigos e colegas da vida, da faculdade e da república do Dragan, por terem entendido minhas ausências, me suportado, e ouvido meus desabafos nesses anos. Em especial ao Willian Berté, pela amizade, presença, paciência e estímulo ao longo desse curso.

Aos amigos do NR2 e CCSC, Anderson Bergamini, Alisson Yuri, Agnaldo Batista, Andressa Vergütz, Bruno Henrique Schwengber, Bruno Marquez Cremonezi, Cainã Passos, Euclides Peres Farias Junior, Everaldo Andrade, Fernando Nakayama, Giovanni Rosa, Gustavo Henrique Carvalho de Oliveira, Ligia Francielle Borges, Nelson Gonçalves Prates Junior, Paulo Lenz Junior, Uelinton Brezolin, pela convivência e companheirismo, e também por dividirem grande parte dessa jornada comigo. Em especial ao Carlos Alberto Pedroso Junior, pelo desenvolvimento de outras pesquisas com a publicação das nossas análises e propostas.

Ao Prof. Dr. Aldri Luiz dos Santos, meu orientador, sou grato pela oportunidade de desenvolver minha pesquisa no Núcleo de Redes Sem Fio e Redes Avançadas durante o curso de Mestrado em Informática da Universidade Federal do Paraná (UFPR) e pela paciência, estímulo e dedicação exercidos nessa jornada. Agradeço também a oportunidade do contato com os alunos de graduação durante o meu estágio docência.

À Prof^a. Dr^a. Michele Nogueira Lima, pelos comentários e ensinamentos durante o Mestrado, enquanto coordenadora do Centro de Ciência de Segurança Computacional (CCSC) da UFPR. E também pela confiança enquanto professora, por me proporcionar o contato com seus alunos durante meu período de estágio docência.

Ao Programa de Pós-Graduação em Informática da Universidade Federal do Paraná, pelo auxílio administrativo que possibilitou minha participação em eventos e pela infraestrutura computacional. Agradeço também aos funcionários do departamento pelo auxílio com processos burocráticos da instituição.

Ao CNPq, que me proporcionou o financiamento dessa pesquisa.

"Quem é você?"

"[...] Eu sou a Alice, mas não a certa"

"Como sabe?"

"Você mesmo disse isso!"

"Eu disse que nem de longe você era Alice, mas está bem perto de ser a Alice agora. Aliás, você
é quase a Alice"

Alice no País das Maravilhas, 2010.

RESUMO

Os dispositivos das redes IoT geralmente têm capacidades de comunicação, processamento e energia limitados além de terem que lidar com desafios relacionadas a segurança e confiabilidade da comunicação. Para manter a segurança, a IoT emprega a autenticação e a diversidade de mecanismos de autenticação derivados da heterogeneidade da rede fez surgir os sistemas de autenticação adaptativa. Esses sistemas utilizam fatores de entrada para decidir de maneira autônoma o mecanismo mais adequado para uma determinada situação. No entanto, as atuais abordagens de autenticação adaptativa não são adequadas para redes não estruturadas. Elas se restringem a utilização de somente um fator, como o contexto e ignoram outras características dos dispositivos com o qual se interage. Ainda, as técnicas para decidir pela adaptação não são adequadas a restrição de processamento dos dispositivos da IoT. Essa dissertação investigou os benefícios da percepção social, derivada do paradigma da Internet das Coisas Sociais (SIoT), como fator para adaptação da autenticação para tomada e oferecimento de serviços entre os dispositivos IoT de acordo com a compatibilidade do contexto. Assim, propôs-se o sistema GALENA (*manaGement of Adaptive authentication based on poLiciEs aNd sociAl trust*), que determina o mecanismo de autenticação mais adequado para realizar o procedimento de autenticação entre os dispositivos IoT. O sistema lida com a restrição dos dispositivos utilizando uma técnica de políticas para ser a inteligência que dita a necessidade de adaptação. Além disso, para evitar comportamentos maliciosos que atinjam as recomendações sociais trocadas, como o ataque de difamação que visa diminuir a confiança de um dispositivo, o GALENA aplica técnicas de *Data Provenance* para autenticar a fonte das recomendações. Assim, ele é capaz de descartar recomendações de vizinhos maliciosos que visem difamar outros dispositivos. O GALENA foi avaliado através de simulações no NS3 e os resultados obtidos demonstram a sua eficiência na adaptação e seleção do mecanismo de autenticação adequado a cada interação, tendo uma taxa de compatibilidade de cerca de 97% numa rede IoT com 200 dispositivos e de 98% com 400 dispositivos, em todos os cenários analisados, com acurácia máxima da confiança de cerca de 64% nos dois cenários. O GALENA também foi capaz de atingir uma taxa de detecção do ataque de difamação de até 90,62% com 200 dispositivos e de 74,76% com 400 dispositivos, com acurácia da detecção de cerca de 91% e de até 79% respectivamente. O sistema exibiu uma taxa de falsos negativos baixa em torno 10% com 200 dispositivos e de 31% com 400 dispositivos.

Palavras-chave: Ambientes IoT, Autenticação Adaptativa, Políticas, Confiança Social, Difamação

ABSTRACT

The IoT devices usually have limited computational, energetic and communication capabilities, and also they have to deal with challenges related to security and communication reliability. The IoT network employs authentication in order to maintain its security and the diversity of authentication mechanisms derived from the heterogeneity of the network has led to emergence of adaptive authentication systems. These systems resort to input factors in order to determine autonomously the suitable mechanism for a specific situation. However, current adaptive authentication approaches are not suitable for ad hoc networks, since they restrict themselves in using one input factor, such as context, and do not take into account other factors of the devices it interacts. In addition, they employ techniques that are not suitable to the devices processing restrictions. This dissertation investigated the benefits come from social perception, derived from the Social Internet of Things paradigm (SIoT), as adaptation factor in order to exchange services among IoT devices according to context compatibility. Thus, it is presented the GALENA system (*manaGement of Adaptive authentication based on poLiciEs aNd sociAl trust*), which decides the suitable authentication mechanism to apply in authentication procedures in IoT devices. The system address the devices' computational restrictions employing policies that dictates the need for adaptation. Moreover, in order to prevent malicious behaviour aimed at the social recommendations exchanged, such as the badmouthing attack that seeks to diminish the trust over a device, GALENA employs *Data Provenance* techniques to authenticate the source of the recommendation. Thus, it is able to discard manipulated recommendations that aim to defame other devices. GALENA was evaluated through simulations in NS-3 and the results demonstrate its efficiency in adapting and selecting the suitable authentication mechanism each interaction. The system achieved a compatibility rate of 97% in an IoT network with 200 devices and 98% in one with 400 devices, with trust accuracy of 64% in both configurations. It also achieved a detection rate of the badmouthing attack up to 90,62% with 200 devices and up to 74,76% with 400 devices, with an detection accuracy of 91% and of 79% respectively. Further, the system reached a low false negative rate, around 10% with 200 devices and 31% with 400 devices.

Keywords: IoT Environments, Adaptive Authentication, Policies, Social Trust, Badmouthing

LISTA DE FIGURAS

2.1	Arquiteturas propostas para IoT.	22
4.1	Modelo de rede	44
4.2	Arquitetura do GALENA	46
4.3	Funcionamento do GALENA em um Sistema de Transporte Inteligente.	51
4.4	Ataque no cenário exemplo	52
5.1	<i>EC</i> para o Cenário 1	58
5.2	<i>EC</i> para o Cenário 2	59
5.3	<i>EC</i> para o Cenário 1 - DCP	64
5.4	<i>EC</i> para o Cenário 1 - DCS	65
5.5	<i>EC</i> para o Cenário 1 - DSP	66
5.6	<i>EC</i> para o Cenário 1 - DSS	67
B.1	<i>EC</i> para o Cenário 2 - DCP	84
B.2	<i>EC</i> para o Cenário 2 - DCS	85
B.3	<i>EC</i> para o Cenário 2 - DSP	86
B.4	<i>EC</i> para o Cenário 2 - DSS	87

LISTA DE TABELAS

3.1	Requisitos necessários para os SAAs	33
3.2	Resumo dos trabalhos de autenticação adaptativa	34
3.3	Resumo dos trabalhos de gerenciamento de confiança em IoT	38
3.4	Resumo dos trabalhos de gerenciamento de confiança em SIoT	40
3.5	Requisitos necessários para os TMSs.	41
5.1	Configuração comum dos cenários	54
5.2	Valores possíveis por parâmetro	54
5.3	Acurácia da Confiança (AC)	60
5.4	<i>MEA</i> dos Cenários	61
5.5	<i>TAP</i> e <i>TCA</i> para o Cenário 1.	62
5.6	<i>TAP</i> e <i>TCA</i> para o Cenário 2.	62
5.7	<i>AC</i> - DCP	68
5.8	<i>AC</i> - DCS	68
5.9	<i>AC</i> - DSP	69
5.10	<i>AC</i> - DSS	69
5.11	<i>MEA</i> - DCP	70
5.12	<i>MEA</i> - DCS	70
5.13	<i>MEA</i> - DSP	70
5.14	<i>MEA</i> - DSS	70
5.15	<i>TAP</i> e <i>TCA</i> do DCP - Cenário 1	71
5.16	<i>TAP</i> e <i>TCA</i> do DCS - Cenário 1	71
5.17	<i>TAP</i> e <i>TCA</i> do DSP - Cenário 1	71
5.18	<i>TAP</i> e <i>TCA</i> do DSS - Cenário 1	71
5.19	T_{fp} , T_{fn} , T_{acc} , T_{det} para os Comportamentos DSP e DSS	72
B.1	<i>TAP</i> e <i>TCA</i> do DCP - Cenário 2.	83
B.2	<i>TAP</i> e <i>TCA</i> do DCS - Cenário 2	83
B.3	<i>TAP</i> e <i>TCA</i> do DSP - Cenário 2	83
B.4	<i>TAP</i> e <i>TCA</i> do DSS - Cenário 2	83

LISTA DE ACRÔNIMOS

6LoWPAN	IPv6 over Low -Power Wireless Personal Area Networks (IPv6 sobre Redes Pessoais de Baixa Energia)
ABAC	Attribute Based Access Control (Controle de Acesso baseado em Atributos)
C-LOR/LOR	Co-location object relationship (Relacionamento por Co-localização)
CoI	Communities of Interest (Comunidades de Interesse)
C-WOR/WOR	Co-work object relationship (Relacionamento por Cooperação de Trabalho)
DCP	Difamação Constante com Identificação Própria
DCS	Difamação Seletiva com Identificação Própria
DDoS	Distributed Denial of Service (Negação de Serviço Distribuída)
DINF	Departamento de Informática
DNS-SD	DNS-Based Service Discovery (Descoberta de Serviços baseado em DNS)
DSP	Difamação Constante com Identificação Sybil
ECC	Elliptic-curve cryptography (Criptografia de Curvas Elípticas)
GALENA	Management of Adaptive Authentication based on Policies and Social Trust (Sistema de Gerência de Autenticação Adaptativa baseado em Políticas e Confiança Social)
HMAC	Hash-based Message Authentication Code (Código de Autenticação de Mensagem baseado em Hash)
IEEE	Institute of Electrical and Electronics Engineers (Instituto de Engenheiros Eletricistas e Eletrônicos)
IoT	Internet of Things (Internet das Coisas)
IPv6	Internet Protocol v6 (Protocolo de Internet v6)
M2M	Máquina-a-Máquina
MAC	Message Authentication Code (Código de Autenticação de Mensagem)

MIT	Massachussets Institute of Technology (Instituto de Tecnologia de Massachussets)
ML	Machine Learning (Aprendizado de Máquina)
NS-3	Network Simulator-3
OOR	Ownership Object Relationship (Relacionamento por propriedade)
PAP	Policy Administration Point (Ponto de Administração de Políticas)
PDP	Policy Decision Point (Ponto de Decisão de Políticas)
PEP	Policy Enforcement Point (Ponto de Aplicação de Políticas)
PIP	Policy Information Point (Ponto de Informação de Políticas)
POR	Parental Object Relationship (Relacionamento por Semelhança)
PPGINF	Programa de Pós-Graduação em Informática
PPG	Programa de Pós-Graduação
PUF	Physical Unclonable Function (Função Física Não-clonável)
RBAC	Role-Based Access Control (Controle de acesso baseado em papéis)
RFID	Radio-Frequency Identification (Identificação por Radiofrequência)
RSA	Rivest–Shamir–Adleman
RSSI	Radio Signal Strength Indicator (Indicação de Força do Sinal Recebido)
SAA	Sistemas de Autenticação Adaptativa
SADPT	Serviço de Controle de Adaptação
SDCAP	Serviço de Descoberta de Capacidades
SDES	Serviço de Descoberta de Vizinhaça
SDN	Software Defined Networks (Redes Definidas por Software)
SDPOL	Serviço de Políticas
SGAUTH	Subsistema de Gerência de Autenticação
SGDE	Subsistema de Gerência de Descoberta
SIoT	Social Internet of Things (Internet das Coisas Sociais)

SIR-M	Susceptible-Infective-Recovered with Maintenance (Suscetível-Infectado-Recuperado com Manutenção)
SISCO	Serviço de Interação Social e Confiança
SLOC	Serviço de Localização
SOA	Service-Oriented Architecture (Arquitetura Orientada a Serviços)
SOR	Social Object Relationship (Relação Social)
SP	Service Provider (Provedor de Serviço)
SR	Service Requester (Tomador de Serviço)
SSGSOC	Subsistema de Gerência Social
SVOR	Serviço de Validação de Origem
TMS	Trust Management Systems (Sistemas de Gerenciamento de Confiança)
TRS	Trust and Recommender Systems (Sistemas de Recomendação e Confiança)
UDP	User Datagram Protocol
UFMS	Universidade Federal do Mato Grosso do Sul
UFPR	Universidade Federal do Paraná
VNF	Virtual Network Functions (Funções de Rede Virtualizadas)
WBAN	Wireless Body Area Network (Rede de Área Corporal)
WPAN	Wireless Personal Area Network (Rede Pessoal sem Fio)

LISTA DE SÍMBOLOS

α	Alfa, primeira letra do alfabeto grego
β	Beta, segunda letra do alfabeto grego
γ	Gama, terceira letra do alfabeto grego
δ	Delta, quarta letra do alfabeto grego
λ	Lambda, décima primeira letra do alfabeto grego
μ	Mu, décima segunda letra do alfabeto grego
ω	Ômega, última letra do alfabeto grego
e	Número de Euler
τ	Interações totais entre dois dispositivos
D	Conjunto dos dispositivos da rede
D_{mov}	Conjunto dos dispositivos com mobilidade da rede
D_{sta}	Conjunto dos dispositivos estáticos da rede
O_{Id}	Conjunto dos serviços ofertados por um dispositivo da rede
M_{Id}	Conjunto de mecanismos de adaptação de um dispositivo
S	Função que calcula a sociabilidade de um dispositivo
$\mathcal{L}$	Função de mapeamento do ambiente
$\mathcal{F}$	Função de filtro sobre o Id
C	Função de filtro sobre o contexto
$\mathcal{P}_j$	Política de autenticação
p_i^{mec}	Perfil de autenticação i do mecanismo mec
t e t_{now}	Notação de tempo
T_{abs}	Taxa de detecção
T_{fp}	Taxa de falsos positivos
T_{fn}	Taxa de falsos negativos
T_{acc}	Acurácia da detecção
$C_{i,j}^t$	Confiança de i para j no instante t
$C_{i,j}^{pred}$	Confiança predita de i para j
$C_{i,j}^{act}$	Confiança de referência de i para j
C_i	Média de confiança do dispositivo i
R_i	Recomendações a respeito de i
N_i	Quantidade de dispositivos que recomendaram o dispositivo i
int	Total de interações entre os dispositivos
$int\varphi_j$	Taxa de aplicação da política $\mathcal{P}_j$
$I_{i,j}$	Variável binária que traduz o resultado da interação de i e j

T_{det}	Taxa de detecção
T_{atk}	Total de recomendações que constituíam um ataque
R_d	Recomendações que eram ataque

SUMÁRIO

1	INTRODUÇÃO	17
1.1	PROBLEMA	18
1.2	OBJETIVOS	19
1.3	CONTRIBUIÇÕES	20
1.4	ESTRUTURA DA DISSERTAÇÃO	20
2	FUNDAMENTOS	21
2.1	INTERNET DAS COISAS	21
2.1.1	Modelos de Arquiteturas	22
2.1.2	Domínios de Aplicação	22
2.2	SERVIÇO DE AUTENTICAÇÃO	23
2.3	INTERNET DAS COISAS SOCIAIS	23
2.3.1	Confiança social.	24
2.4	ATAQUES CONTRA A CONFIANÇA	24
2.5	POLÍTICAS.	26
2.6	<i>DATA PROVENANCE</i>	26
2.7	RESUMO	27
3	TÉCNICAS DE AUTENTICAÇÃO ADAPTATIVA E SISTEMAS DE GERENCIAMENTO DE CONFIANÇA SOCIAL NA IOT	28
3.1	AUTENTICAÇÃO ADAPTATIVA	28
3.1.1	Baseada em Aprendizagem de Máquina	28
3.1.2	Baseada em Teoria dos Jogos	29
3.1.3	Baseada em Políticas e Ontologias	30
3.1.4	Discussão dos Sistemas de Autenticação Adaptativa na IoT	32
3.2	GERENCIAMENTO DE CONFIANÇA	34
3.2.1	Confiança Social	36
3.2.2	Perspectivas da Composição da Confiança	37
3.2.3	Técnicas Contra o Ataque de Difamação	41
3.3	RESUMO	42
4	AUTENTICAÇÃO ADAPTATIVA DE DISPOSITIVOS IOT SOCIAIS RESISTENTE A ATAQUES DE DIFAMAÇÃO	43
4.1	CARACTERÍSTICAS DOS AMBIENTES IOT E DOS ATAQUES	43
4.1.1	Ambientes de Redes IoT	43
4.1.2	Interação Social entre Dispositivos	44
4.1.3	Modelo do Ataque de Difamação	45

4.2	SISTEMA GALENA	45
4.2.1	Gerência de Descoberta.	46
4.2.2	Gerência Social	47
4.2.3	Gerência de Autenticação.	48
4.3	FUNCIONAMENTO	50
4.3.1	Exemplo de Funcionamento em um Sistema de Transporte Inteligente	51
4.4	RESUMO	52
5	AVALIAÇÃO	53
5.1	IMPLEMENTAÇÃO	53
5.2	AMBIENTE E CONFIGURAÇÕES	54
5.3	MÉTRICAS	55
5.4	ANÁLISE DOS RESULTADOS E DISCUSSÃO	57
5.4.1	Desempenho	57
5.4.2	Robustez das recomendações sociais	62
5.5	RESUMO	72
6	CONCLUSÕES	73
6.1	QUESTÕES DE PESQUISA	74
6.2	TRABALHOS FUTUROS	74
	REFERÊNCIAS	76
	APÊNDICE A – METODOLOGIA DO LEVANTAMENTO BIBLIOGRÁFICO	82
	APÊNDICE B – RESULTADOS DA AVALIAÇÃO DE SEGURANÇA . . .	83
B.1	<i>TAP</i> E <i>TCA</i> PARA OS ATAQUES NO CENÁRIO 2	83
B.2	<i>EC</i> PARA OS ATAQUES NO CENÁRIO 2	84

1 INTRODUÇÃO

A miniaturização dos dispositivos computacionais e a abrangência das comunicações sem fio apoiaram o surgimento das redes de sensores sem fio e o paradigma da Internet das Coisas, (do inglês *Internet of Things* – IoT). Esse paradigma compreende uma grande quantidade de objetos como veículos, eletrodomésticos, entre outros, com sensores e atuadores atrelados a eles a fim de coletar informações sobre o ambiente físico e influenciar suas decisões e configurações (Qin et al., 2020). Esses dispositivos IoT normalmente denominados dispositivos inteligentes ou simplesmente objetos comunicam-se entre si e com os usuários visando oferecer serviços específicos com base no ambiente que eles se encontram. Espera-se para o ano de 2035 que cerca de 1 trilhão de dispositivos estejam conectados entre si provendo diversos serviços personalizados aos usuários (ITUNews, 2018); Além disso, esses dispositivos têm o potencial de impactar a vida das pessoas por estarem presentes em diferentes ambientes urbanos (Datamation, 2022). Os dispositivos IoT não só têm capacidade de sensoramento como atuam sobre os ambientes que se inserem visando melhorar os serviços existentes. Assim, a IoT também é definida como uma intersecção entre as pessoas, os sistemas e o mundo físico (Atzori et al., 2017).

A IoT se faz cada vez mais presente e pervasiva em diversos ambientes organizados da sociedade, como residências, indústrias, hospitais, cidades inteligentes, entre outras (Qin et al., 2020; Atzori et al., 2017), suportando necessidades específicas de sensoramento e gerenciamento de serviços, muitos deles interligados, em cada um desses ambientes. As cidades inteligentes agregam outras aplicações existentes em uma cidade que são apoiados pelos dispositivos IoT (Gardašević et al., 2016). Elas são baseadas na arquitetura orientada a serviço (do inglês, *Service Oriented Architecture* – SOA) o que permite aos dispositivos IoT conversarem autonomamente entre si e também sua interoperação. Nas cidades inteligentes os dispositivos IoT oferecem diversos serviços visando ao aumento da qualidade de vida dos seus habitantes. Ao prestarem serviços, de maneira isolada ou através da composição de outros serviços, os dispositivos levam em consideração o contexto e situação atual do usuário.

As cidades inteligentes são compostas de outras aplicações aos cidadãos, como os sistemas de transporte inteligente (do inglês, *Intelligent Transport systems*), casas inteligentes (do inglês, *Smart Homes*), IoT na energia ou grids elétricos (do inglês, *Smart Grids*), aplicações na saúde (do inglês, *E-Health*), entre outros (Atzori et al., 2017). Cada uma dessas aplicações impacta de uma maneira diferente no cotidiano das pessoas. Os sistemas de transporte inteligente visam aumentar a eficiência do tráfego e aumentar a segurança no transporte. As casas inteligentes englobam os dispositivos para automação doméstica, como lâmpadas e equipamentos domésticos inteligentes. Na energia, os dispositivos IoT permitem um uso mais consciente da energia através do controle inteligente das redes de distribuição e atuam na sua produção. Na saúde, os dispositivos IoT estão presentes nos dispositivos vestíveis, como relógios inteligentes, e permitem a equipe médica e hospitalar uma interação com o paciente a distância (Qin et al., 2020). Assim, visto que parte desses dispositivos são dotados de mobilidade, eles trocam serviços em diferentes domínios ao longo do tempo. Ademais, cada uma dessas aplicações que constituem uma cidade inteligente têm requisitos de funcionamento e de segurança distintos, pois envolvem diferentes ambientes e compreendem dispositivos heterogêneos.

De uma maneira geral, uma rede IoT pode ser definida como uma rede híbrida, aberta, ubíqua e heterogênea (Al-Fuqaha et al., 2015) e a sua hibridéz decorre da diversidade de arquiteturas de rede que a compõe, como redes estruturadas e não estruturadas. Ela é heterogênea pois dispositivos com diferentes capacidades computacionais estão presentes, constituindo um

desafio para aplicações IoT. A rede se apresenta aberta e ubíqua, pois qualquer dispositivo em qualquer situação pode requerer ou ofertar serviços a outros dispositivos (Qin et al., 2020). As redes IoT também se mostram dinâmicas, pois alguns dispositivos são dotados de mobilidade e constroem conexões com outros dispositivos próximos de maneira imprevisível. No entanto, a dinamicidade dessa rede trás também o desafio de escalabilidade. Dessa maneira, uma gerência automática e autônoma são características desejáveis nos dispositivos IoT (Atzori et al., 2017).

Todavia, a medida que aumenta a interação com os dispositivos e estes estão presentes em vários ambientes com diferentes propósitos e requisitos, a segurança naturalmente torna-se uma preocupação. Pelo fato da rede ser aberta, faz-se improvável a adoção de certas medidas de segurança em larga escala pelos diferentes atores da rede. Ainda, desafios como confidencialidade dos dados, privacidade e confiança tornam-se importantes, pois os dispositivos IoT lidam com dados sensíveis dos usuários. A confidencialidade e a privacidade dos dados estão intrinsecamente ligadas ao controle de acesso e, especificamente a autenticação entre os dispositivos, tanto autonomamente quanto por iniciativa do usuário. A autenticação visa garantir a identidade dos objetos sendo a primeira etapa do controle de acesso. Após a autenticação verifica-se, na etapa de autorização, se os dispositivos podem realizar a ação que solicitaram. Assim, garante-se que apenas dispositivos reconhecidos e autorizados tenham acesso a dados sensíveis. Desse modo, torna-se necessário que os dispositivos IoT possuam mecanismos de autenticação adequados ao ambiente no qual se encontram ou que venham a interagir e, ainda, que a escolha desses mecanismos ocorra de maneira autônoma (Arias-Cabarcos et al., 2019).

1.1 PROBLEMA

Dentre os muitos serviços demandados pelos dispositivos IoT para estabelecer uma comunicação segura está o serviço de autenticação. Este serviço visa identificar um dispositivo perante ao outro a fim de que a comunicação ocorra perante participantes identificados e um meio de comunicação seguro (El-hajj et al., 2019) a fim de que serviços sejam trocados ou informações acessadas. As aplicações em dispositivos IoT também necessitam de níveis diferentes de segurança a depender do ambiente que o dispositivo está localizado e a medida que o dispositivo potencialmente transita entre ambientes com diferentes requerimentos de segurança. Assim, esses dispositivos devem suportar diversos mecanismos de autenticação com o intuito de tomar serviços nas diversas localizações da rede e nos diversos níveis de segurança requeridos.

A diversidade de mecanismos de autenticação resultou na criação de **Sistemas de Autenticação Adaptativa (SAAs)**, que determinam um mecanismo de autenticação a ser utilizado com base em fatores de adaptação (Arias-Cabarcos et al., 2019) como a localização e o comportamento do usuário. Assim, os SAAs trazem flexibilidade a gestão da autenticação ao permitirem ao dispositivo se adequar ao nível de segurança requerido pela comunicação ou desejado quando interage com dispositivos nas diversas localidades de rede. Esses sistemas empregam técnicas para determinar a necessidade de adaptação como aprendizado de máquina, teoria dos jogos e políticas. Entretanto, os sistemas adaptativos existentes na literatura se mostram inadequados às redes IoT massivas e abertas, como as presentes em *Smart Cities*, na medida que essas soluções mostram-se centralizadas quanto a sua arquitetura, e, portanto, não escalam para todos os ambientes. Ainda, essas soluções empregam técnicas de adaptação inadequadas aos dispositivos com restrição de recursos que formam a IoT, como aquelas baseadas em aprendizado de máquina e teoria dos jogos, que mostram-se computacionalmente custosas, no lugar de técnicas leves, como o uso de políticas.

Os dispositivos que transitam entre domínios da IoT em múltiplos ambientes carecem de SAAs que consideram na tomada de decisão de adaptação as relações subjetivas construídas

pelos dispositivos à medida que eles transitam pelos ambientes. Assim, os sistemas existentes não avaliam de forma assertiva os dispositivos ao analisar fatores de adaptação fixos. Por outro lado, a percepção social permite que o comportamento dos dispositivos seja avaliado de forma assertiva (Chen et al., 2018) e a autenticação tenha o nível de segurança adequado. Entretanto, o uso da percepção social como fator de adaptação implica em garantir que as recomendações sociais trocadas sejam legítimas, pois estão sujeitas a ataques, como o ataque de difamação, do inglês *Badmouthing*, por exemplo. Assim, os SAAs também deveriam incluir contramedidas diante de ataques cujo comportamento tentam manipular os fatores de adaptação adotados pelo sistema.

Desse modo, torna-se necessário uma solução adequada às restrições dos dispositivos e que utilizem percepções compatíveis com as interações e com os ambientes diferentes de uma rede aberta e orientada a serviços. Além disso, a solução deveria ser capaz de avaliar o comportamento de dispositivo IoT vizinho de maneira autônoma para a adaptação do mecanismo de autenticação a ser aplicado e também ser capaz de proteger os fatores empregados na adaptação. Diante disso, as seguintes questões foram exploradas:

- **Múltiplos fatores sociais e da percepção do ambiente podem ser incorporados aos SAAs?** Existem diversos SAAs que empregam um único fator para adaptação. Assim, um SAA que incorpore não só a percepção social mas também a percepção do ambiente, possibilitaria uma adaptação mais assertiva e mais adequada a medida que os dispositivos transitassem pelos ambientes.
- **Qual é o impacto da influência de cada fator social na confiança final estabelecida entre os dispositivos IoT?** A literatura oferece uma variedade de modos de se derivar um valor para a percepção social. No entanto, diversas combinações dos fatores sociais considerados existem e influenciam no valor da confiança social obtida e na definição da adaptação, por consequência.
- **Como proteger as recomendações sociais entre os dispositivos IoT diante de ataques de difamação nos ambientes?** As recomendações sociais constituem um dos componentes da percepção social e está sujeita a manipulações que objetivam alterar a confiança final, como o ataque de difamação. Os vários trabalhos que empregam percepção social na IoT consideram diversas técnicas para mitigar o efeito desse ataque. No entanto, as formas de mitigação empregadas são limitadas por serem fixas, necessitarem de coordenação prévia, ou estarem vulneráveis a variações de comportamentos do ataque de difamação.

1.2 OBJETIVOS

Esta dissertação tem como objetivo desenvolver um modelo de Sistema de Autenticação Adaptativa que incorpora múltiplas percepções sociais de modo a prover uma seleção robusta do mecanismo de autenticação adequado aos diferentes ambientes de redes IoT. Além disso, ele deve ser resiliente contra ataques que venham a manipular os dados sociais trocados entre os dispositivos, bem como adequar-se às restrições dos dispositivos em que ele executa. Para atingir o objetivo geral proposto, os seguinte objetivos específicos foram estabelecidos:

- Determinar os fatores e as técnicas de adaptação nos SAAs para IoT e sua adequação para os ambientes de rede não estruturados e dinâmicos, além das suas limitações.
- Investigar como a percepção social tem sido empregada na IoT e determinar sua aptidão para ser utilizada como fator de adaptação em SAAs.

- Propor uma solução de gestão de autenticação assertiva na avaliação do comportamento dos dispositivos IoT vizinhos a fim de empregar o modelo de autenticação adequado ao contexto ambiental e ao mesmo tempo robusta contra ataques que manipulam os fatores de adaptação.

1.3 CONTRIBUIÇÕES

O desenvolvimento dessa dissertação resultou em contribuições científicas na área da computação, com ênfase em redes sem fio estruturadas e segurança de redes e na avaliação das relações sociais entre os dispositivos. A seguir as contribuições estão descritas de forma detalhada:

- *Um levantamento sobre o estado da arte:* Foi realizado um estudo, classificação e discussão sobre as técnicas de autenticação adaptativa para redes IoT. Além disso, realizou-se uma classificação e discussão sobre como a confiança social tem sido utilizada na IoT. Finalmente, determinou-se os mecanismos que os trabalhos sobre percepção social empregam para mitigar ataques que visam manipular a confiança.
- *Proposição e Avaliação de um SAA:* Foi proposto o SAA GALENA que baseia-se no uso de políticas para adaptação e emprega a percepção social e do ambiente como fatores para adaptação. Ele permite determinar o mecanismo de autenticação adequado a uma interação. Ele mostra-se resiliente contra ataques de difamação na rede, um tipo de ataque de manipulação dos dados sociais, que visa alterar as recomendações sociais empregadas pelo sistema. Além disso, realizou-se uma análise e discussão sobre o desempenho do GALENA através de simulações da eficiência na adaptação do mecanismo de autenticação considerando cenários com dispositivos pessoais trocando serviços entre eles e que suportam diferentes mecanismos de autenticação. Também avaliou-se sua eficácia na mitigação de vários comportamentos do ataque de difamação.

1.4 ESTRUTURA DA DISSERTAÇÃO

Esta dissertação está organizada em seis capítulos. O Capítulo 2 apresenta os fundamentos relacionados a Internet das Coisas e Internet das Coisas Sociais. Ainda, ele traz a definição de confiança nas redes IoT e os ataques a que ela está sujeita. O Capítulo 3 discute os trabalhos sobre autenticação adaptativa na IoT e os trabalhos que tratam do gerenciamento de confiança. Em seguida, o Capítulo 4 descreve o sistema proposto, GALENA, e o seu funcionamento. O Capítulo 5 descreve o processo de avaliação do sistema, detalhando os cenários de avaliação e as métricas selecionadas para mensuração do resultado. Por fim, o Capítulo 6 conclui essa dissertação com as considerações finais e as possibilidades de trabalhos futuros.

2 FUNDAMENTOS

Este capítulo descreve os principais fundamentos necessários à compreensão do contexto da pesquisa do problema. A Seção 2.1 apresenta as características das redes IoT, domínios de aplicação e arquitetura. A Seção 2.2 detalha o funcionamento do serviço de autenticação. A Seção 2.3 descreve o paradigma da Internet das Coisas Sociais como arquitetura de rede. Já a Seção 2.4 caracteriza os ataques que podem ocorrer nessa arquitetura. Ainda, a Seção 2.5 apresenta o uso de políticas no contexto de gerenciamento da IoT. Por fim, a Seção 2.6 define o conceito de a *Data Provenance* e os benefícios ao provimento de sistemas seguros.

2.1 INTERNET DAS COISAS

A interconexão de objetos computacionais ao nosso redor e da Internet ocasionou o surgimento da Internet das Coisas (IoT). Esses dispositivos estão inseridos nos mais variados ambientes humanos e urbanos, colaborando em diversos domínios de aplicação, visando aumentar a qualidade de vida de seus habitantes (Gardašević et al., 2016). Por sua ubiquidade é esperado que eles tenham reflexo na economia, gerando um impacto econômico de até 11 trilhões de dólares por ano em 2025 (McKinsey, 2015). O termo “Internet das Coisas” foi cunhado por Kevin Ashton, pesquisador do *Massachusetts Institute of Technology* - MIT em 1999 (Ashton et al., 2009) sua definição da IoT era de uma coleção de objetos interoperáveis e identificáveis de maneira única e interligados através da tecnologia RFID (Identificação por Radiofrequência, do inglês *Radio-Frequency Identification*). Essa definição evolui e engloba todos os objetos – daí denominados Coisas – que coletam informações e estabelecem comunicação entre si, que denominam-se objetos inteligentes. Esses objetos são equipados com sensores, atuadores, capacidade de processamento e de comunicação, além de uma fonte de energia. Entretanto, esses objetos têm sofrido com restrições de energia e processamento (Gardašević et al., 2016; Atzori et al., 2010). A rede IoT é intrinsecamente heterogênea dada a variedade de dispositivos existentes. Além disso, sua interconexão permite que eles prestem serviços personalizados que variam de simples medições de parâmetros ambientais – como iluminação, umidade, etc – até o gerenciamento automatizado de procedimentos logísticos e da produção industrial.

Os variados serviços da IoT são agrupados em *Domínios de Aplicação* que ditam o objetivo dessas aplicações como *Smart city*, *Smart Agriculture*, *Intelligent Transportation Systems* e outras. Na *Smart City* (Cidade Inteligente) as soluções IoT são voltadas a melhora do dia-a-dia urbano. Na *Smart Health* – área médica e de saúde – o objetivo da IoT é o monitoramento remoto e a prevenção de situações críticas. Na *Smart Agriculture* (Agricultura Inteligente) a IoT trabalha melhorando o gerenciamento de fazendas e a utilização de recursos existentes. Nos *Intelligent transportation systems* (Sistemas de Transporte Inteligente – ITS), a IoT coopera na maior eficiência e segurança dos sistemas de transporte. Esses e outros domínios de aplicação serão detalhados na Subseção 2.1.2.

No entanto, a troca de serviços exige que os dispositivos comuniquem-se entre si empregando as tecnologias e os protocolos adequados as limitações que eles apresentam. A comunicação sem fio ocorre utilizando-se protocolos padrões como o protocolo IEEE (do inglês, *Institute of Electrical and Electronics Engineers*) 802.11, também conhecido como Wi-Fi; Protocolos de baixa energia como o 802.15.1 – *Bluetooth* – e o protocolo 802.15.4 – que define redes sem fio pessoais de baixa taxa de transmissão (do inglês, *Wireless Personal Area Network* – WPAN) – também são utilizados. Além disso, são utilizados protocolos como o IPv6 (*Internet*

Protocol v6), UDP (*User Datagram Protocol*), entre outros (Al-Fuqaha et al., 2015). Porém, com a diversidade de protocolos disponíveis demanda que eles sejam categorizados em uma arquitetura, que será detalhada na próxima subseção.

2.1.1 Modelos de Arquiteturas

Não há um modelo de arquitetura padrão para a IoT, porém a necessidade de uma arquitetura aberta, flexível e baseada em camadas tem sido detectada (Gardašević et al., 2016; Al-Fuqaha et al., 2015). A literatura oferece alguns modelos, onde destacam-se os modelos de três e cinco camadas, detalhados na Figura 2.1. O modelo de três camadas apresenta as camadas de percepção, de rede e de aplicação. A camada de percepção engloba os sensores e atuadores existentes no dispositivo IoT. A camada de rede é responsável por disseminar e transmitir os dados, e é aqui onde se inserem os protocolos de comunicação. Por fim, a camada de aplicação responsabiliza-se por interpretar os dados coletados de acordo com o domínio de aplicação no qual o dispositivo está inserido. A arquitetura de cinco camadas divide a IoT em camada de Objetos, Abstração de Objetos, Gerência de Serviços, Aplicação e Negócio. A camada Objeto representa os sensores e atuadores dos dispositivos. A camada de abstração transfere os dados produzidos pelos Objetos para a camada de Serviço. Nessa camada, as requisições e os dados recebidos são processados e os serviços requeridos são prestados. A camada de Aplicação provê o serviço solicitado ao usuário e depende do domínio de aplicação que o dispositivo está inserido. Por fim, a camada de Negócio faz a gerência de toda a rede e dos serviços oferecidos.

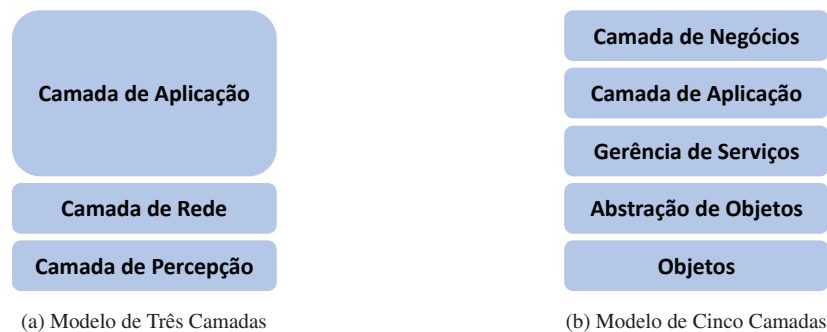


Figura 2.1: Arquiteturas propostas para IoT

2.1.2 Domínios de Aplicação

As redes IoT podem ser aplicadas em diversos domínios com o objetivo de melhorar a execução de tarefas, auxiliar a tomada de decisão, entre outros. Esses domínios estão ligados com áreas como cidades inteligentes, saúde, logística, indústria, etc. O uso da IoT nessas áreas viabiliza novos serviços e produtos. A seguir detalhamos alguns domínios de aplicação.

Smart City: Nessa aplicação, as soluções IoT visam aumentar a qualidade de vida dos ambientes urbanos provendo uma variedade de serviços. Esses serviços são subdivisões das cidades inteligentes e envolvem transporte inteligente, controle inteligente do tráfego, de casas, etc. Os dispositivos comunicam-se uns com os outros diretamente – comunicação denominada Máquina-a-Máquina (M2M) – e são acessíveis diretamente (Gardašević et al., 2016). Um exemplo de cidade inteligente é a cidade de Santander, na Itália (Marche et al., 2020, 2018).

eHealth/Smart Health: Esse domínio de aplicação engloba aplicações médicas e de saúde e promove o monitoramento em tempo real, a prevenção de condições críticas, a administração automática de remédios, etc. Os dispositivos IoT dessa aplicação permitem monitorar dados

como batimento cardíaco, pressão sanguínea, saturação de oxigênio, etc. O monitoramento permite que paciente e médico possam se consultar a distância e permitem que a equipe médica e familiares tenham informações prontamente disponíveis (Qin et al., 2020).

Smart Industry: Nesse domínio a IoT, amplia melhora a gerência dos equipamentos e processos. Na linha de produção as máquinas tornam-se inteligentes e podem verificar autonomamente a presença de problemas e a necessidade de manutenção. Além disso, permitem a gestão automatizada da cadeia de suprimentos (Qin et al., 2020; Bahga e Madiseti, 2016).

2.2 SERVIÇO DE AUTENTICAÇÃO

A autenticação é um dos serviços necessários ao funcionamento seguro das redes IoT. A autenticação consiste do processo no qual um atributo intrínseco de um dispositivo é verificado, comumente a sua identificação (El-hajj et al., 2019). Na literatura diversos mecanismos de autenticação foram propostos para a IoT (Arias-Cabarcos et al., 2019; Malik et al., 2019; Ferrag et al., 2017), sendo necessário que o dispositivo seja dotado de uma variedade de mecanismos de autenticação para requisitar serviços nos mais variados pontos da rede que suportarão diferentes mecanismos. Além disso, o dispositivo poderia utilizar um mecanismo de autenticação menos complexo computacionalmente com dispositivos os quais ele já tenha alguma relação de confiança e em contextos considerados seguros. A adequação aos contextos e seus dispositivos, portanto, gera uma economia de recursos do dispositivo IoT, a medida que muitos mecanismos são complexos e demandam gastos de energia e processamento.

Desta forma, surgiu a necessidade de que os dispositivos possam selecionar *adaptativamente* os mecanismos adequados em cada interação. Assim, os sistemas auto-adaptativos se especializaram no campo dos sistemas de autenticação, gerando os sistemas de autenticação adaptativos (Arias-Cabarcos et al., 2019). Esses sistemas utilizam entradas, denominadas fatores, para realizar a escolha do mecanismo de autenticação a ser aplicado. Os fatores podem ser fatores contextuais, como a localização do usuário, comportamentais, como o padrão de movimentação ou uso do dispositivo, percepção de risco, entre outros. Desse modo, o dispositivo IoT seria capaz de manter a comunicação segura e com gasto de recursos adequado a situação que ele se encontra num dado momento e local.

2.3 INTERNET DAS COISAS SOCIAIS

A Internet das Coisas Sociais – *SIoT* (do inglês Social Internet of Things) é um paradigma de organização de rede proposto por Atzori et al. (2012). Esse paradigma nasceu da junção dos conceitos de Internet das Coisas e Redes Sociais e torna-se importante quando os dispositivos IoT são autônomos. Esse paradigma permite, também, que teorias já aplicadas no campo das relações sociais humanas também seja aplicado em sua análise. Ainda, os dispositivos herdam de seus donos certas características sociais, porém, eles também as criam e mantêm autonomamente. E, dessa forma, criam uma “inteligência social” nessa rede que é utilizada para navegação na sua estrutura, descoberta e composição de serviços, fazendo com que a rede SIoT seja uma rede orientada a serviços (do inglês, *Service Oriented Architecture* – SOA).

O paradigma SIoT propõe cinco principais relações que os objetos podem criar entre si (Atzori et al., 2012) mas que permitem que outras relações também sejam derivadas delas. A forma de representação dessas relações é um grafo do tipo estrela, onde o dispositivo central mantém as relações com os dispositivos nas pontas. Duas relações são próximas entre si, a relação *Co-location object relationship* (Relacionamento por co-localização – C-LOR) e *Co-work object relationship* (Relacionamento por cooperação de trabalho – C-WOR). Essas duas relações

são criadas quando os dispositivos constantemente ficam na presença um do outro e ocorrem principalmente entre objetos que são estáticos. A relação C-WOR ocorre quando, além de estarem em contato entre si, os dispositivos também cooperam para oferecer um mesmo serviço.

A relação *Ownership Object Relationship* (Relacionamento por propriedade – OOR) ocorre entre objetos heterogêneos que pertencem a um mesmo dono, como computadores, *tablets* e *smartphones*. Já a relação *Parental Object Relationship* (Relacionamento por Semelhança – POR) ocorre em objetos homogêneos, como aqueles de mesmo fabricante e produzidos em um mesmo espaço de tempo. Finalmente, a relação *Social Object Relationship* (Relação social – SOR) é a relação que é criada quando os dispositivos entram em contato, esporádica ou continuamente.

2.3.1 Confiança social

O paradigma de SIoT traz consigo também o conceito de confiança, mais precisamente confiança social. O conceito de confiança é definido de maneira diferente para cada área (Cho et al., 2015), entretanto algumas definições são comuns. Dois objetos estabelecem uma relação de confiança entre si, um deles assume o papel de *trustor* (fiduciante) – aquele que confia – e o outro objeto assume o papel de *trustee* (fiduciário) – aquele em quem se confia. O *trustor* emprega um processo para avaliar a confiança que ele tem sobre o objeto *trustee*, estabelecendo um valor para essa relação. Pode-se dizer então que esse valor é a confiança percebida pelo *trustor* em relação as interações e comportamento do *trustee*. Ainda, durante o processo de estabelecimento da confiança, o *trustor* pode escolher utilizar a confiança indireta, ou reputação. Ela é obtida através da experiência direta de outros objetos, ou seja, percebida por eles, sobre o *trustee*. Esses objetos, ao enviar a confiança que eles têm sobre o objeto que está sendo avaliado, enviam recomendações. Ou seja, a recomendação é a forma com que a reputação é compartilhada.

A confiança social é uma categoria de confiança que deriva das relações sociais. Utiliza-se não somente as relações sociais descritas acima, como também outros atributos, como centralidade – que mede a importância de um objeto em uma rede, a conectividade – que mede quão um objeto está conectado, a similaridade – ou semelhança entre dois objetos, etc (Aalibagi et al., 2019; Cho et al., 2015; Bao e Chen, 2012) que são derivados daquelas relações através da utilização de algoritmos sobre o grafo que as representam. À confiança determinada através de atributos ou características sociais, dá-se o nome de confiança social.

Essas duas confianças subsidiam a tomada de decisão em diversas aplicações IoT, visto que elas levam em conta o contexto heterogêneo e a restrição de recursos. A confiança tem sido empregada principalmente no controle de acesso (Gwak et al., 2018; Bernabe et al., 2015), composição de serviços (Al-Hamadi et al., 2019; Bao e Chen, 2012), segurança (Khan et al., 2017; Kowshalya e Valarmathi, 2018) e roteamento (Hellaoui et al., 2016). No entanto, não se tem explorado a sua utilização como fator de autenticação em sistemas de autenticação adaptativos.

2.4 ATAQUES CONTRA A CONFIANÇA

O emprego de confiança como recurso para subsidiar a tomada de decisão nos sistemas, torna-os vulneráveis a ataques que visam alterar de forma maliciosa a confiança percebida sobre um dispositivo. Isso pode causar diversas consequências ao funcionamento usual da rede IoT, visto que o ator malicioso pode utilizar este ataque como ataque inicial e, a partir dele, efetuar outros tipos de ataques ou até mesmo efetuar ataques em conjunto. Os principais ataques que influem na confiança são o ataque de autopromoção (*Self-promoting*), de boa recomendação (*Good mouthing*), de má-recomendação ou difamação (*Badmouthing*), o ataque *Ballot-stuffing* e o ataque de *Whitewashing* (Chen et al., 2016); e esses ataques podem ocorrer tanto em rede estruturadas quanto não estruturadas.

A consequência desses ataques são variadas e dependem do processo que utiliza a confiança. No controle de acesso, em especial, a dispositivo-alvo do ataque pode não conseguir se conectar à rede ou ser forçado a se desconectar por causa de sua baixa confiança. Ainda, na composição de serviços, o alvo pode sofrer uma negação de serviço. Já no roteamento, o dispositivo-alvo pode não rotear pacotes ou necessitar autenticar todos os pacotes recebidos. Assim, os sistemas que utilizem confiança devem estar cientes desses ataques para serem resilientes a eles, ou contar com mecanismos de mitigação. A seguir, os ataques citados são explicados, em conjunto com o comportamento do atacante e a consequência do ataque.

- *Self-promoting* (Auto de Promoção): O ataque de autopromoção é um ataque no qual o atacante e o dispositivo-alvo são o mesmo dispositivo. O objetivo do atacante é aumentar sua importância a fim de ser selecionado como provedor de serviço. O ataque ocorre quando o atacante emite boas recomendações sobre si. Quando ele é selecionado como provedor de serviço ele então provê serviço defeituoso. Desse modo ele perturba o funcionamento da rede IoT e pode desestabilizá-la (Chen et al., 2016). Ainda, quando escolhido como provedor de serviço, ele pode realizar outros ataques que não sejam contra a confiança.
- *Good mouthing* (Ataque de Boa Recomendação): O ataque de boa recomendação é semelhante ao ataque de autopromoção por também aumentar a influência e confiança sobre um dispositivo-alvo, porém, o alvo é um outro dispositivo. O atacante emite então uma recomendação com valor de confiança maior do seria a confiança real (Suryani et al., 2018). Para que esse ataque ocorra, os dois dispositivos, o atacante e o dispositivo-alvo, devem trabalhar em conjunto. As consequências desse ataque são também semelhantes às do ataque de autopromoção, mal funcionamento da rede.
- *Ballot-stuffing*: Nessa classe de ataque, um grupo de atacantes age de forma coordenada, ou seja em conluio. Assim, eles podem aumentar ou diminuir a confiança sobre um alvo de maneira mais efetiva pois disporão de mais recomendações maliciosas na rede (Chen et al., 2016; Bao e Chen, 2012). As consequências são as mesmas do ataque de difamação e de boa recomendação, porém elas ocorrem de forma mais dramática, dada a quantidade de atacantes.
- *Whitewashing*: Com o *whitewashing*, o atacante visa ter sua reputação frente aos outros nós reiniciada. Para isso ele sai e entra na rede diversas vezes, e também em localizações diferentes, de modo que sua má reputação seja esquecida ou lavada, daí o nome do ataque (Chen et al., 2016; Cho et al., 2015). O atacante pode realizar também esse ataque em conjunto com outros ataques, como o de falsificação de identidades – o ataque *Sybil*, de modo que a reputação não seja ligada a sua identidade real. A consequência desse ataque é a permanência do atacante na rede com a possibilidade ataques subsequentes.
- *Badmouthing* (Ataque de Difamação/Má-Recomendação): O ataque de má-recomendação – ou ainda, difamação – pelo contrário, visa diminuir a reputação de um dispositivo-alvo. Nesse tipo de ataque, somente o atacante se comporta de forma maliciosa. A difamação ocorre quando o atacante emite – de forma contínua ou intermitente, ou, ainda, associado a outros ataques como o *Sybil* – uma recomendação sobre o alvo menor do que a confiança real. Dessa forma, a confiança percebida dos outros nós sobre o alvo é diminuída. Assim, o dispositivo requisitante pode sofrer uma negação de serviço. Ainda, outra consequência possível é a exclusão ou isolamento do dispositivo alvo da rede devido a sua baixa reputação (Reddy et al., 2019). Com o

isolamento do dispositivo alvo, o dispositivo atacante pode vir a tomar o lugar dele na rede, oferecendo serviços e possibilitando outros ataques. Guo et al. (2017) aponta que esse é um dos mais comuns tipos de ataque contra confiança. Ainda, ele aponta que a utilização de confiança social é um dos meios para se defender contra esse tipo de ataque.

2.5 POLÍTICAS

Uma política é um método de ação para apoiar decisões, que são aplicadas em um contexto específico, e.g. políticas em determinada unidade organizacional de uma empresa; Ou as políticas são um conjunto de regras para gerenciar e controlar o acesso a recursos de rede (Waldbusser et al., 2001). Uma política é definida como um conjunto de condições e ações, no qual as ações são realizadas quanto as condições forem atingidas. As políticas também passam por um processo de abstração, pois precisam ser especificadas, utilizando-se a linguagem comum ou linguagens de domínio específico, para posteriormente serem traduzidas para o ambiente em que serão implantadas. Nas redes IoT, as políticas têm sido presentes para seu gerenciamento (Katsikogiannis et al., 2018; Li et al., 2018; Fedrecheski et al., 2019; Silva et al., 2018), principalmente no controle de acesso. E, pela sua simplicidade, permitem que dispositivos IoT com restrições possam avaliá-las e serem gerenciados.

Segundo Waldbusser et al. (2001), um mecanismo que utilize políticas tem quatro entidades principais, a primeira delas é o Ponto de Administração de Políticas (do inglês, *Policy Administration Point* - PAP), que permite o gerenciamento das políticas. Já, o Ponto de Informação de Políticas (do inglês, *Policy Information Point* - PIP) provê atributos para a tomada de decisão relacionado a uma política. A entidade Ponto de Decisão de Políticas (do inglês, *Policy Decision Point* - PDP) recebe os atributos da PIP e com base neles seleciona uma política do repositório de políticas. Finalmente, o PDP repassa a decisão para o Ponto de Aplicação de Políticas (do inglês, *Policy Enforcement Point* - PEP).

Essas quatro entidades cooperam para que as políticas sejam realizadas. O PAP permite ao gerente da rede configurar nos dispositivos (ou sistemas) as políticas desejadas. Para isso as políticas utilizam dados de entrada, que são subsidiados pelos PIPs. O PDP efetivamente aplica as políticas ou avalia e determina a ação a ser tomada. De posse do resultado, o PEP faz a aplicação e força o cumprimento da ação determinada. Desse modo, um sistema ao empregar políticas pode alterar suas configurações ou avaliar o controle de acesso de maneira dinâmica.

2.6 DATA PROVENANCE

O conceito de *Data Provenance* (proveniência de dados) tem sido aplicado, principalmente, em sistemas médicos e de banco de dados (Elkhodr e Mufti, 2019). As técnicas de proveniência visam atestar, de forma inequívoca, características de um dado como seu histórico de alteração, incluindo o responsável, origem e caminho de processamento, além de registros de data e hora de todas as alterações. Para isso, esses sistemas utilizam técnicas que permitem que tanto os dados das aplicações quanto os dados de proveniência sejam armazenados de forma que sua edição ou deleção não ocorra.

A proveniência de dados divide-se em três processos: *Captura*, *Gerenciamento* e *Análise*. A captura engloba os processos que capturam e geram os eventos de proveniência. Já o Gerenciamento visa reduzir o tamanho dos dados capturados e otimizar a performance em consultas. Por fim, a Análise visa interpretar os dados obtidos e correlacioná-los com os eventos e entidades do sistema (Alam e Wang, 2021). Na IoT, usualmente emprega-se a Data Provenance

para a auditoria do caminho da informação e para ajudar a determinar falhas de segurança. As técnicas como *hashing*, assinatura digital e códigos de verificação autenticados (HMAC) (Alam e Wang, 2021; Pasquier et al., 2018) contribuem para a realização dos objetivos da IoT, pois garantem características como integridade e origem dos dados trafegados na rede (Elkhodr e Mufti, 2019; Jaigirdar et al., 2019; Suhail et al., 2017). Além disso, a depender das características da rede, podem garantir também a confidencialidade dos dados. As técnicas *Data Provenance* auxiliam, também, na formação de confiança entre os dispositivos IoT. Logo, a identificação de cada dispositivo deve ser única, tal que as informações de proveniência sejam corretamente relacionadas com o dispositivo que originou o dado (Suhail et al., 2017) e, assim, a relação de confiança seja corretamente criada. Desse modo, o conceito de *Data Provenance* auxilia na manutenção da segurança e funcionamento da rede IoT.

2.7 RESUMO

Este capítulo apresentou os fundamentos sobre Internet das Coisas, sua arquitetura, tecnologias que possibilitam sua execução. Foi descrito também o funcionamento da autenticação no contexto de IoT. Ainda, mostrou-se como a confiança é utilizada na IoT e os ataques a que ela está sujeita. Foi descrita também a utilização de políticas como ferramenta de gerenciamento das redes e dispositivos IoT. Por fim, detalhou-se o conceito de *Data Provenance* para suportar o funcionamento dos serviços dessa rede.

3 TÉCNICAS DE AUTENTICAÇÃO ADAPTATIVA E SISTEMAS DE GERENCIAMENTO DE CONFIANÇA SOCIAL NA IOT

Este capítulo apresenta a revisão da literatura acerca das técnicas da autenticação adaptativa e do uso de confiança social e não social na Internet das Coisas. A Seção 3.1 destaca e discorre sobre o estado da arte da autenticação adaptativa. A Seção 3.2 introduz e discute os trabalhos que tratam do gerenciamento da confiança na Internet das Coisas.

3.1 AUTENTICAÇÃO ADAPTATIVA

A autenticação adaptativa permite que um sistema dinamicamente selecione os melhores mecanismos para confirmar a identidade de um usuário ou dispositivo baseado em diversos fatores, como contexto, risco e comportamento (Arias-Cabarcos et al., 2019). Além de perceber a mudança nesses fatores, o sistema deve determinar a natureza da mudança – conforme a percepção do risco – e efetivamente adaptar-se à mudança, alterando o mecanismo de autenticação empregado, assim como rejeitando a autenticação e, portanto, não permitindo o acesso. Os sistemas de autenticação adaptativa (SAAs), de um modo geral, diferenciam-se pela técnica utilizada para adaptarem-se, podendo ser classificados em técnicas baseadas em *aprendizado de máquina* (ML), *teoria dos jogos*, *políticas* e *ontologias*. A seguir, destacam-se os trabalhos que aplicam cada uma dessas técnicas e, ao final, sumariza-se suas complexidades, fatores de adaptação e organização na Tabela 3.2. A descrição da metodologia do levantamento bibliográfico aplicado nesta pesquisa, com as strings de busca, critérios de inclusão e exclusão, encontram-se no Apêndice A.

3.1.1 Baseada em Aprendizagem de Máquina

Os sistemas que empregam a técnica de aprendizado de máquina levam em conta o comportamento do dispositivo, bem como do usuário, e seu contexto. Inicialmente, esses sistemas aprendem o comportamento usual do dispositivo, e em seguida empregam uma técnica de ML para detectar a natureza da mudança e determinar a adaptação necessária. A seguir são descritos os principais trabalhos que empregam ML para SAAs visto que são os mais representativos quando fala-se de diversidade de organização. Em Hintze et al. (2019), os autores propuseram o sistema CORMORANT para autenticação adaptativa usuário-para-máquina. Este sistema emprega diversos fatores como entrada, tais como a maneira de andar e digitar do usuário, sua senha e a proximidade entre os dispositivos. Ainda, o sistema leva em conta diversos equipamentos que o usuário possui para realizar a autenticação entre dispositivos de maneira autônoma e não-supervisionada.

O CORMORANT emprega a técnica de aprendizado de máquina para determinar se a mudança nos fatores corresponde ao padrão de uso do usuário autorizado. Ele executa em todos os dispositivos do usuário, de maneira que cada um possa avaliar isoladamente e autonomamente a mudança no fator de entrada específico e também se comunicar com os outros dispositivos para receber a avaliação deles quanto à mudança observada nos padrões. Se determinado que o usuário que está acessando não é o usuário autorizado, ou ainda, se os dispositivos se deixarem a proximidade uns dos outros o CORMORANT, então, aumenta o nível de segurança requerido. Um exemplo de aumento seria passar a exigir o uso de PIN e anteriormente autenticar implicitamente. Apesar de reconhecer a percepção de posse de dispositivos pelo usuário, que

pode ser transposta para o paradigma de SIoT, o CORMORANT não utiliza fatores sociais para a autenticação adaptativa, o que permitiria que a avaliação da mudança dos fatores ocorresse de forma mais otimizada para dispositivos IoT.

Em Gebrie e Abie (2017), os autores propuseram um sistema de autenticação baseado na percepção de risco. O sistema é treinado com padrões de utilização do usuário e dos dispositivos para classificar as atividades como normais, suspeitas, anormais e críticas. A medida que o uso desvia do normal e o risco aumenta, o sistema adaptativamente demanda que o usuário ou dispositivo aplique um método de autenticação diferente e, opcionalmente, com complexidade diferente da atual. Não somente o método de autenticação pode ser alterado, como também a frequência da (re-)autenticação e, caso o sistema determine que o risco esteja no patamar mais alto, ele pode rejeitar a possibilidade do dispositivo autenticar-se, para tentar evitar a troca de informações nesse cenário. O sistema proposto emprega quatro características para definir o comportamento de um dispositivo: o Indicador de Potência do Sinal Recebido (do inglês, *Received Signal Strength Indication* – RSSI), o ganho do canal de comunicação, a assinatura temporal do canal e as diferenças na frequência utilizando o efeito doppler. O sistema trata da autenticação do sensor para o dispositivo gateway, limitando que a avaliação a esse dispositivo, que teria mais recursos para lidar com a tarefa de ML. A proposta dos autores aparenta-se incipiente e não detalha como as características são reconhecidas e classificadas. Além disso, o sistema mostra-se limitado, pois não considera a autenticação gateway–dispositivo.

Em Hayashi et al. (2013), os autores propuseram o sistema CASA (*Context-Aware Scalable Authentication*) para autenticação escalável usuário–dispositivo, que emprega fatores passivos, que são aqueles que podem ser obtidos sem a interação com o usuário, a fim de modular o método de autenticação ativa como senhas e PINs no dispositivo. O CASA classifica o usuário que tenta o acesso como legítimo ou não e faz a avaliação de risco levando em conta os fatores passivos. Esses fatores, de acordo com os autores, podem ser a localização, características comportamentais e proximidade com dispositivos. Depois, o classificador Naive Bayes faz a escolha do fator ativo de autenticação com base no risco calculado. A efetividade do CASA foi avaliada do ponto de vista da usabilidade percebida pelo usuário e se deu em três ensaios em que foram coletados comentários sobre o sistema. Após a análise dos resultados, os autores agregaram ao protótipo a proximidade de dispositivos como fator passivo a ser considerado. O sistema possui diversas fragilidades reconhecidas pelos autores, sendo uma delas a baixa quantidade de fatores considerados e um modelo de usuário muito simples. O modelo que um atacante pode assumir (modelo adversarial) assumido pelos autores mostra-se limitado, pois não considera ataques por atores que dispõem de recursos computacionais para atacar o CASA.

3.1.2 Baseada em Teoria dos Jogos

A Teoria dos Jogos é uma técnica aplicada para a adaptação de sistemas que pode tomar diversos fatores como entrada e contrabalanceá-los para atingir um equilíbrio. Na Teoria dos Jogos, modela-se matematicamente um conjunto de interações entre atores, visando a tomada de decisão de forma otimizada. A seguir, apresenta-se os trabalhos relevantes que empregam a Teoria dos Jogos para adaptação que demonstram a viabilidade dessa técnica em redes IoT. Em Arfaoui et al. (2018), os autores propuseram um sistema de autenticação adaptativa baseado no risco para redes de área corporal (do inglês *Wireless Body Area Network* - WBAN). Este sistema estima e prediz riscos para implementar as contramedidas necessárias para mitigá-los equilibrando a segurança com a performance da rede. Deriva-se o risco da análise das informações contextuais (característica do canal de comunicação e tráfego) e também da capacidade energética do dispositivo e de memória. Cada uma dessas informações é modelada matematicamente como um processo de decisão de Markov para serem utilizadas pelos jogadores do jogo de otimização.

O sistema pode ou otimizar as contramedidas para cada um dos componentes ou realizá-la de maneira multidimensional. Quando multidimensional, o ponto de equilíbrio de Nash determina o balanceamento entre segurança e impacto no desempenho. Esse equilíbrio ocorre quando a segurança é máxima e o impacto no desempenho torna-se mínimo. A avaliação preliminar dos autores demonstra que o sistema obtém melhor desempenho com o equilíbrio multidimensional em contraste com apenas tentar mitigar o ataque. Embora ofereça um equilíbrio entre segurança e desempenho, a natureza de otimização e a complexidade do sistema o tornam inadequado para dispositivos IoT.

Hamdi e Abie (2014) apresentaram um trabalho de segurança adaptativa também baseado na teoria dos jogos que emprega características como energia, memória e comunicação para modelar o comportamento do dispositivo. Nesse sistema a intrusão é orientada por um modelo Suscetível-Infectado-Recuperado com Manutenção (do inglês, *Susceptible-Infective-Recovered with Maintenance* - SIR-M). Ele traduz como uma intrusão se espalha pela rede através da comunicação entre nós comprometidos e nós sadios e a velocidade com que os nós se recuperam. Aqui, utiliza-se o equilíbrio de Nash para balanço entre segurança e decaimento energético. Porém, as soluções têm que ser Pareto eficientes, a fim de diminuir o campo de probabilidades. Essas soluções caracterizam-se por maximizar as entradas, ou seja, a segurança é tão alta quanto a limitação energética permite. Segundo avaliação preliminar dos autores, o sistema permite que os dispositivos tenham sua vida estendida, demonstrando que ele consegue balancear a segurança com o gasto energético.

Abordagens baseadas em Teoria dos Jogos também têm sido aplicadas em outros tipos de redes, que não puramente IoT. Em Assis et al. (2017), os autores empregaram a teoria dos jogos para mitigar ataques de negação de serviço distribuídos (do inglês *Distributed Denial of Service* - DDoS) em redes definidas por software (do inglês *Software Defined Networking* - SDN). O módulo de mitigação baseado em teoria dos jogos recebe do analisador de rede o comportamento esperado e as conexões suspeitas, permitindo a análise das possíveis ações do atacante e do sistema de defesa para determinar a melhor contramedida de segurança para ser empregada. As ações do atacante, o comportamento esperado e as estratégias de defesa são modelados como um jogo e seu resultado é definido empregando-se o equilíbrio de Nash. Assim que o módulo de mitigação determina a contramedida necessária, o controlador SDN ou o *firewall* de rede aplicam-na.

3.1.3 Baseada em Políticas e Ontologias

As abordagens baseadas em políticas e ontologias têm sido aplicadas como meios simples e leves para o provimento de adaptação na IoT. Além disso, um grupo de ontologias pode, também, ser traduzido para um conjunto de políticas. Desse modo, emprega-se o níveis dos fatores de adaptação analisados como entrada das regras e ontologias, para que proporcionem a adaptação necessária. A seguir apresenta-se os trabalhos mais relevantes que empregam políticas e ontologias para adaptação em IoT. Sylla et al. (2020) propôs um sistema de autenticação para redes IoT baseado na arquitetura como um serviço (do inglês, *as a Service*), a fim de oferecer segurança ciente do contexto. A arquitetura proposta separa o sistema em dois planos – Plano de Conhecimento (do inglês, *Knowledge Plane* - KP) e Plano de Segurança e Privacidade (do inglês, *Security and Privacy Plane* - SPP) – a fim de prover modularidade ao sistema para se encaixar no paradigma “*as a Service*”. O KP obtém o contexto e realiza o cálculo de risco, enquanto o SPP recebe as informações do KP e determina a política de segurança a ser aplicada. A solução dos autores adapta a autenticação com base no contexto e no risco associado a ele, que são determinados e calculados pelos componentes do KP. O sistema determina o contexto de acordo com os dados obtidos dos dispositivos do usuário e avalia o risco de acordo com o modelo

de ataque associado com aquele contexto. De posse desses dados, o Gerenciador de Políticas de Contexto de Segurança (*Context Security Policy Manager – CSMP*) do SPP resgata da base que armazena as políticas aquela que deve ser aplicada e a repassa para o componente responsável por aplicá-la. As políticas ditam, para o dispositivo IoT, quais ações ou mecanismos que o dispositivo deve utilizar a fim de atingir o nível de segurança necessário para o contexto. Por se tratar de um sistema “*as a service*”, sua arquitetura é centralizada, o que pode comprometer sua escalabilidade em cenários que apresentam grande quantidade de dispositivos. Além disso, como a transferência do contexto entre os dispositivos emprega criptografia simétrica, ela depende de um pré-registro dos dispositivos participantes da rede.

Farris et al. (2017) propuseram um framework adaptativo para proteção de redes IoT com arquitetura SDN e seus dispositivos através da implantação de contramedidas de segurança. O framework divide-se em dois planos, sendo um Plano de Orquestração de Segurança (*Security Orchestration Plane – SOP*), que interpreta as políticas e determina as contramedidas associadas, monitora e analisa os dados de comportamento da rede, e um Plano de Imposição de Segurança (*Policy Enforcement Plane – PEP*), onde se localizam os dispositivos, seus controladores e a camada de gerência da rede SDN. O componente central do SOP é o orquestrador de segurança que recebe os dados em tempo real da rede dos dispositivos virtuais e físicos, oriundos do componente de monitoramento e análise. O orquestrador também é responsável por aplicar as políticas e dirigir a implantação das contramedidas, que podem ser tanto a mudança de configuração em dispositivos, quanto a composição de funções virtuais de rede (do inglês *Virtual Network Functions – VNF*). Assim como a proposta anterior, esse framework tem alto nível de centralização, principalmente pela sua arquitetura baseada em SDN, podendo apresentar problemas de escalabilidade. Também, não é adequado para redes baseadas em serviços e com grande quantidade de dispositivos autônomos pois necessita que todos os dispositivos tenham um administrador comum, o que não ocorre em redes baseadas em serviços.

Um conjunto de ontologias pode, eventualmente, ser traduzida para um conjunto de políticas. As ontologias representam os objetos, suas propriedades e relações, a fim de especificar um determinado domínio, neste caso o domínio de segurança em IoT. Em Hamme et al. (2018), os autores propuseram um sistema de autenticação multifatorial e baseado em confiança, que também utiliza ontologias para decidir adaptativamente levando em consideração o risco. Em relação à arquitetura, o sistema incorpora o paradigma de autenticação federada e cada participante da federação, seja o Provedor de Serviço (do inglês, *Service Provider – SP*), Provedor de Identidade (IdP) ou o próprio usuário, avalia o nível de confiança dele para os outros, para uma determinada ação, tais como a autenticação propriamente dita e o fornecimento de fatores de autenticação. Avalia-se o risco como a acurácia que um fator de autenticação exibe e o risco influi diretamente na avaliação das ontologias. Caso a acurácia de um fator diminua – seja por estar comprometido, seja por mal funcionamento – abaixo de um limiar, essa redução desencadeia uma situação de não confiança (*distrust*). O sistema determina os fatores de autenticação a ser empregados a partir da avaliação das ontologias, que levam em consideração o risco de cada fator e sua situação de *distrust*, se existir. Essa situação acarreta o não uso daquele fator, levando ao emprego de outros fatores para autenticação. Desse modo, o sistema considera diversos fatores para autenticação de acordo com as regras pre-determinadas nas ontologias. Apesar da aplicação de técnica semelhante à regras, que são leves, o sistema tem problemas de escalabilidade, pois à medida que aumentam as requisições de autenticação ou a complexidade das ontologias, o atraso para autenticação e composição dos fatores de autenticação também se elevam.

Aman e Snekenes (2015) propuseram o sistema EDAS (*Autonomic Event-Driven Adaptive Security*), que emprega ontologias e apoia-se em eventos. Assim como na proposta anterior, o EDAS utiliza a percepção de risco para adaptação. Ele determina o risco com base nos

eventos gerados pelos dispositivos da rede. O EDAS emprega mecanismos de correlação para a análise dos eventos, e, para mitigar falsos positivos e negativos, diversos eventos são analisados em um dado contexto e dentro de um espaço de tempo determinado. O risco é então repassado ao mecanismo de adaptação propriamente dito que emprega ontologias para representar o estado atual da rede e determinar a adaptação necessária a partir do risco percebido. As ontologias são agrupadas em três contextos – de usuário, do dispositivo e da segurança – e captam as preferências do usuário, as capacidades do dispositivo, além de métricas de segurança. Assim que o mecanismo de adaptação recebe um evento de risco, ele o utiliza como parâmetro para avaliar a ontologia e determinar a adaptação necessária ao risco percebido. O EDAS analisa e consome os eventos gerados pelos dispositivos e permite que a adaptação ocorra em tempo real. Além disso, o EDAS leva em conta as capacidades do dispositivo e seu contexto a fim de balancear a segurança contra outras propriedades, tal como a disponibilidade do dispositivo.

3.1.4 Discussão dos Sistemas de Autenticação Adaptativa na IoT

Esta seção apresenta uma discussão do estado-da-arte sobre os sistemas de autenticação adaptativa (SAAs) na IoT, detalhados nas subseções anteriores. Esses trabalhos foram analisados e sumarizados conforme as características vistas na Tabela 3.2. Identificou-se as técnicas de adaptação e os fatores empregados para a adaptação. Em seguida, eles foram analisados diante dos critérios de *adaptação*, *organização* e *percepção empregada para a adaptação*. Os SAAs baseados em Aprendizado de Máquina (ML) determinam o desvio do comportamento normal de um usuário ou um dispositivo, porém as técnicas de aprendizado de máquina empregadas podem não ser adequadas a todos os tipos de dispositivos IoT por causa da complexidade da técnica. Além disso, esses sistemas necessitam de treinamento com um conjunto de dados livre de ataques para determinar o comportamento normal do dispositivo. Os SAAs baseados em Aprendizado de Máquina, como Sánchez et al. (2020) e Fang et al. (2020), empregam técnicas sofisticadas de ML a fim de tornar o sistema mais preciso. Porém uma maior precisão também traz um alto custo de implementação. Além da técnica complexa, alguns desses sistemas também são centralizados e podem sofrer problemas de escalabilidade quando a rede tona-se densa e heterogênea, como ocorre nas aplicações IoT voltadas a serviços. A fim de contornar a inadequação por falta de capacidade, trabalhos como Aman e Kausar (2019) fazem a transferência da computação para a Fog. Esses sistemas falham ao desconsiderar fatores para autenticação, tais como as relações sociais entre os dispositivos, considerando por vezes somente um fator. Alguns trabalhos, como Hintze et al. (2019) e Hayashi et al. (2013), estabelecem um grupo de dispositivos confiáveis a fim de obter dados para autenticação, porém não se utilizam do paradigma da SIoT para construir esse grupo. Da mesma forma, a confiabilidade da comunicação tanto dispositivo-fog quanto intra-grupo não é considerada, exigindo que esses dispositivos sejam pré-autenticados e pré-reconhecidos entre si.

Os SAAs baseados em Teoria dos Jogos caracterizam-se por utilizar valores que podem ser modelados matematicamente, como decaimento energético e padrões de tráfego. Esses trabalhos buscam uma otimização entre a contramedida a ser empregada e fatores intrínsecos do sistemas, como gasto energético, comunicação, entre outros. Portanto, essas abordagens não incorporam outros fatores para adaptação – como sua localização e as relações sociais que podem existir entre os nós – e se restringem a empregar fatores que podem ser modelados matematicamente. Além disso, por sua natureza matemática, a abordagem em teoria dos jogos não pode ser utilizada por todos os tipos de dispositivos IoT, por existirem restrições de capacidade energética e de processamento.

Os SAAs baseados em ontologias mostram-se similares aqueles baseados em políticas, pois as ontologias também podem ser traduzidas para políticas. Porém, a medida que a base

de conhecimento cresce com a adição de limitações ou requerimentos, sua avaliação pode sofrer atrasos, como reconhecido pelos autores de Hamme et al. (2018) e de Aman e Sneekenes (2015). Além disso, o processo de avaliação pode não ser adequado para todos os dispositivos devido a sua complexidade e o espaço para armazenamento da base de conhecimento pode se tornar proibitivo. Já as políticas se apresentam como técnica mais leve e simples, além da facilidade em serem avaliadas e permitirem a segregação das políticas que não dizem respeito a um determinado dispositivo. A arquitetura centralizada das propostas apresenta-se como uma fragilidade, possibilitando um ponto único de falha, além de não abordarem questões como segurança na comunicação e/ou transferência de eventos.

Os trabalhos voltados para as redes SDN, como Tripathy et al. (2018) e da Costa Júnior et al. (2018), também levaram em conta a percepção de risco para se adaptarem; enquanto o trabalho de Park et al. (2016) considerou os recursos requeridos pelo tráfego. Esses trabalhos também se adaptam empregando políticas, que codificam as necessidades de segurança requeridas no momento da avaliação de risco. Porém, justamente por serem baseados na arquitetura SDN, eles mostram-se a redes IoT massivas e voltadas a serviço. Os trabalhos de Hamme et al. (2018) e Aman e Sneekenes (2015) incorporaram características desejáveis em sistemas voltados para a IoT, tais como a avaliação do contexto e a percepção de confiança. Além disso, outros trabalhos dessa seção também consideram a percepção da capacidade de cada dispositivo a fim de balancear a ação a ser tomada. Porém, esses trabalhos desconsideram fatores para a adaptação, como características sociais, e a necessidade de tomada de decisão autônoma.

Tabela 3.1: Requisitos necessários para os SAAs

Trabalhos de Autenticação Adaptativa na IoT	Fator de Adaptação	Disponibilidade	Autônomo	Descentralizado	Escalável	Integridade
(Aman e Sneekenes, 2015)	Risco	✓	✓			
(Hamme et al., 2018)	Risco	✓	✓	✓	✓	
(Farris et al., 2017)	Comportamento	✓				✓ CoAP-EAP/DTLS-PSK
(Sylla et al., 2020)	Contexto/Risco	✓	✓			✓ PSK

A análise do estado-da-arte sobre os Sistemas de Autenticação Adaptativa em IoT demonstrou que o cenário atual, no qual as redes são dinâmicas e os dispositivos apresentam mobilidade, demanda soluções de segurança distintas daquelas tradicionalmente empregadas nas redes existentes para garantir sua segurança. A mobilidade dos dispositivos IoT, no entanto, impõe restrições quanto a localização, a entrada e saída de dispositivos, bem como as mudanças de ambientes, dificultando que métodos tradicionais de autenticação ocorram adaptativamente nas redes IoT (El-hajj et al., 2019). Com base nos desafios e restrições descritos acima, exemplifica-se os requisitos necessários aos SAAs, elencados na Tabela 3.1, com trabalhos selecionados da literatura. Nesse contexto, os SAAs que utilizam mais de um fator, inclusive aqueles derivados das relações estabelecidas entre os dispositivos, como veremos na Seção 3.2, mostram-se promissores, pois permitem que um dispositivo adapte-se conforme ele se desloca pela rede e ainda sim seja capaz de ter um nível de segurança adequado.

Tabela 3.2: Resumo dos trabalhos de autenticação adaptativa

Trabalho	Técnica	Complexidade	Fatores	Organização	Rede
(Sánchez et al., 2020)	Aprendizado de Máquina	Alta	Comportamento		Internet
(Fang et al., 2020)	Aprendizado de Máquina	Alta	Risco		IoT
(Hintze et al., 2019)	Aprendizado de Máquina	Alta	Comportamento Contexto	Descentralizado	IoT
(Aman e Kausar, 2019)	Aprendizado de Máquina	Alta	Contexto	Centralizado Distribuído	IoT
(Gebrie e Abie, 2017)	Aprendizado de Máquina	Alta	Contexto Comportamento Risco	Centralizado	IoT
(Hayashi et al., 2013)	Aprendizado de Máquina	Alta	Contexto	Centralizado	IoT
(Tripathy et al., 2018)	Políticas	Baixa	Risco	Centralizado	SDN-IoT
(da Costa Júnior et al., 2018)	Políticas	Baixa	Risco	Centralizado	SDN-IoT
(Farris et al., 2017)	Políticas	Baixa	Comportamento	Centralizado	SDN-IoT
(Hamme et al., 2018)	Políticas	Baixa	Contexto Risco		IoT
(Park et al., 2016)	Políticas	Baixa	Recurso	Centralizado	SDN
(Aman e Snekenes, 2015)	Políticas	Baixa	Risco	Centralizado Distribuído	IoT
(Arfaoui et al., 2018)	Teoria dos Jogos	Média	Contexto Energia	Descentralizado	IoT
(Assis et al., 2017)	Teoria dos Jogos	Média	Comportamento	Centralizado	IoT
(Hamdi e Abie, 2014)	Teoria dos Jogos	Média	Contexto Energia	Descentralizado	IoT

3.2 GERENCIAMENTO DE CONFIANÇA

A literatura apresenta uma variedade de trabalhos focados no gerenciamento da confiança para a Internet das Coisas (Ud Din et al., 2019). Esta seção destaca as propostas associadas a esta pesquisa, que empregam características sociais como *sociabilidade*, *amizade* e *centralidade* na gerência da confiança a fim de influenciar fatores de experiência direta e indireta. Os trabalhos estão organizados entre aqueles que **incorporam e não incorporam atributos sociais**. Os trabalhos que incorporam atributos sociais se diferenciam pela característica social considerada e pela aplicação dessa característica a fim de obter o valor de confiança final.

Os trabalhos de confiança não social – ou somente confiança – são precursores dos trabalhos que incorporam a sociabilidade no cálculo da confiança e trazem diversos fundamentos para estes, como formas de calcular a confiança e mecanismos de esquecimento (desconsideração ou também decaimento) de experiências passadas. Na confiança não social, o trabalho de Putra et al. (2019) propôs um sistema de controle de acesso que incorpora a gerência de confiança. O trabalho estendeu o controle de acesso baseado em atributos (do inglês, *Attribute-based Access Control* - ABAC) (Hu et al., 2014), adicionando os valores de confiança e reputação como atributos para permitir um controle de acesso dinâmico. Este controle de acesso ocorre de forma descentralizada em blockchain, que armazena os atributos existentes e também mantém informações de reputação. O sistema emprega *smart contracts* – códigos imutáveis que são executados na blockchain – para codificar as políticas e para realizar o controle de acesso propriamente dito. Modela-se a confiança como uma função de Gompertz (Eq. 3.1) e emprega-se confiança local e reputação para determinar seu valor. Na Equação 3.1, a determina a assíntota, o termo b o parâmetro de deslocamento no eixo X, e o termo c a taxa de evolução. A confiança evolui à medida que dois nós têm boas experiências – ou seja, o serviço foi prestado de forma satisfatória e/ou o acesso foi permitido – e diminui de forma significativa conforme más experiências ocorrem. A equação também considera a um fator de esquecimento, valorizando interações recentes e preterindo relações antigas interações passadas (I_n). O uso desse fator de esquecimento apresenta

benefícios, pois permite que os dispositivos não tenham que armazenar todo o histórico de interações na memória. Porém, o uso de blockchain pode não ser adequado a todos os dispositivos devido a capacidade de armazenamento limitada e seu alto custo computacional. O protocolo de gerência da confiança também não estabelece limites superiores para a reputação ou uma forma de normalização para a mesma escala de variação considerada na confiança, entre 0 e 1.

$$T = a * e^{-b * e^{-c * I_n}} \quad (3.1)$$

Al-Hamadi et al. (2019) propuseram um modelo de gerência da confiança para a comunidade de serviços inteligentes, que tem como objetivo determinar o melhor prestador para um serviço. Nesse cenário, a comunidade de serviços inteligentes engloba uma grande diversidade de dispositivos IoT, que oferecem uma variedade de serviços. Na proposta, a confiança é multidimensional e leva em consideração a confiança direta entre tomadores e prestadores de serviço (*Service Requester* – SR e *Service Provider* – SP), a confiança indireta entre SR e SP e a performance do SP quanto a uma métrica específica, e.g. “tempo de espera”. Obtém-se a confiança indireta agregando as recomendações de outros SRs e ponderando pelas respectivas credibilidades. O sistema é mediado por um componente na nuvem que calcula e armazena todos os valores de confiança. Esse componente repassa para o tomador de serviço o valor da confiança, para que o usuário faça a escolha – seja utilizando a métrica e desconsiderando a confiança, seja escolhendo o nó mais confiável dentre as possibilidades – ou ainda optando pelo nó que tenha a melhor métrica dentre os confiáveis.

A confiança direta entre SR–SP é calculada conforme ao sistema de reputação Beta de Josang, proposto por Josang e Ismail (2002), e envolve as interações entre eles. Existe um decaimento da confiança, de modo que as interações mais recentes são valorizadas frente aquelas menos recentes. A Equação 3.2 exibe o cálculo da confiança direta e seu decaimento. Os termos α e β representam as interações boas e ruins, respectivamente. O termo $e^{-\lambda_d(t_{now}-t)}$ representa o decaimento como uma função exponencial decrescente dependente do termo $-\lambda_d$, taxa de decaimento, e do termo $(t_{now} - t)$, variação do tempo observada. Além disso, o sistema também considera experiências indiretas, ou seja, a reputação de um nó, obtida através da opinião de outros nós sobre o serviço e ponderada pelo nível de credibilidade que eles apresentam. Considera-se a credibilidade para filtrar as recomendações, descartando aquelas de baixa credibilidade, a fim de evitar ataques que visem manipular a confiança, e.g. ataques de difamação. Uma das fragilidades detectadas pelos autores é que o uso de um serviço centralizado pode ser inviável – devido a carga de processamento imposta ao servidor central – e que soluções descentralizadas podem aliviar essa carga.

$$T = \frac{\alpha * e^{-\lambda_d(t_{now}-t)}}{(\alpha + \beta) * e^{-\lambda_d(t_{now}-t)}} \quad (3.2)$$

Em Gwak et al. (2018), os autores buscaram incorporar a confiança no controle de acesso baseado em papéis (do inglês, *Role-Based Access Control* – RBAC) na IoT pública, que também exibe interações do tipo SR–SP. Os autores propuseram um método de gerência de confiança de modo que esta possa ser estimada mesmo que não haja interações prévias entre dois nós, a fim de permitir realizar um controle de acesso dinâmico. O sistema conta com um gerenciador de confiança e um gerenciador adaptativo que trabalham em conjunto para obter os dados de reputação de um nó, calcular sua confiança e realizar o controle de acesso. O sistema adota a lógica subjetiva de Jøsang e Bhuiyan (2008) para separar em dois grupos o nível de confiança, que é estimado através da Equação 3.3. Determina-se o termo b_y^x , confiança direta do nó y para o nó x , através das interações positivas e negativas entre esses dois nós. O termo u_y^x

balanceia a equação entre as interações diretas e reputação. Finalmente, o termo a_y^x representa a reputação de um em que se utiliza o conceito de grupo de interesses para sua obtenção (Pinel et al., 2006). A incorporação da confiança na controle de acesso baseado em papéis permite o sistema modular o controle de acesso e impedir que um nó exibindo comportamento malicioso participe da rede.

$$P(\omega_y^x) = b_y^x + u_y^x * a_y^x \quad (3.3)$$

Em Hellaoui et al. (2016), os autores propuseram o sistema TAS-IoT para segurança adaptativa no roteamento de pacotes. A proposta volta-se para autenticação da origem de pacotes recebidos por um dispositivo, que são autenticados se este dispositivo não confiar no dispositivo de origem. A decisão de autenticação ocorre localmente em cada dispositivo e sua adaptação foca na economia de recursos, dado que as funções criptográficas exigem alto consumo de recursos. Compõe-se a confiança a partir de três fatores – a confiança direta, a percepção que o dispositivo receptor tem a respeito do dispositivo de origem e a recomendação dos vizinhos sobre o dispositivo de origem – e varia entre zero e um. O TAS-IoT obtém a confiança direta pela experiência direta entre os nós. Determina-se a percepção de comportamento ouvindo o meio sem fio compartilhado e verificando se o dispositivo origem autenticou ou não o pacote e, ainda, se ele retransmitiu o pacote com alterações. Finalmente, define-se a recomendação através das opiniões dos outros dispositivos acerca do dispositivo origem.

3.2.1 Confiança Social

Aalibagi et al. (2019) propuseram um mecanismo de gerência de confiança para a internet das coisas sociais (SIoT) voltada a serviços. As interações sociais são modeladas como um grafo para extrair relações implícitas entre os dispositivos SR e os dispositivos SP. Os autores extraíram do grafo construído anteriormente diversos valores relacionados às relações sociais para elaborar uma matriz que possibilita determinar o nó mais confiável e influente para realizar o serviço requisitado. Os dispositivos calculam a confiança com base na sua similaridade, centralidade e amizade. A confiança na rede pode ser representada como uma matriz de adjacência $G = (V, U, W)$, onde V são os dispositivos SR e U , os dispositivos SP. W representa o nível de confiança que V tem sobre U . Como o dispositivo SR não possui a visão geral da rede, ou seja, não possui a matriz G , ele aproxima, através de fatoração matricial, as matrizes S e R , que representam um vetor de características de cada tipo de dispositivo. Essas matrizes são usadas para reconstruir a matriz G localmente, permitindo a seleção do dispositivo mais confiável. Apesar do mecanismo encontrar corretamente um provedor de serviço com nível de confiança alto, ele não leva em conta o contexto dos nós para calcular a confiança social. Além disso, a manipulação de matrizes e sua fatoração podem não ser adequadas para todos os dispositivos, devido a complexidade matemática dos seus cálculos.

Em Chen et al. (2018), os autores propuseram um sistema de gerenciamento de confiança como um serviço (*Trust as a Service* - TaaS) no contexto de cidades inteligentes (*smart cities*). O TaaS é um serviço em *cloud* que pode ser utilizado tanto para solicitação, quanto para composição de serviços. O servidor em *cloud* armazena e processa os dados de reputação entre os dispositivos de um determinado segmento da rede. Quanto ao aspecto social, o sistema considera três atributos entre os dispositivos: a amizade, o contato social e a sua comunidade de interesses. Esses atributos são comparados por sua similaridade, ocorrendo sempre que dois nós entram em contato. Os dispositivos trocam essas informações de uma maneira segura, utilizando mensagens autenticadas com código de autenticação de mensagem baseado em Hash (do inglês, *Hash-based Message Authentication Code* - HMAC) e respeitando a privacidade, tal que dispositivos e seus interesses

não comuns não sejam revelados. A Equação 3.4 mostra o cálculo da confiança. O termo μ é responsável por balancear a confiança direta e a indireta e a sua alteração adaptativa permite que comportamentos maliciosos sejam filtrados e desconsiderados. Os termos t^d e t^r representam, respectivamente, a confiança direta e a reputação, que é balanceada com a similaridade social entre os dispositivos. A incorporação dos atributos sociais permite o comportamento do dispositivo ser avaliado, revelando comportamentos maliciosos a serem filtrados.

$$t = \mu * t^d + (1 - \mu) * t^r \quad (3.4)$$

O trabalho de Kowshalya e Valarmathi (2018) propôs o sistema *DynamicTrust* voltado para a segurança na comunicação entre dispositivos SIoT. Nesse sistema, o dispositivo de maior centralidade – denominado autenticador –, gera e distribui chaves criptográficas. Assim, quando dois dispositivos desejam comunicar-se, eles avaliam a confiança do outro dispositivo, e, caso o nível de confiança seja adequado, eles trocam informações autenticadas ao empregar o código gerado pelo dispositivo autenticador. O *DynamicTrust* avalia a confiança através de quatro atributos: **honestidade, cooperação, comunidade de interesse e energia**. O sistema avalia a confiança de maneira distinta caso haja ou não interações prévias entre os dispositivos. No primeiro caso, a confiança em relação a cada atributo é avaliada utilizando-se as interações prévias, a confiança direta, a centralidade de um nó e um fator de confiabilidade. Esse fator é obtido a partir da interação do mesmo dispositivo em uma situação semelhante, porém em outra localização da rede, podendo ser zero. Contrariamente, se os dispositivos nunca interagiram, a confiança é avaliada através da interação direta com uma testemunha, a confiança que a testemunha tem com o dispositivo e a centralidade desse dispositivo. Assim como em outras propostas, o valor da confiança decai ao longo do tempo.

Em Suryani et al. (2017), os autores propuseram o *Contrust* que emprega um método de avaliação de confiança para proteger a comunicação entre dispositivos. A percepção de comunidade é o único atributo social considerado e é utilizado para compartimentalizar a confiança entre diferentes comunidades. Assim como em (Kowshalya e Valarmathi, 2018), avalia-se a confiança quando os dispositivos começam a trocar mensagens. O *Contrust* determina a confiança final através da confiança direta e da reputação de um dispositivo, sendo consideradas em um determinado instante de tempo. Elas podem ser balanceadas por um fator α que valoriza mais a confiança direta do que a reputação. A confiança direta é obtida das interações entre os dispositivos i e j na mesma comunidade e na confiança de i para j em uma outra comunidade, se existir. A reputação decai de acordo com a tendência do nível de confiança e conforme a avaliação da confiança em instantes consecutivos de tempo. Um dos pontos fortes da proposta é uma espécie de “pré-autenticação”, utilizando o método Diffie-Hellman de troca de chaves, em que os nós de uma mesma comunidade negociam uma chave de sessão para encriptar os dados sociais a serem trocados, a fim de evitar ataques durante essas trocas.

3.2.2 Perspectivas da Composição da Confiança

Esta seção apresenta uma discussão do estado-da-arte sobre o gerenciamento de confiança e confiança social na IoT. Os trabalhos foram analisados e sumarizados conforme suas características, nas Tabelas 3.3 e 3.4. Dos trabalhos de confiança não social, destacam-se as suas características e a forma de decaimento, se existente. Já nos trabalhos de confiança social, além das características para compor a confiança, foram identificados os ataques que esses trabalhos estão sujeitos e quais deles os trabalhos mostram-se resilientes.

O gerenciamento de confiança nas redes IoT visa apoiar outros serviços e lhe trazer flexibilidade. Desse modo, os trabalhos consideram diversos atributos para compor a confiança

final. Porém, por não incorporarem atributos sociais, os trabalhos de confiança não social necessitam de outras estratégias para mitigação de possíveis ataques de recomendação, como o ataque de difamação. Dentre os trabalhos de confiança não social, a proposta de Gwak et al. (2018), incorpora a confiança não social no controle de acesso utilizando a lógica subjetiva. Em Putra et al. (2019), os autores apresentaram um sistema que emprega uma arquitetura em blockchain, que manipula recomendações falsas mitigadas pela assinatura presente nas operações. Outros trabalhos como Tan et al. (2016) e Reddy et al. (2019) levam em conta a similaridade das recomendações para desconsiderar recomendações manipuladas. A Tabela 3.3 sumariza os trabalhos que tratam da confiança não social na IoT, os ataques considerados e como se dá a obtenção da confiança.

$$T = \alpha * D + (1 - \alpha) * R \quad (3.5)$$

Outra questão limitante dos trabalhos de confiança não social é a gama de fatores ou atributos a serem considerados para o cálculo da confiança e como esta pode ser composta. Vários trabalhos como Hellaoui et al. (2016), Tan et al. (2016), Reddy et al. (2019) e Putra et al. (2019) consideraram somente a confiança direta e as recomendações para o cálculo da confiança, aproximando esse cálculo da Equação 3.5. Nela, D representa a confiança direta, R as recomendações e α dá mais importância a um dos fatores em detrimento do outro. Os trabalhos Khan et al. (2017) e Gwak et al. (2018) utilizaram a lógica subjetiva para avaliação da confiança. Em contrapartida, Al-Hamadi et al. (2019) e Putra et al. (2019) empregaram, respectivamente, a distribuição beta de Josang (Eq. 3.2) e a distribuição de Gompertz.

Tabela 3.3: Resumo dos trabalhos de gerenciamento de confiança em IoT

Trabalho	Características consideradas	Tipos de Ataques
(Hellaoui et al., 2016)	Confiança direta Confiança indireta (Observação e reputação)	On-off
(Khan et al., 2017)	Confiança direta (Lógica subjetiva)	Autopromoção Difamação Conluio
(Tan et al., 2016)	Confiança direta Confiança indireta	Difamação Conluio
(Gwak et al., 2018)	Confiança direta (Lógica Subjetiva) Confiança indireta (I-sharing)	DoS Sybil Ataques de manipulação da confiança
(Reddy et al., 2019)	Confiança direta Confiança indireta	Difamação Conluio
(Al-Hamadi et al., 2019)	Confiança direta (Distribuição beta de Josang) Confiança indireta (Credibilidade)	Autopromoção Conluio Má recomendação Não-cooperação Fabricação de recomendação
(Putra et al., 2019)	Confiança direta (Gompertz) Confiança indireta	Difamação Newcomer

Os trabalhos de confiança não social formam a base do gerenciamento de confiança na IoT e foram usados, principalmente, relacionados a sistemas de recomendação e confiança (do inglês, *Trust and Recommender Systems* - TRSs). Percebe-se, através da Tabela 3.3, que a maioria dos trabalhos analisados tratou do ataque de difamação, que objetiva diminuir a confiança que uma parte da rede detém sobre um determinado dispositivo, o que demonstra que esse ataque afeta o funcionamento usual dos sistemas baseados em confiança, devendo ser levado em conta quando se considera o emprego de um TRS, para qualquer fim que seja. Dentre os trabalhos

elencados, percebe-se que existem diversas estratégias para a mitigação desse ataque, tais como a assinatura das informações, que é uma forma de *Data Provenance*, e a similaridade entre as recomendações e grupos de interesse. Como será visto adiante, outras estratégias podem ser empregadas aliadas às citadas para mitigação do ataque de difamação.

Apesar da manipulação da confiança ser um problema conhecido em sistemas de gerenciamento de confiança, os trabalhos de Premarathne (2017) e Abderrahim et al. (2017b), que empregaram confiança social, não avaliaram as propostas quanto a agentes maliciosos atuando na rede. A manipulação da confiança, através de ataques como o de difamação, por atores maliciosos pode levar à negação de serviço ou ainda à prestação do serviço por um dispositivo não confiável. Assim como o TRS, os sistemas de gerenciamento de confiança baseados em confiança social (TMS) também empregam estratégias para mitigar a participação de atores maliciosos, como nas propostas de Suryani et al. (2017) e Kowshalya e Valarmathi (2018), em que uma forma de “pré-autenticação” é empregada para se evitar que os dados sociais sejam adulterados quando em trânsito, garantindo sua irretratabilidade e integridade e fazendo com que a proveniência desses dados seja confirmada. Além disso, esses sistemas utilizam limiares dinâmicos de confiança para a escolha dos dispositivos que irão se comunicar, aplicando uma espécie de filtro, causando a exclusão dos dispositivos com baixa confiança da rede. Outra estratégia empregada pelos TMSs envolve o balanceamento das recomendações pela confiança que o dispositivo recebedor tem sobre os dispositivos que enviaram as recomendações, assim como nos TRSs. O sistema proposto em Abderrahim et al. (2016), por exemplo, ponderou as recomendações recebidas através de nós garantidores, a fim de filtrar recomendações desonestas.

A utilização de um limiar dinâmico de confiança ou mesmo de limiares diferenciados de acordo com o contexto dos dispositivos se mostra insuficiente para detectar atores maliciosos, pois os atacantes podem associar outros tipos de ataque, que fazem que a utilização do limiar sem valor. Além do limiar, os trabalhos se concentram, principalmente, em identificar agentes maliciosos que manipulam a confiança através do ataque de difamação. A curva de crescimento da confiança dos sistemas é pensada de modo que comportamentos maliciosos sejam punidos rapidamente e o crescimento da confiança seja mais lento. Desse modo, a medida que um nó malicioso atua, sua reputação diminui rapidamente. Aliado a essa estratégia, os dispositivos também alteram dinamicamente a relação entre confiança direta e indireta, possibilitando que a confiança percebida pelos dispositivos seja mais próxima da confiança em um estado sem ataque.

Quanto aos atributos sociais considerados, os trabalhos empregam uma gama deles. As comunidades de interesse (CoI), por exemplo, são utilizadas para compartimentalizar o comportamento do nó em diferentes comunidades da rede. Em Abderrahim et al. (2017a), os autores utilizaram, além das CoIs, a confiança direta e a reputação para determinar a confiança de um nó. Em Chen et al. (2014), os autores agregaram a amizade entre os dispositivos e seu contato social para o cálculo da confiança. Os trabalhos de Khani et al. (2018) e Premarathne (2017) utilizaram os quatro atributos sociais como propostos por Atzori et al. (2012) (SOR, WOR, LOR e POR, vide Seção 2.3), enquanto outros trabalhos consideraram atributos como amizade e contato social. Quando os trabalhos representam as interações sociais através de grafos, eles são capazes de inferir características como centralidade, que mede a influência de um dispositivo na rede. Em Jafarian et al. (2020), os autores empregaram a similaridade dos atributos sociais em conjunto com a confiança direta e reputação, formando um hiperplano para a utilização de técnicas de aprendizado de máquina voltadas para a escolha do dispositivo mais confiável. A Tabela 3.4 classifica os TMSs de confiança social conforme os ataques considerados e as características sociais empregadas.

Tabela 3.4: Resumo dos trabalhos de gerenciamento de confiança em SIoT

Proposta	Autor	Características Sociais	Ataques
_ ^a	(Jafarian et al., 2020)	Contexto Reputação	Autopromoção Difamação Conluio Prestação Oportunística de Serviço
_ ^a	(Aalibagi et al., 2019)	Amizade Centralidade Similaridade	Autopromoção Difamação Conluio Prestação Oportunística de Serviço Whitewashing
TaaS	(Chen et al., 2018)	Amizade Contato Social Comunidades de Interesse	Autopromoção Difamação Conluio Prestação Oportunística de Serviço Discriminação
DynamicTrust	(Kowshalya e Valarmathi, 2018)	Confiança direta Confiança indireta Honestidade Centralidade Confiabilidade Energia	Difamação Sybil
TMSContext	(Khani et al., 2018)	QoS esperado QoS anunciado Amizade Comunidade de Interesse Relações sociais de Atzori	Autopromoção Boa recomendação Difamação On-off
MAG-Siot	(Premarathne, 2017)	Relações sociais de Atzori	
TM-Coi	(Abderrahim et al., 2017a)	Confiança direta Confiança indireta Comunidade de Interesse	Boa recomendação Difamação On-off
CTMS-Siot	(Abderrahim et al., 2017b)	Amizade Capacidades do objeto Comunidade de Interesse Credibilidade Reputação	_ ^b
DTMS	(Abderrahim et al., 2016)	Confiança direta Confiança indireta Reputação Garantidor	Boa recomendação Difamação On-off
Contrust	(Suryani et al., 2017)	Confiança direta Confiança indireta Comunidade de Interesse	Autopromoção Boa recomendação Difamação
_ ^a	(Chen et al., 2014)	Confiança Direta Confiança Indireta Amizade Contato Social Comunidades de Interesse	Autopromoção Conluio Difamação Prestação Oportunística de Serviço

^a Os autores não nomearam a proposta^b Nenhum ataque foi considerado no trabalho

A incorporação de características sociais pelas propostas supracitadas permite que os TMSs avaliem com mais precisão os nós participantes da rede. Porém, vários sistemas apresentam algumas fragilidades. Em Jafarian et al. (2020); Suryani et al. (2017); Abderrahim et al. (2017a), o emprego dos atributos sociais se limita às Comunidades de Interesse, a fim de compartimentalizar o comportamento do objeto. Nesses trabalhos, a avaliação da confiança se vale somente dos componentes confiança direta e reputação. A adição de amizade e contato social,

como em Chen et al. (2014); Aalibagi et al. (2019); Chen et al. (2018); Abderrahim et al. (2017b, 2016), não aproveita outras características e interações sociais. Adicionalmente, em Aalibagi et al. (2019); Jafarian et al. (2020), as técnicas utilizadas para avaliação da confiança, fatoração matricial e aprendizado de máquina, respectivamente, podem não ser adequados aos dispositivos IoT por sua complexidade, visto que os dispositivos têm restrição de energia e processamento.

A análise do estado-da-arte sobre o uso de Confiança e Confiança Social em IoT demonstrou que os sistemas propostos na literatura têm sido empregados em diversas aplicações, principalmente voltados ao controle de acesso (Autorização) e à seleção e composição de serviços. Assim, a Tabela 3.5 sumariza os requisitos necessários aos TMSs quando utilizados apoiando os SAAs. Nesse contexto, os sistemas que consideram confiança permitem que um dispositivo avalie com assertividade o comportamento dos outros dispositivos e regule o acesso a determinados serviços ou recursos. Porém, os TMSs estão sujeitos a ataques que manipulam a confiança, como o ataque de difamação, e necessitam empregar estratégias para mitigá-los.

Tabela 3.5: Requisitos necessários para os TMSs

Trabalhos	Autônomo	Não-repúdio	Integridade	Ataque de Difamação
(Aalibagi et al., 2019)				
(Chen et al., 2018)		✓ PSK	✓ PSK	✓ Ajuste de threshold
(Kowshalya e Valarmathi, 2018)		✓ DH	✓ DH	✓ Ajuste de threshold e Nós garantidores
(Suryani et al., 2018)		✓ DH	✓ DH	✓ Ajuste de threshold e DH

3.2.3 Técnicas Contra o Ataque de Difamação

Como visto, os sistemas que utilizam confiança (TMSs) devem se preocupar com os ataques contra esse atributo como o ataque de difamação (ou má-recomendação), que é um dos ataques comuns contra a confiança (Chen et al., 2016). Para mitigar esse tipo de ataque, os sistemas usam diversas estratégias, tais como filtragem, similaridade, a própria composição da confiança e técnicas de *Data Provenance*. Em geral, essas estratégias estão incorporadas nos sistemas de gerenciamento de confiança e podem ser empregadas em conjunto.

A estratégia de filtragem separa as recomendações recebidas a fim de selecionar algumas recomendações, descartando as demais. A filtragem pode ocorrer através de um limiar fixo ou variável. Com o limiar fixo, os TMSs aplicam sempre o mesmo limiar para filtragem. Já na filtragem com limiar variável, os TMSs efetuam cálculos para determinar dinamicamente esse limiar (Guo et al., 2017). A estratégia de similaridade analisa as recomendações recebidas e descarta aquelas dissimilares em relação às recomendações recebidas. Essas duas estratégias (filtragem e similaridade) podem ser empregadas em conjunto, com a similaridade determinando o nível mínimo de recomendação para a filtragem.

As estratégias que contém a mitigação do ataque de difamação no próprio cálculo da confiança, fazem-no através do balanceamento dinâmico do peso das recomendações. Dessa forma, mesmo que más recomendações cheguem, elas contribuem pouco para o valor final da confiança. É importante ressaltar que vários trabalhos contam somente com essa estratégia de mitigação, e.g. Chen et al. (2014, 2018), e que o mecanismo que determina essa mudança de peso é fixo, ou seja, cada dispositivo utiliza a mesma configuração até ser reconfigurado manualmente.

Por fim, a estratégia de Data Provenance para mitigação da difamação englobam os trabalhos que utilizam alguma técnica de proveniência dos dados, como assinaturas ou formas de “pré-autenticação”. Em Hellaoui et al. (2016) utiliza-se a autenticação de origem como forma de

atestar a fonte da informação e determinar a confiança sobre o nó que emitiu a recomendação, permitindo o descarte de recomendações sem origem definida e/ou não confiáveis. Putra et al. (2019) também aplicou a autenticação de origem, porém na blockchain, a fim de garantir a origem e a integridade dos dados. Outros trabalhos como Chen et al. (2018); Kowshalya e Valarmathi (2018); Suryani et al. (2017) empregaram alguma forma de comunicação segura, assemelhando-se a uma “pré-autenticação”, quando chaves são negociadas apenas para a troca inicial de recomendações, possibilitando os dispositivos trocarem recomendações de forma segura. Esses trabalhos diferenciam-se na forma de pré-autenticação; enquanto os dois primeiros fazem-na par-a-par, o último pré-autentica dentro de uma mesma Comunidade de Interesses.

A análise do estado-da-arte na mitigação do ataque de difamação/má-recomendação aponta que os trabalhos que incorporam Data Provenance podem avaliar o comportamento dos outros dispositivos assertivamente ao desconsiderar recomendações que não tenham sua origem e integridade atestadas. Assim, a mitigação baseada nessas técnicas podem ser incorporadas em TMSs quando estes são empregados como fator de avaliação de dispositivos em um sistema mais amplo, como um Sistema de Autenticação Adaptativa.

3.3 RESUMO

Este capítulo apresentou como tem sido tratado o problema da autenticação adaptativa em redes de Internet das Coisas. As três principais técnicas empregadas foram apresentadas, bem como aquelas baseadas em Políticas. Para cada técnica, discutiu-se seus pontos positivos e negativos, além de fatores utilizados para autenticação. Detalhou-se também como a confiança e a confiança social têm sido tratadas em redes IoT e como os sistemas que empregam a confiança (social ou não) mitigam os ataques à confiança, em especial o ataque de difamação.

4 AUTENTICAÇÃO ADAPTATIVA DE DISPOSITIVOS IOT SOCIAIS RESISTENTE A ATAQUES DE DIFAMAÇÃO

Este capítulo apresenta a proposta de um sistema de gerência adaptativa de autenticação baseada em confiança social para ambientes IoT resiliente a ataques de difamação. O sistema, chamado de GALENA (ManaGement of Adaptive Authentication Based on PoLiciEs aNd SociAl Trust), determina de maneira dinâmica o mecanismo de autenticação mais adequado em um determinado ambiente e nível de sociabilidade entre dispositivos. Inicialmente, a Seção 4.1 apresenta uma visão geral sobre os ambientes IoT e a interação social entre os dispositivos, além da caracterização do ataque de difamação. Em seguida, a Seção 4.2 exibe a arquitetura do sistema GALENA, detalhando suas partes e como elas se relacionam. Por fim, a Seção 4.3 demonstra o funcionamento do sistema.

4.1 CARACTERÍSTICAS DOS AMBIENTES IOT E DOS ATAQUES

Esta seção descreve uma visão geral sobre as características dos ambientes IoT considerados em termos dos tipos de dispositivos existentes e serviços oferecidos, e as interações sociais estabelecidas entre esses dispositivos decorrentes da sua mobilidade. Também, descreve-se o comportamento e o modo como o ataque de difamação impacta na percepção social entre esses dispositivos. As características necessárias ao SAA proposto, como adaptabilidade ao ambiente, suporte à heterogeneidade dos dispositivos, operação de maneira *ad hoc* e descentralização, foram definidas a partir do estado-da-arte dos SAAs descrito na Seção 3.1 do Capítulo 3. Essas características constituem as premissas norteadoras ao desenvolvimento do sistema GALENA, descrito em seguida.

4.1.1 Ambientes de Redes IoT

Considera-se que cada ambiente IoT compreende um conjunto de dispositivos IoT identificados por $D = \{d_1, d_2, d_3, \dots, d_i\}$, onde $d_i \in D$, e que possuem, cada, um identificador (*Id*) único. Ao longo do seu funcionamento as dispositivos proveem e solicitam uma coleção de serviços $O_{Id} \subseteq S = \{s_1, s_2, \dots, s_j\}$ uns dos outros, tanto autonomamente ou por iniciativa do usuário, tornando-os prestadores (do inglês, *Service Provider* – SP) e tomadores de serviço (do inglês, *Service Requester* – SR) em instantes e localizações diferentes da rede. Além disso, as características do ambiente onde os dispositivos estão inseridos determinam se eles são estáticos ($d_i \in D_{sta}$) ou móveis ($d_i \in D_{mov}$) – tal que $D = D_{mov} \cup D_{sta}$ – e quais restrições de energia, processamento e armazenamento eles apresentam; bem como os serviços que os dispositivos provêem. Os dispositivos são capazes de determinar sua localização – caso sejam móveis – ou sua localização vem pré-configurada. A Figura 4.1 apresenta uma visão estática da rede indicando os diversos domínios de redes IoT e quais dispositivos podem fazer parte dela. É importante ressaltar que devido a mobilidade entre os dispositivos, eles interagem com dispositivos em outros domínios de redes IoT que não a de operação usual.

A interação entre os dispositivos ocorre através de protocolos que respeitam suas limitações computacionais. A comunicação ocorre através de um meio sem fio em um canal assíncrono e compartilhado e os dispositivos trocam mensagens utilizando o protocolo 6LoWPAN sobre o padrão IEEE 802.15.4 ou o padrão Wi-Fi, por serem protocolos adequados para interligar entre si os dispositivos com restrição e com a Internet convencional para formar a

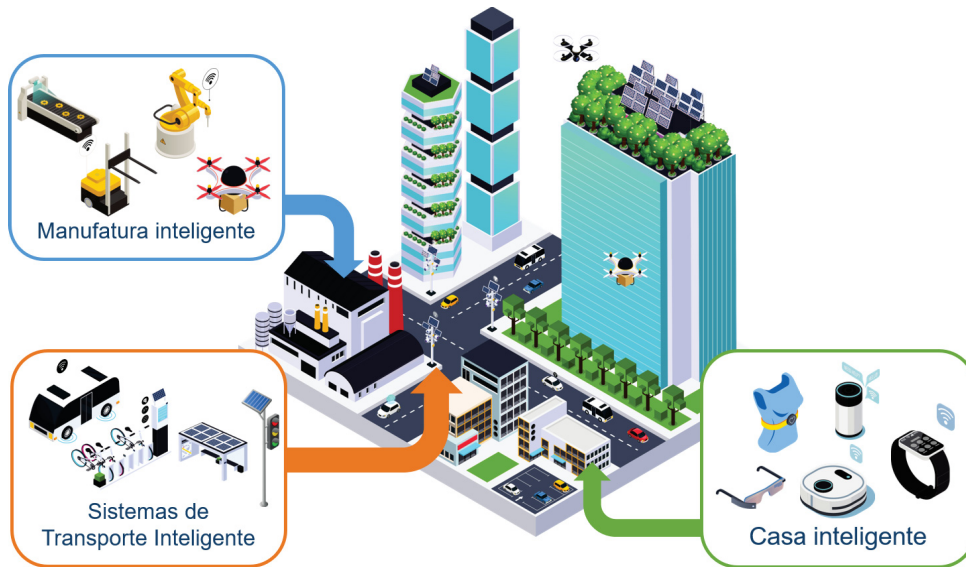


Figura 4.1: Modelo de rede

IoT (Morabito e Jimenez, 2020). Os dispositivos formam uma rede *ad hoc* e autenticam-se a fim de prover ou tomar serviços. Para isso, suportam um conjunto de diferentes mecanismos de autenticação $\mathcal{M}_{Id} \subseteq \mathcal{M} = \{m_1, m_2, \dots, m_k\}$ de acordo com suas capacidades de comunicação e de processamento (Malik et al., 2019). Os mecanismos, por sua vez, necessitam de configurações específicas para serem utilizados, e.g. tamanho da chave e assinatura do certificado. A notação P_i^m , referencia sequencialmente i um determinado perfil do mecanismo m que agrupa as configurações específicas para esse mecanismo. A medida que os dispositivos interagem, eles também criam e mantêm relações sociais entre si, que será explicado seguidamente.

4.1.2 Interação Social entre Dispositivos

O modelo de interação social dita como os objetos criam e mantêm relações sociais. Três relações são consideradas nesse trabalho: *Co-location object relationship* (Relacionamento por co-localização – C-LOR), *Co-work object relationship* (Relacionamento por cooperação de trabalho – C-WOR) e *Social object relationship* (Relação social – SOR), como definidas por Atzori et al. (2012). Dispositivos utilizados no mesmo ambiente criam a relação C-LOR, mesmo que não provejam o mesmo conjunto de serviços. Já a relação C-WOR ocorre entre dispositivos do mesmo ambiente que, além disso, proveem o mesmo serviço. Por fim, os dispositivos criam a relação SOR quando entram em contato entre si, esporádica ou continuamente.

Os dispositivos constituem as relações C-LOR e C-WOR de maneira similar. Para criá-las, os dispositivos primeiramente encontram outros dispositivos próximos e trocam informações sobre os serviços que eles proveem. Em seguida eles verificam se existe intersecção entre os serviços, caso haja, a relação criada é C-WOR, senão C-LOR. Essas relações ocorrem em dispositivos que são estáticos. Similarmente, quando quaisquer dois dispositivos entram em contato, eles criam a relação SOR. Caso o contato seja esporádico, a relação é fraca e pode não perdurar. Alternativamente, a medida que mais interações ocorrem esta relação torna-se mais forte. As outras relações sociais também sofrem decaimento e podem extinguir-se caso o dispositivo for movido (ou mover-se) e abandonar a vizinhança dos dispositivos com os quais ele criou as relações C-LOR ou C-WOR.

4.1.3 Modelo do Ataque de Difamação

Como visto na Seção 2.4, a característica do ataque de difamação nos ambientes IoT consiste de um dispositivo malicioso que objetiva diminuir a confiança que outros dispositivos têm sobre o dispositivo-alvo. A redução da confiança impacta diretamente na manutenção desse dispositivo na rede e na disponibilização e tomada de serviços. Além disso, uma vez que o dispositivo-alvo esteja isolado, o atacante pode buscar tomar o lugar do alvo como provedor de serviços e assim causar instabilidade na rede IoT, com maior consumo de recursos, bem como perpetuar ataques mais sofisticados. Dessa forma, é importante que sistemas de autenticação adaptativa que utilizam confiança social sejam resilientes a esse ataque para que requisitos de segurança como disponibilidade e integridade não sejam afetados.

Quanto ao ataque de difamação, considera-se que o dispositivo malicioso opera de maneira isolada, i.e. não há cooperação entre dispositivos maliciosos, isto é, não há um ataque em conluio. No entanto, o ataque pode ocorrer em conjunto com outros ataques na camada de rede, como o ataque *Sybil*. O ataque de difamação ocorre no momento que os dispositivos consultam informações sociais uns dos outros. O dispositivo atacante pode atuar de duas formas quanto a sua identificação: Na primeira, ele propaga má-recomendações sobre o dispositivo-alvo, utilizando, para tanto, sua própria identificação. Na segunda forma, ele utiliza outra identificação (Ataque associado a *Sybil*) a fim de não prejudicar a sua própria identificação, i.e. ter sua própria confiança diminuída por realizar o ataque. Quanto a frequência do ataque, o atacante pode realizá-lo: *Constantemente*, ou seja, as recomendações enviadas são sempre um ataque, ou *Seletivamente*, ou seja, nem toda recomendação enviada é um ataque. Dessa forma, são quatro as combinações de tipos de ataque:

- Identificação própria com Difamação Constante
- Identificação Sybil com Difamação Constante
- Identificação própria com Difamação Seletiva
- Identificação Sybil com Difamação Seletiva

4.2 SISTEMA GALENA

Esta seção descreve a arquitetura do sistema GALENA, suas interações e modo de funcionamento. A especificação do sistema assumiu que o ataque de difamação ocorre localmente e isoladamente, como descrito na Seção 2.4 e Subseção 4.1.3. Também, assume-se que uma entidade externa cria e configura as políticas no GALENA e, por fim, o Serviço de Localização nunca falha. Ainda, o sistema emprega *Data Provenance* para mitigação do efeito do ataque de difamação.

A arquitetura do GALENA compreende três subsistemas e um serviço externo que interagem entre eles, como representados na Figura 4.2. O subsistema de **Gerência de Descoberta (SGDE)** coordena a descoberta de outros dispositivos ao seu redor, dissemina suas capacidades de autenticação e serviços disponíveis. O subsistema de **Gerência de Autenticação (SGAUTH)** controla a adaptação e a gestão de políticas de autenticação. O subsistema de **Gerência Social (SGSOC)** controla a requisição, a validação e posterior agregação das informações sociais sobre os dispositivos; bem como a verificação da proveniência dos dados sociais. Finalmente, o **Serviço de Localização (SLOC)** provê informações sobre o ambiente aos outros subsistemas. O serviço de localização obtém o contexto primário, ou seja o posicionamento específico dos dispositivos, dados pelos sistemas de posicionamento global (do inglês, *Global Navigation Satellite Systems - GNSS*). A partir do contexto primário, ele deriva um contexto secundário, semântico e referente

ao ambiente em si, utilizando-se sistemas online de localização e determina um ambiente, por exemplo, uma “casa” ou “escola”, que podem ser utilizados pelos outros subsistemas.

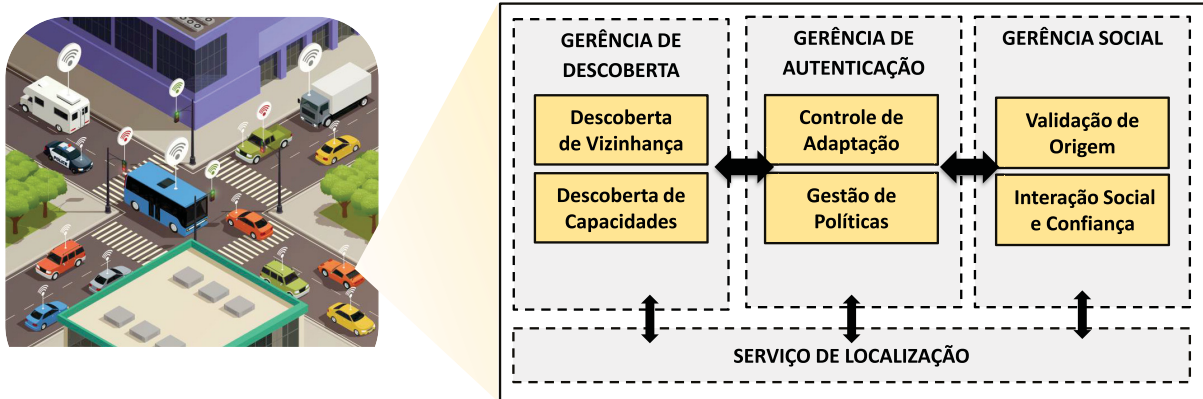


Figura 4.2: Arquitetura do GALENA

4.2.1 Gerência de Descoberta

O subsistema de Gerência de Descoberta (SGDE) compõe-se do serviço de descoberta de vizinhança (*SDES*) e do serviço de descoberta de capacidades (*SDCAP*). Esses serviços cooperam para a descoberta de dispositivos e seus serviços. O Algoritmo 1 descreve o funcionamento desses serviços, onde o serviço de descoberta anuncia a presença do dispositivo em intervalos periódicos configuráveis e também recebe outros anúncios da presença de dispositivos próximos, visando a criação de um conjunto de vizinhos (l.1-12). Já o serviço de descoberta de capacidades (*SDCAP*) recebe e responde as solicitações quanto aos serviços oferecidos pelo dispositivo e os mecanismos de autenticação suportados e relaciona-os com os vizinhos já descobertos (l.13-18). O *SDCAP* pode empregar técnicas como *mDNS* (*DNS Multicast*) e *DNS-SD* (*DNS-Based Service Discovery*) para descobrir as capacidades e os serviços dos dispositivos conhecidos, conforme descrito em Al-Fuqaha et al. (2015).

Algoritmo 1: Anúncio de Presença e Disseminação de Capacidades

```

1  procedure AnnouncePresence()
2      NeighborList  $\leftarrow$  0
3      while True do
4          SendAnnounce()
5          WaitInterval()
6      end
7  end procedure
8  procedure ReceiveAnnounce()
9      NeighborId  $\leftarrow$  GetId()
10     NeighborList  $\leftarrow$  NeighborList  $\cup$  NeighborId
11     RequireCapabilities(NeighborId)
12 end procedure
13 procedure RequireCapabilities(NeighborId)
14     NeighborCapabilities[NeighborId]  $\leftarrow$  RequireNeighborCapabilities(NeighborId)
15 end procedure
16 procedure AnswerCapabilitiesRequest
17     SendServicesAndAuthenticationMechanisms()
18 end procedure

```

4.2.2 Gerência Social

O subsistema de Gerência Social (SGSOC) coordena o recebimento, a disseminação, e validação e consolidação dos dados sociais. Ele compõe-se do serviço de interação social e confiança (SISCO) e o serviço de validação de origem (SVOR). O Algoritmo 2 descreve o funcionamento desses serviços, onde o SISCO recebe de outros dispositivos as requisições de dados sociais sobre terceiros e responde às requisições com a confiança percebida em relação a esses terceiros (l.9-11). Ele também agrega e atualiza a estrutura que contém as relações sociais formadas empregando o Protocolo de Confiança Social, descrito a seguir, para derivar o valor da confiança e atualizá-la a medida que as interações com outros dispositivos ocorrem.

O SVOR valida a origem e a integridade dos dados sociais recebidos, utilizado-se de códigos de verificação autenticados (HMAC) como técnica de *Data Provenance* a fim de identificar o ataque de difamação do segundo tipo e descartar seu efeito. As técnicas de *Data Provenance* estão descritas na Seção 2.6). O serviço utiliza a potência do sinal recebido (RSSI), que é o mesmo para os dois dispositivos, como chave MAC (*Message Authentication Code*) dos dados sociais trocados (l.2 e l.13), garantindo sua origem e integridade. Quando o SVOR recebe uma requisição de dados sociais (l.1-5), ele a repassa ao SISCO para que este verifique a confiança social percebida em relação aquele dispositivo. Após, o SISCO encaminha a confiança percebida para o SVOR, que por sua vez efetuará o cálculo MAC e o envio desses dados para o dispositivo requisitante. Por outro lado, ao receber os dados sociais solicitados, o SVOR valida se a origem é conhecida e se a mensagem possui o código HMAC correto (l.12-16).

Algoritmo 2: Recebimento e Envio de Mensagens Sociais com Data Provenance

```

1 procedure ReceiveSocialDataRequest(NeighborId, SocialScore)
2   key  $\leftarrow$  GetRSSI()
3   SocialScore  $\leftarrow$  GetSocialScore(NeighborId)
4   SendSignedSocialData(NeighborId, SocialScore, key)
5 end procedure
6 procedure SendSocialDataRequest(NeighborId)
7   SendRequestSocialScore(NeighborId)
8 end procedure
9 procedure GetSocialScore(NeighborId)
10  return  $S(\textit{NeighborId})$ ;                                /* Valor da Eq. 4.1 */
11 end procedure
12 procedure RecvSocialData(NeighborId, SocialScore)
13  key  $\leftarrow$  GetRSSI()
14  ValidateDataProvenance(NeighborId, message, key)
15   $R_{Id} \leftarrow R_{Id} + \textit{SocialScore}$ ;    /* Referente a variável  $R_{Id}$  da Eq. 4.2 */
16 end procedure

```

4.2.2.1 Protocolo de Confiança Social

O protocolo de confiança social, implementado pelo SISCO, dita como as relações sociais são reduzidas em um valor entre 0 e 1, que representa o nível ou *score* de confiança social. O SISCO manipula a estrutura que armazena as relações sociais mantidas pelo dispositivo e atualiza-o a medida que novas interações acontecem e informações antigas são esquecidas. Por fim, esse serviço calcula a confiança social aplicando a Equação 4.1, que corresponde a função S da Definição 4.1 na Subseção 4.2.3.

$$S(Id) = \alpha * LOR_{Id} + \beta * WOR_{Id} + \gamma * SOR_{Id} \quad (4.1)$$

A confiança restringe-se à escala unitária pela seguinte equação: $\alpha + \beta + \gamma = 1$. O SISCO calcula o termo LOR_{Id} utilizando a distância entre ele e o dispositivo vizinho e normaliza-o – através da normalização logística – para valores entre 0 e 1. Valores próximos de 0 indicam que os nós estão afastados e aqueles próximos de 1, que os dispositivos estão em proximidade. Por sua vez, o serviço obtém o valor WOR_{Id} a partir similaridade entre os serviços ofertados pelo dispositivo vizinho e o próprio dispositivo.

$$SOR_{Id} = \delta * \left(\frac{\mu_{Id}}{\tau_{Id}} \right) * e^{-\lambda_d(t_{now}-t)} + (1 - \delta) * R_{Id} \quad (4.2)$$

O SISCO determina o valor SOR a partir da Equação 4.2, que leva em conta o total de interações com sucesso e as interações totais. O valor μ_{Id} representa as interações com sucesso, i.e. que o serviço requisitado foi realmente provido, e τ_{Id} são as interações totais. O termo $e^{-\lambda_d(t_{now}-t)}$ exprime o decaimento como uma função exponencial decrescente dependente do termo $-\lambda_d$, taxa de decaimento, e do termo $(t_{now} - t)$, 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. o *score* percebido por eles, sobre o dispositivo com o qual se quer interagir. Já o valor δ balanceia entre a confiança direta, representada pelo primeiro termo da soma, e a confiança indireta, ou recomendação, representada pelo segundo termo.

O SISCO atualiza o *score* social em dois momentos: Quando um dispositivo solicita uma recomendação e quando está interagindo diretamente com outro dispositivo a fim de prover ou obter serviços. No primeiro momento, as relações C-LOR, C-WOR e SOR já foram criadas e o dispositivo somente repassa o *score* já calculado. Contrariamente, se ele está interagindo diretamente com o dispositivo, as relações são criadas conforme o modelo de interação social (visto anteriormente na Subseção 4.1.2) e calcula-se o *score* conforme as Equações 4.1 e 4.2. Os valores α , β , γ , $e^{-\lambda_d(t_{now}-t)}$, e δ podem ser ajustados conforme a operação do GALENA, para ser resiliente ao ataque de difamação.

4.2.3 Gerência de Autenticação

O subsistema de Gerência de Autenticação (SGAUTH) compõe-se do serviço de controle de adaptação (*SADPT*) e do serviço de gestão de políticas (*SPOL*) e seu funcionamento está descrito no Algoritmo 3. O SGAUTH concentra as responsabilidades típicas de um Ponto de Decisão de Políticas (PDP) e de um Ponto de Aplicação de Políticas (PEP). Ou seja, ele determina a política e toma a ação derivada da sua aplicação (conforme apresentado na Seção 2.5). Para a autenticação de um dispositivo em um dado ambiente, o SADPT consulta o serviço SPOL a fim de conhecer as políticas determinadas para aquele ambiente (l.2-3). Em seguida, o SADPT obtém dados do subsistema de gerência social (l.3) e do serviço de disseminação (l.4) – que funcionam como Ponto de Informação de Políticas (PIP) – provendo valores para subsidiar o SADPT na escolha da política mais adequada (l.6-7). Configuram-se as políticas no momento da implantação, caso os dispositivos sejam estáticos, ou durante a operação, caso os dispositivos permitam interação com o usuário.

Algoritmo 3: Adaptação do Mecanismo de Autenticação

```

1 procedure ApplyPolicy(NeighborId)
2   context ← GetContext(); // Interface com SLOC
3   policies ← GetContextPolicies(context); // Interface com SPOL
4   socialScore ← GetSocialScore(NeighborId); // Definido no Alg. 2
5   capabilities ← NeighborCapabilities[NeighborId]; // Obtido pelo Alg. 1
6   auth_profile ← DecideProfile(NeighborId, Capabilities, SocialScore, Context, Policies)
7   ApplyAuthProfile(auth_profile); // Aplica o mecanismo de autenticação no
   dispositivo
8 end procedure

```

As políticas no sistema GALENA codificam as regras de autenticação previamente definidas pelo usuário ou administrador do dispositivo e se assemelham com aquelas do sistema de controle de acesso baseado em atributos (ABAC) (Hu et al., 2013) e consistem de tuplas, com os seguintes atributos: $\mathcal{P}_j : \langle Id, AuthCapabilities, \mathcal{T}_{Id}, context \rangle = P_i^m$. Uma política $\mathcal{P}_j$ emprega o Id do dispositivo, os mecanismos de autenticação suportados $AuthCapabilities = \{m_1, m_2, \dots, m_j\}$, e o valor da confiança social, além do ambiente, para determinar o mecanismo de autenticação a ser aplicado. Algumas definições se fazem necessárias para se definir uma política e são apresentadas a seguir:

Definição 4.1 (Mapeamento da sociabilidade) A função $S(Id)$ calcula a sociabilidade de um nó a partir do seu Id

Definição 4.2 (Filtro sobre o Id) A função $\mathcal{F}(value)$ define um filtro com o valor $value$, que pode ser um conjunto, sobre o identificador de um dispositivo.

Definição 4.3 (Filtro sobre o Ambiente) A função $C(value)$ define um filtro com o valor $value$, que pode ser um conjunto, sobre o ambiente que um dispositivo se encontra.

Definição 4.4 (Política) Uma política $\mathcal{P}_j$ leva em consideração o Id , os mecanismos de autenticação suportados, a sociabilidade e o ambiente. Essas entradas são mapeadas para um determinado mecanismo de autenticação. As políticas têm a forma de uma tupla: $\langle Id, AuthCapabilities, \mathcal{T}_{Id}, Context \rangle = P_i^m$.

Um exemplo prático caracterização de uma política e uso das definições acima pode ser observado a seguir:

$$\mathcal{P}_1 : \langle \mathcal{F}(*), \{PUF, RSA\}, S(Id) > 0,5, C("escola") \rangle = P_1^{RSA}$$

Essa política, com identificador sequencial 1, se aplica para qualquer dispositivo ($\mathcal{F}(*)$), que suportem os mecanismos PUF (Função Física Não-clonável, do inglês, *Physical Unclonable Function*) e RSA (do inglês, *Rivest–Shamir–Adleman*) de autenticação. Além disso, a sociabilidade percebida pelo dispositivo sobre o outro dispositivo deve ser maior que 0,5. Há uma restrição no ambiente de aplicação dessa política, que no exemplo é *escola* (filtro $C("escola")$). Outros exemplos de definição de políticas podem ser observados na Subseção 4.3.1. Assim, após a determinação da política adequada aquele ambiente e dispositivo feita pelo SPOL, o SADPT aplica-a e instrui o dispositivo a utilizar o mecanismo de autenticação selecionado para aquela interação.

4.3 FUNCIONAMENTO

Esta seção detalha o funcionamento do sistema GALENA na seleção de perfis de autenticação e na resiliência diante do ataque de difamação. O sistema atua em quatro fases: (i) Descoberta, (ii) Sociabilização, (iii) Aplicação de Regras e, por fim, (iv) Autenticação para posterior tomada de serviços. A **Gerência de Descoberta** atua nas fases (i), (iii) e (iv) do sistema. Na fase (i), o **Serviço de Descoberta de Vizinhança** (SDES) opera continuamente e periodicamente enviando mensagens de presença a todos os dispositivos que estejam dentro de seu raio de transmissão, dessa forma os dispositivos podem encontrar uns aos outros a medida que eles se movimentam. Conforme o SDES descobre os dispositivos vizinhos, ele insere os dispositivos descobertos na estrutura de vizinhança.

Ao mesmo tempo que o SDES opera, o **Serviço de Descoberta de Capacidades** (SDCAP) utiliza a estrutura de vizinhança para consultar os outros dispositivos e determinar quais serviços eles proveem e quais mecanismos de autenticação eles suportam. Após essa consulta, o SDCAP armazena a resposta em uma estrutura que associa o identificador (*Id*) de cada dispositivo com os seus serviços e mecanismos de segurança suportados. Ele também responde a requisições de outros dispositivos sobre a capacidade do dispositivo que ele está sendo executado. É importante ressaltar que esses serviços limpam periodicamente as estruturas que eles gerenciam para não sobrecarregarem o dispositivo com o armazenamento de dados obsoletos. Durante a fase (i), o dispositivo – autonomamente ou por iniciativa do usuário – irá solicitar ou receber a solicitação de serviço de algum dos outros dispositivos vizinhos. Porém, para que os dispositivos interajam eles precisam estar autenticados para garantir a integridade e confidencialidade da comunicação. Para isso, eles determinam adaptativamente e autonomamente qual mecanismo de autenticação eles utilizarão para proteger a comunicação. Desse modo, inicia-se a fase de sociabilização.

A **Gerência Social** atua na fase de sociabilização – fase (ii) – a fim de obter os dados sociais para construir o grafo das relações sociais. Quando o dispositivo recebe alguma solicitação de dados sociais, o **Serviço de Validação de Origem** verifica sua assinatura MAC (*Data Provenance*). Caso a assinatura seja considerada válida, o SVOR repassa a solicitação para o **Serviço de Interação Social e Confiança**. Este serviço recupera a confiança social sobre o dispositivo que está sendo requerida a informação e repassa para o primeiro serviço para assinatura da mensagem e seu posterior envio. Caso o SVOR não considere a mensagem válida durante verificação da *Data Provenance*, ela é descartada. Sua invalidez pode sinalizar uma tentativa de ataque difamação, onde um dos dispositivos conhecidos está tentando diminuir a confiança do dispositivo alvo. Alternativamente, o dispositivo pode requisitar dados sociais para outros dispositivos, através do SVOR. Após a recepção e validação dos dados pelo SVOR, eles são repassados ao SISCO, para posterior cálculo da confiança, de acordo com o Protocolo de Confiança Social descrito na Subseção 4.2.2.1. Após o SISCO calcular o valor da confiança, ele a envia ao SPOL, iniciando, assim, a terceira fase, correspondente a Aplicação de Regras.

Durante a Aplicação de Regras, fase (iii), o **Serviço de Políticas** (SPOL) recebe o atual ambiente onde o dispositivo se encontra, através do Serviço de Localização (SLOC), e os dados sociais advindos do Serviço de Interação Social e Confiança (SISCO). Além disso, ele obtém as informações sobre os mecanismos de autenticação que o outro dispositivo suporta através do SDCAP. Em seguida, o Serviço de Políticas obtém as políticas configuradas e faz sua aplicação, priorizando aquelas mais específicas em detrimento das mais amplas. As políticas ditarão qual mecanismo de autenticação a ser empregado para comunicação e suas configurações associadas. Após a aplicação de regras da política determinada, o SADPT instrui o dispositivo a utilizar o mecanismo de autenticação selecionado para proteger a comunicação. A autenticação, prestação

e/ou obtenção de serviço constituem a quarta e última fase do sistema (fase *iv*); ela ocorre entre os dispositivos sem a participação direta do GALENA, visto que ele somente configura o mecanismo de autenticação determinado pela política.

4.3.1 Exemplo de Funcionamento em um Sistema de Transporte Inteligente

Considere um ambiente IoT de Sistemas de Transporte Inteligente com os seguintes dispositivos IoT: Um veículo inteligente, um semáforo inteligente, um dispositivo de iluminação pública inteligente e um usuário com um dispositivo pessoal, como um smartphone, ilustrado na Figura 4.3. Estes dispositivos e seus serviços baseiam-se em Marche et al. (2018). Os dispositivos são identificados, respectivamente, pelos *Ids*, *A*, *B*, *C* e *D*. Na fase de Descoberta (fase *i*), o dispositivo *A* descobre os dispositivos vizinhos (*B*, *C* e *D*) e os serviços oferecidos por eles. Por iniciativa do usuário ele requisitará o serviço de Informação de Tráfego, oferecido pelo dispositivo *D*.

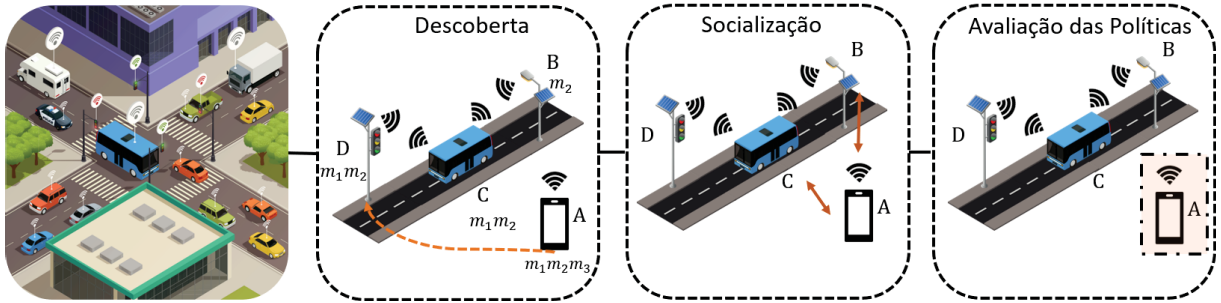


Figura 4.3: Funcionamento do GALENA em um Sistema de Transporte Inteligente

Na fase (*ii*), a de Sociabilização, o dispositivo *A* requisita aos dispositivos vizinhos, *B* e *C*, o *score* social que eles têm a respeito de *D*. O SVOR do dispositivo *A* valida as repostas de *B* e *C* e as repassa ao SISCO. Assumindo que $S_B^D = 0,7$ e $S_C^D = 0,8$ representam a confiança de *C* e *B*, respectivamente, em relação a *D*. O SISCO determina o valor de *R*, da Equação 4.1, como 0,75. Considere que os dispositivos *D* e *A* não possuem serviços em comum mas estão próximos, de maneira que $LOR = 0,95$ e $WOR = 0$. Ainda, os dispositivos nunca interagiram, logo a confiança direta também é zero. Os pesos da equação foram configurados como $\alpha = 0,5$, $\beta = 0$ e $\gamma = 0,5$ e $\delta = 0,5$, de modo que a confiança final é $S_A^D = 0,85$.

O ataque de Difamação ocorre durante a fase (*ii*), de sociabilização. Para isso, o dispositivo *C* – o atacante – dará uma recomendação abaixo do *score* real, ou seja, ele enviará $S_C^D < 0,7$, fazendo com que a confiança S_D^A seja diminuída, como na Figura 4.4(a). A diminuição da confiança levará a uma negação de serviço, a depender da política configurada; Note, ainda, que neste tipo de difamação, o atacante usa sua própria identificação. Desse modo, a resiliência diante do ataque consiste na configuração dos parâmetros das Equações 4.1 e 4.2. Já no segundo tipo de difamação, o atacante também enviará $S_B^D < 0,7$, porém com outra identificação, e.g. com $Id = E$, alterando essa confiança para S_E^A no recebimento, que pode ser observado o na Figura 4.4(b). Como isso ocorre depois da fase de descoberta, o SVOR tentará validar a origem da mensagem, mas falhará por não conhecer nenhum dispositivo *E* e descartará a recomendação.

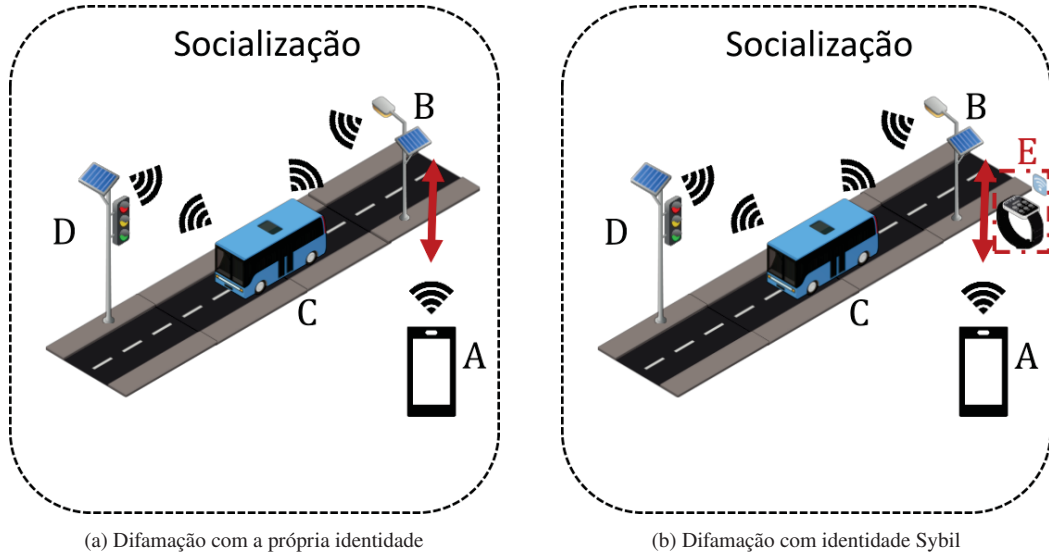


Figura 4.4: Ataque no cenário exemplo

Na fase (iii), de Aplicação de Políticas, o Serviço de Políticas recebe $S_A^D A$ e o ambiente – advindo do Serviço de Localização – determinado como “universidade”. As regras configuradas no dispositivo são as seguintes:

$$\begin{aligned}
 \mathcal{P}_1 : \langle \mathcal{F}(Id, *), \{PUF, RSA\}, S(Id) > 0, 9, C("casa") \rangle &= P_1^{PUF} \\
 \mathcal{P}_2 : \langle \mathcal{F}(Id, *), \{ECC, RSA\}, S(Id) > 0, 8, C(*) \rangle &= P_1^{ECC} \\
 \mathcal{P}_3 : \langle \mathcal{F}(Id, *), \{ECC, RSA\}, S(Id) > 0, 8, C("universidade") \rangle &= P_2^{ECC}
 \end{aligned}$$

Desse modo, o SPOL determina que a regra a ser aplicada é a $\mathcal{P}_3$, pois ela contém a combinação exata do ambiente. Essa política dita ao SADPT que configure no dispositivo o mecanismo de autenticação P_2^{ECC} . Ressalta-se que essas fases também ocorrem paralelamente no dispositivo A. Na fase (iv), considerando que a Sociabilização ocorreu sem ataques, os dispositivos se autenticam utilizando o mecanismo de autenticação selecionado (P_2^{ECC}) e interagem provendo e consumindo o serviço de Informação de Tráfego, como requisitado no começo da interação.

4.4 RESUMO

Este capítulo descreveu o sistema GALENA para gestão adaptativa da autenticação baseada na confiança social e resistente a ataques de difamação. Definiu-se os ambientes IoT e a interação social existente entre os dispositivos e o impacto do ataque de difamação. Em seguida, detalhou-se a arquitetura do sistema e o seu funcionamento. A descrição do funcionamento destacou a relevância da confiança social no processo de adaptação da autenticação dos dispositivos. Ao final, detalhou-se o funcionamento do GALENA e como ele atua para garantir a adaptação da autenticação ao selecionar o mecanismo de autenticação adequado a uma determinada interação.

5 AVALIAÇÃO

Este capítulo apresenta uma avaliação do sistema GALENA para gerência adaptativa de autenticação baseada em confiança social resiliente a ataques de difamação. A avaliação tem como objetivo analisar a eficiência do sistema em selecionar adaptativamente o perfil adequado de autenticação entre os dispositivos de acordo com as políticas definidas, ambiente e sociabilidade percebida, além de resistir a manipulações da confiança social. Assim, dois aspectos do sistema são avaliados: a sua capacidade de adaptação e aspecto social, além de aspectos de segurança quanto a difamação. A Seção 5.1 descreve a implementação do GALENA no simulador NS-3. A Seção 5.2 detalha o cenário de teste empregado nas simulações, bem como os parâmetros de simulação configurados e as políticas de segurança empregadas. A Seção 5.3 detalha as métricas para aferir o desempenho e a segurança do sistema. A Seção 5.4 analisa e discute os resultados obtidos na avaliação.

5.1 IMPLEMENTAÇÃO

O GALENA¹ foi implementado e avaliado pelo simulador discreto de eventos NS-3 (Network Simulator 3) (Riley e Henderson, 2010), versão 3.29, dado ao seu emprego no âmbito científico para o estudo de novas soluções para uso em redes. O NS-3 é uma ferramenta de código aberto, codificado na linguagem C++ com suite de *build* em python. O NS-3 suporta os principais protocolos de comunicação de redes, oferecendo condições de se avaliar soluções no contexto de vários tipos de redes, inclusive Internet das Coisas (IoT). Além disso, o simulador é capaz de ler *traces* de mobilidade e também de simular a mobilidade aleatória dos dispositivos. Este simulador também provê diversos módulos que contêm os principais protocolos de comunicação no contexto da IoT, incluindo aqueles capazes de simular o protocolo de rede IPv6, sua adaptação para redes baseadas no protocolo IEEE 802.15.4, a camada de tradução 6LoWPAN e o protocolo Wi-Fi (IEEE 802.11).

De acordo com a arquitetura do simulador, o GALENA foi codificado como um *ns3::Application*, intitulada *GalenaApplication*, e posteriormente implantada em cada dispositivo simulado. É nessa aplicação que as estruturas de controle de vizinhança e capacidades se localizam, ela também orquestra a comunicação entre os serviços e funciona também como o SADPT. O SDES e o SDCAP foram implementados como funções do *GalenaApplication* que atualizam as estruturas de vizinhança e capacidades. O SLOC também foi implementado dentro do *GalenaApplication* e acessa diretamente o estado do simulador para obter a distância do outro dispositivo. As funções relacionadas a manutenção da confiança (SISCO) foram implementadas em um módulo independente chamado *trustManager* que contém as funções relacionadas a atualização e cálculo da confiança. O *trustManager* tem funções para obter as confianças direta e indireta e atualiza as interações positivas quando é instruído pelo *GalenaApplication*. Do mesmo modo, as funções relacionadas às políticas (SPOL) foram abstraídas em um *policyManager*, que controla a inserção e avaliação de políticas. O *policyManager* possui duas funções externas, uma para inserir políticas no banco de políticas e outra para determinar uma política com base nos parâmetros enviados pelo *galenaApplication*. O *policyManager* também possui funções que avaliam cada componente de uma política.

O simulador NS-3 oferece uma série de pontos de interceptação (do inglês, *hooks*) para a execução de funções definidas pelo usuário (também chamadas de *callbacks*) quando

¹Disponível em <https://github.com/yanuehara/galena>

determinado evento dentro da simulação ocorrer. Esses *hooks* permitiram a captura do RSSI e a assinatura das mensagens sociais trocadas durante o envio e recebimento das mensagens trocadas, possibilitando que a parte de segurança do GALENA fosse implementada. O *callback ns3::WifiPhy::MonitorSnifferTx* permitiu a interceptação das mensagens enviadas pelo dispositivo e a assinatura dos pacotes que carregavam informações sociais. Como os pacotes não podem ser modificados nesse estado a assinatura do pacote foi inserida em uma tabela global dentro da simulação. Do mesmo modo, o *callback ns3::WifiPhy::MonitorSnifferRx* permitiu a interceptação do pacote que chegava ao dispositivo e a verificação da sua assinatura, sinalizando para o GalenaApplication se ela era válida ou inválida. As funções de criptografia foram providas pela biblioteca *Sodium* (Denis e Contributors, 2013) na versão *1.0.18-stable*, descrita como uma moderna biblioteca para encriptação, desencriptação, assinatura e hashings de senhas. Para geração dos HMACs foi empregada a função *crypto_generichash* dessa biblioteca, que implementa a função de *hashing* BLAKE2b (Saarinen e Aumasson, 2015). Esse arcabouço de funções e *callbacks* constituem o SVOR e implementam a *Data Provenance* dos dados sociais trocados dentro da simulação.

5.2 AMBIENTE E CONFIGURAÇÕES

As simulações ocorreram dentro do mesmo ambiente, análogo a uma *Smart City* com dispositivos pessoais – smartphones – sendo carregados por seus donos. Dentro desse ambiente, temos três cenários – com 200 e 400 – permitindo avaliar o comportamento do GALENA na adaptação do mecanismo de autenticação. Assume-se que todos os dispositivos na rede oferecem um determinado conjunto de serviços e suportam um conjunto de mecanismos de autenticação. Os serviços oferecidos pelos dispositivos foram obtidos do dataset de (Marche et al., 2018), voltado especialmente para simulações de redes de Internet das Coisas Sociais (SIoT) e correspondem ao conjunto *Localização, Data e horário, Presença, Ambiente, Consumo de Energia e Movimento* que caracterizam o tipo de dispositivo “Celular pessoal” contido no *dataset*. Ainda, os dispositivos suportam os seguintes mecanismos de autenticação: RSA, ECC, autenticação simétrica (identificado por SIM) e sem senha (NOPASS). Os cenários avaliados correspondem a cenários com 200 e 400 dispositivos, com mobilidade aleatória (através da função *RandomWalk2dMobilityModel* do NS-3) dentro de um espaço de 1600x1600 metros. Esses parâmetros são comuns a todas as configurações e estão sumarizadas na Tabela 5.1.

Os cenários foram divididos em 21 configurações que correspondem as configurações possíveis dos parâmetros α , β , γ e δ das Equações 4.2 e 4.1. Além disso, para os cenários de ataque, foram considerados os quatro tipos de ataque de difamação, detalhados na Subseção 4.1.3: Identificação própria com Difamação Constante (**DCP**), Identificação Sybil com Difamação Constante (**DSP**), Identificação própria com Difamação Seletiva (**DCS**), Identificação Sybil com Difamação Seletiva (**DSS**). Cada uma das 21 configurações foi simulada também com os quatro tipos de ataque, resultando em 81 configurações nessa situação. Um resumo das configurações específicas pode ser visto na Tabela 5.2.

Tabela 5.1: Configuração comum dos cenários

Parâmetro	Valores
Quantidade de dispositivos	200 e 400
Tamanho da simulação	1600x1600
Tempo de simulação	360s
Mecanismos de autenticação	RSA, ECC, SIM e NOPASS

Tabela 5.2: Valores possíveis por parâmetro

Parâmetro	Valores
α	0,2, 0,3 e 0,5
β	0,2, 0,3 e 0,5
γ	0,2, 0,3 e 0,5
δ	0,2, 0,5 e 0,8

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

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

5.3 MÉTRICAS

A avaliação do GALENA ocorreu a partir da análise dos resultados obtidos das simulações. Elas refletem o comportamento do GALENA e caracterizam as relações que ocorreram durante a simulação. Para isso, definiu-se dois grupos de métricas para avaliação. Aquelas relacionadas a adaptação e relações sociais e as relacionadas a detecção do ataque de difamação. As primeiras caracterizam a adaptação propriamente dita e como a escolha dos fatores influencia no cálculo da confiança. As últimas traduzem o quão efetiva a Data Provenance é na detecção do ataque.

A análise da adaptação da autenticação se dá pelas métricas **Evolução da Confiança** (*EC*), **Média do Erro Absoluto** (*MEA*), **Acurácia da confiança** (*AC*), **Taxa de aplicação de Políticas** (*TAP*) e **Taxa de Compatibilidade** (*TCA*). Já as métricas relacionadas a segurança de GALENA contra os ataques de difamação consistem da **Taxa de Detecção** (T_{abs}), **Taxa de Falsos Positivos** (T_{fp}), **Taxa de Falsos Negativos** (T_{fn}) e **Acurácia** (T_{acc}). Desta maneira, as métricas serão detalhadas a seguir:

A **Evolução da Confiança** (*EC*) baseia-se no trabalho de (Chen et al., 2018) e mensura a média da confiança de todos os dispositivos em cada segundo de simulação, obtendo uma curva que mostra a evolução e manutenção dessa confiança com o passar do tempo. Os valores também foram separados nos componentes da confiança: Confiança, Confiança Direta, Confiança Indireta (Recomendações) e SOR. Na equação, t representa cada momento do tempo de simulação e N o total de dispositivos. $C_{i,j}^t$ indica a confiança de i para j no instante t . A *EC* é obtida através da Equação 5.1.

$$EC^t = \frac{\sum_{i,j} C_{i,j}^t}{|N|} \quad (5.1)$$

A **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 e baseia-se em (Tan et al., 2016). Ela permite determinar a qualidade das recomendações recebidas, i.e., se elas se aproximam da confiança do dispositivo. Na equação, C_i indica a média de confiança em relação ao dispositivo i , R_i representa as recomendações a respeito de i e N_i a quantidade de dispositivos que recomendaram o dispositivo i . A acurácia da confiança é obtida através da Equação 5.2.

$$AC = \sum_i \frac{\frac{\sum R_i}{|N_i|}}{C_i} \quad (5.2)$$

O **Média do Erro Absoluto** (*MEA*) afere o erro entre a média do somatório da diferença entre as confianças de todos os dispositivos (N) da simulação analisada e do cenário de referência, permitindo aferir o quanto cada simulação se distancia ou se aproxima do cenário de referência,

traduzindo o quanto as alterações dos pesos da equação influenciam no cálculo da confiança. Este valor é obtido pela Equação 5.3 e se mantém entre 0 e 1.

$$MEA = \frac{\sum_{i,j} |C_{i,j}^{pred} - C_{i,j}^{act}|}{|N|} \quad (5.3)$$

A **Taxa de aplicação de Políticas** (TAP) mensura a porcentagem 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 aplicações da política. A TAP baseia-se em (Gwak et al., 2018) é definida pela Equação 5.4.

$$TAP = \frac{\sum int}{int_{\mathcal{P}}} \quad (5.4)$$

A **Taxa de Compatibilidade** (TCA) também baseia-se em (Gwak et al., 2018) e 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 o total de interações.

$$TCA = \frac{\sum_0^T \sum_{i,j} I_{i,j}}{int} \quad (5.5)$$

A seguir são detalhadas as métricas associadas sobre a segurança do CALENA diante de ataques de difamação:

A **Taxa de Detecção** (T_{det}) contabiliza os ataques identificados corretamente pelo GALENA através da Data Provenance. Ela corresponde a razão entre o total de detecções de recomendações que eram ataques, R_d , e a quantidade de ataques T_{atk} . Esta métrica apresenta valores entre 0% e 100% e é definida pela Equação 5.6.

$$T_{det} = \frac{\sum R_d}{T_{atk}} \quad (5.6)$$

A **Acurácia** (T_{acc}) quantifica a precisão da detecção do ataque de difamação. A T_{acc} é obtida através da razão entre a soma dos Verdadeiros Positivos e Verdadeiros Negativos e a quantidade de ataques ocorridos ($FalsePos + TrueNeg + FalseNeg + TruePos$). A Acurácia é determinada pela Equação 5.7 e apresenta valores na escala unitária, quanto mais perto de 1, mais preciso o sistema.

$$T_{acc} = \frac{TruePos + TrueNeg}{FalsePos + TrueNeg + FalseNeg + TruePos} \quad (5.7)$$

A **Taxa de Falsos Positivos** (T_{fp}) determina quantas vezes o GALENA identificou um ataque quando este não estava acontecendo. Seu valor é determinado pela razão entre os Falsos Positivos ($FalsePos$) e a soma de Falsos Positivos e Verdadeiros Negativos ($TrueNeg$) – dispositivos identificados corretamente como não atacantes. A Taxa de Falsos Positivos é determinada pela Equação 5.8 e apresenta valores na escala unitária.

$$T_{fp} = \frac{FalsePos}{FalsePos + TrueNeg} \quad (5.8)$$

A **Taxa de Falsos Negativos** (T_{fn}) determina quantas vezes o sistema identificou um ataque como uma recomendação legítima. Seu valor é determinado pela razão entre os Falsos Negativos ($FalseNeg$) e a soma dos Falsos Negativos e Verdadeiros Positivos ($TruePos$) – dispositivos legítimos identificados corretamente. A Taxa de Falsos Negativos pode ser obtida pela Equação 5.9 e também apresenta valores na escala unitária.

$$T_{fn} = \frac{FalseNeg}{FalseNeg + TruePos} \quad (5.9)$$

5.4 ANÁLISE DOS RESULTADOS E DISCUSSÃO

A análise dos resultados da avaliação do GALENA leva em conta o seu desempenho na adaptação com base nas relações sociais criadas e mantidas e a sua eficácia na detecção e mitigação do ataque de difamação através do uso de *Data Provenance*. Os dados brutos e processados gerados no processo de avaliação encontram-se disponíveis em (de Moraes, 2022).

5.4.1 Desempenho

Para analisar o comportamento dos dispositivos na criação e manutenção das relações sociais, os valores de confiança foram separados em suas partes constituintes: Confiança Direta e Indireta, Recomendações e SOR. Dessa forma, através da Evolução da Confiança (EC), podemos perceber como a escolha dos pesos das Equações 4.1 e 4.2 afetam a confiança final.

A Evolução da Confiança (EC) para as várias combinações de pesos dos parâmetros α , β , γ e δ no Cenário 1, correspondente a 200 dispositivos, pode ser vista na Figura 5.1. Cada grupo de gráficos representa uma configuração específica dos valores da Equação 4.2. Cada coluna, por sua vez, representa os valores de δ 0, 2, 0, 5 e 0, 8 da Equação 4.2. 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 é esperado porque o cenário contém poucos dispositivos em um grande espaço, fazendo com que eles se encontrem pouco. Assim, quando um dispositivo requisita o valor de confiança sobre um terceiro, essa resposta do emissor é 0, 5, indicando uma opinião neutra sobre esse terceiro. Ou seja, o dispositivo não tende a não confiar ($C_{i,j} < 0, 5$) nem a exibir alguma confiança ($C_{i,j} > 0, 5$).

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 a medida que os gráficos são visualizados da esquerda para direita. Entretanto, para algumas configurações, o SOR se mantém 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, percebe-se que a confiança se restringe ao intervalo entre 0, 8 e 1, 0, devido ao modo como o GALENA compõe a confiança; 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.

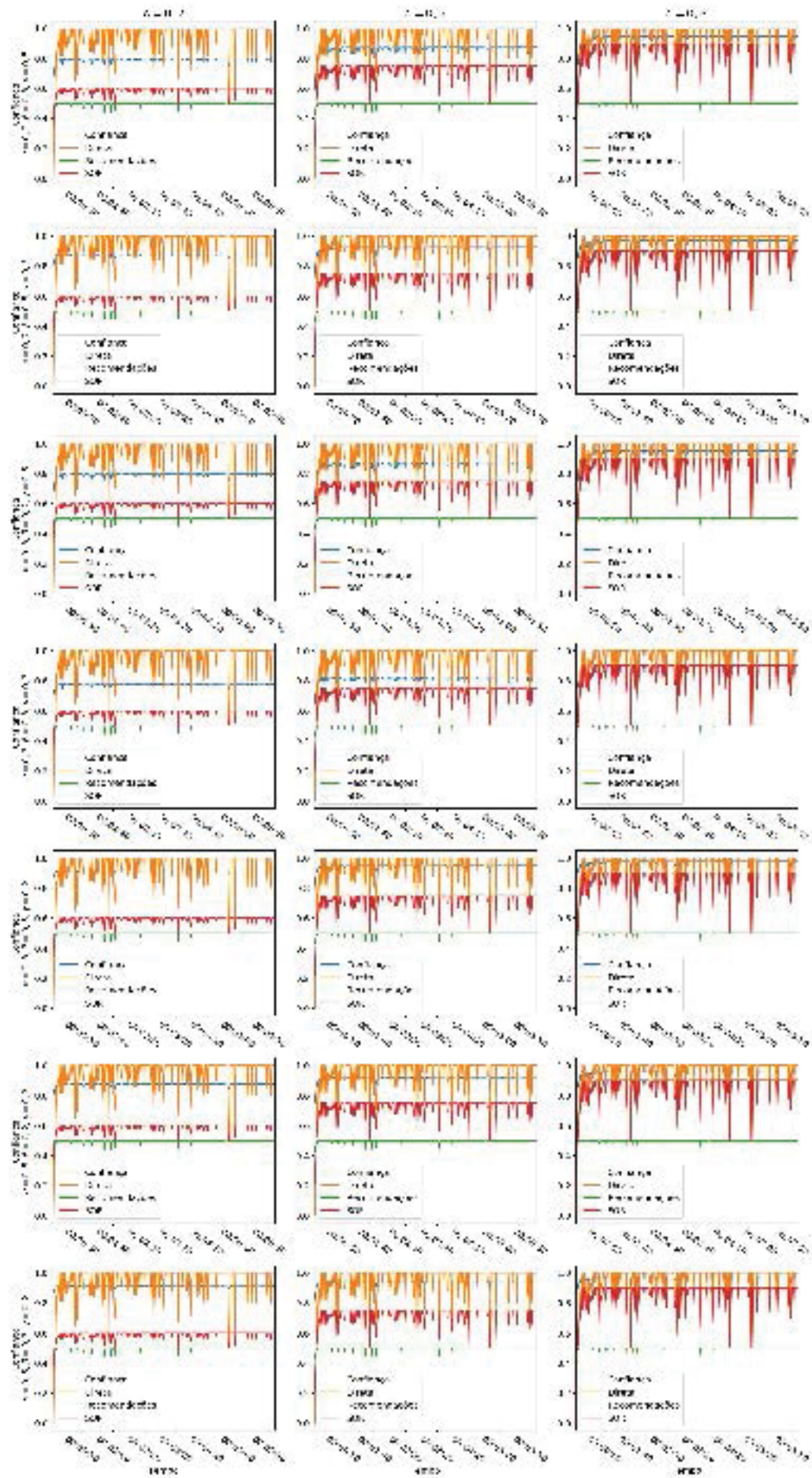


Figura 5.1: *EC* para o Cenário 1

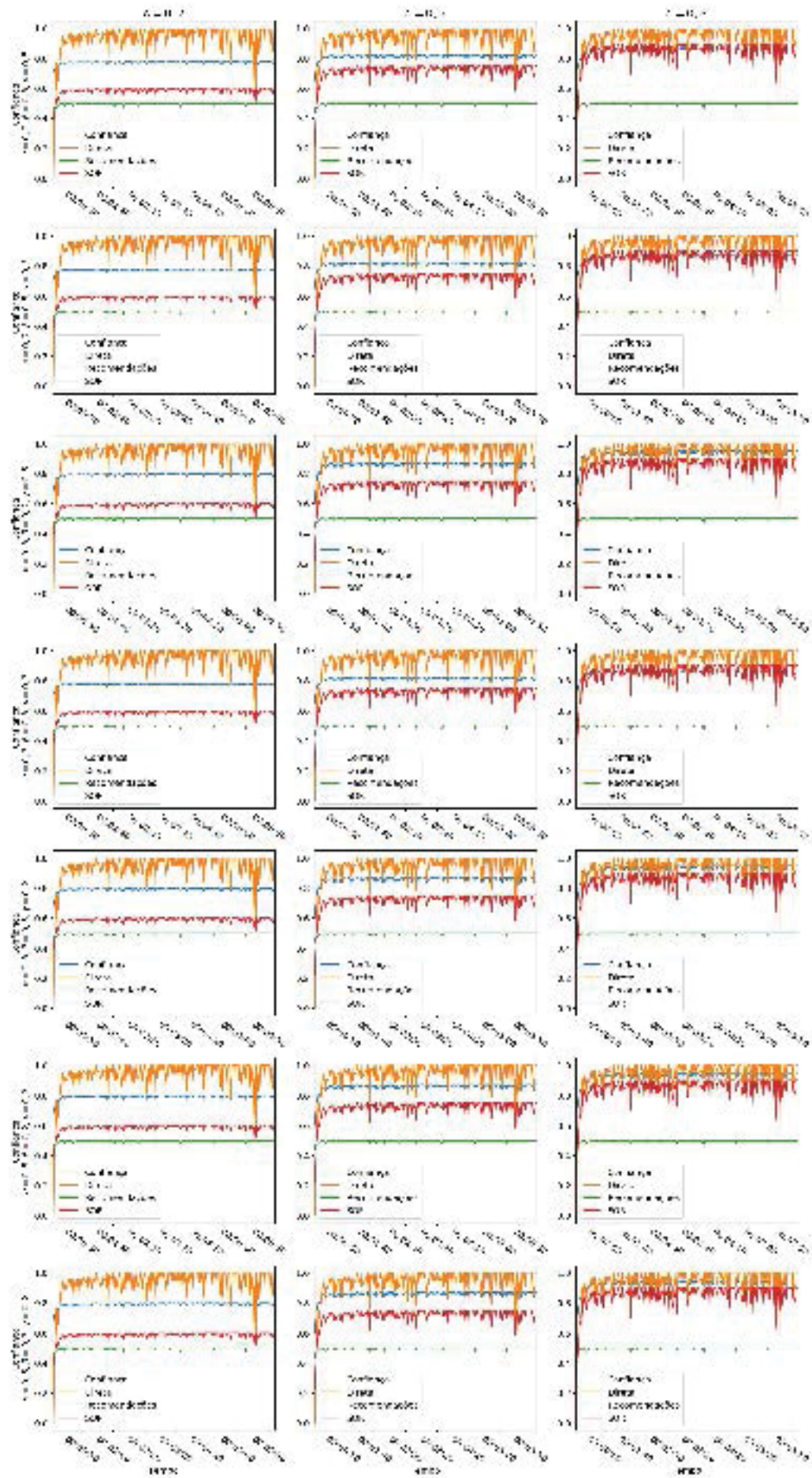


Figura 5.2: *EC* para o Cenário 2

A *EC* para as várias combinações de pesos dos parâmetros no Cenário 2 (400 dispositivos) pode ser vista na Figura 5.2. Os gráficos organizam-se da mesma maneira que no cenário anterior. Neste cenário, as recomendações também se mantiveram perto do valor 0,5, em razão da baixa interação entre os dispositivos devido aos poucos encontros ao longo do ambiente. Isso ocasiona que os dispositivos respondam aos pedidos de recomendação com o valor 0,5, para indicar um valor neutro de confiança de modo a não adicionar viés a confiança calculada. Além disso, o comportamento do SOR ainda é mais visível visto que ele atinge valores maiores a medida que os parâmetros γ e δ são maiores. Com δ igual a 0,2, gráficos da coluna mais a esquerda, percebe-se que o SOR não ultrapassa o limite de 0,6. Porém, para a configuração de δ igual a 0,5, ou seja, a confiança direta e indireta possuem com o mesmo peso, o SOR ultrapassa o limite anterior e se restringe ao intervalo 0,6 a 0,8. Por fim, quando atribui-se mais peso a confiança direta, o SOR ultrapassa o teto do intervalo anterior. Como o GALENA emprega o SOR para a composição da confiança final, percebe-se que a confiança também apresenta o mesmo comportamento. Inicialmente, para δ igual a 0,2 e 0,5, ela se restringe ao intervalo 0,6 a 0,8. Contudo, quando o valor de δ é 0,8 a confiança ultrapassa esse teto, indicando que os dispositivos têm alta confiança entre si e podem negociar um mecanismo de autenticação adequado para esses casos.

Pesos Par. Sociais				Cenários	
α	β	γ	δ	1	2
2	3	5	2	63,10%	59,59%
2	3	5	5	59,18%	64,37%
2	3	5	8	55,72%	55,98%
2	5	3	2	56,69%	63,34%
2	5	3	5	54,74%	59,59%
2	5	3	8	52,91%	55,98%
3	2	5	2	63,17%	63,34%
3	2	5	5	59,24%	55,98%
3	2	5	8	55,77%	59,43%
3	3	3	2	64,16%	59,43%
3	3	3	5	61,67%	61,89%
3	3	3	8	59,36%	63,34%
3	5	2	2	54,00%	61,89%
3	5	2	5	52,80%	63,34%
3	5	2	8	51,66%	64,37%
5	2	3	2	56,85%	64,37%
5	2	3	5	54,89%	59,43%
5	2	3	8	53,05%	61,89%
5	3	2	2	54,10%	59,59%
5	3	2	5	52,90%	59,43%
5	3	2	8	51,75%	55,98%

Tabela 5.3: Acurácia da Confiança (AC)

Apesar da Evolução da Confiança (*EC*) permitir obter um panorama da confiança e das recomendações durante a simulação, é preciso analisar a qualidade dessa confiança através da métrica Acurácia da Confiança (*AC*), sumarizada na Tabela 5.3, para os Cenários 1 e 2. A acurácia da confiança mede a razão entre a recomendação e a confiança para um dispositivo, com a conjectura de que essa razão tenderia para 100% conforme as recomendações alcançassem a confiança real (Tan et al., 2016). Para o cenário 1, percebe-se que a confiança apresentou valores de *AC* entre 51,66% e 61,16%. Como nesse cenário as recomendações se concentraram perto do valor 0,5, a *AC* demonstra que a confiança distanciou-se do valor das recomendações. No cenário 2, os valores de acurácia se mantiveram entre 55,98% e 64,37% demonstrando que também a confiança se distanciou das recomendações. Ao contrário da conjectura de (Tan et al., 2016), para essas configurações esse distanciamento mostra-se benéfico, pois as recomendações foram neutras em sua maioria. Logo, a confiança exibida nessas configurações traduz as relações sociais criadas entre os dispositivos.

Pesos Par. Sociais				Cenários	
α	β	γ	δ	1	2
2	3	5	2	0,02	0,01
2	3	5	5	0,04	0,04
2	3	5	8	0,10	0,10
2	5	3	2	0,06	0,06
2	5	3	5	0,10	0,10
2	5	3	8	0,13	0,13
3	2	5	2	0,02	0,02
3	2	5	5	0,04	0,04
3	2	5	8	0,10	0,10
3	3	3	2	0,03	0,03
3	3	3	5	0,0	0,0
3	3	3	8	0,03	0,03
3	5	2	2	0,10	0,02
3	5	2	5	0,12	0,04
3	5	2	8	0,15	0,10
5	2	3	2	0,05	0,02
5	2	3	5	0,09	0,04
5	2	3	8	0,13	0,10
5	3	2	2	0,10	0,02
5	3	2	5	0,12	0,04
5	3	2	8	0,15	0,10

Tabela 5.4: *MEA* dos Cenários

A Média do Erro Absoluto (*MEA*) indica como, a medida que os pesos são alterados, a confiança se distancia ou se aproxima de um valor considerado como “real”. Para o valor real da confiança, tomou-se a média das confianças da combinação $\alpha = \beta = \gamma = 0,33$ e $\delta = 0,5$. Essa configuração foi escolhida por apresentar o mesmo valor para cada componente da confiança e considerar de maneira equivalente as recomendações e a experiência própria. Os resultados da *MEA* encontram-se sumarizados na Tabela 5.4. Para uma mesma combinação de α , β , γ , percebe-se que a *MEA* aumenta a medida que δ também aumenta. Ainda, duas configurações ($\alpha = 0,2, \beta = 0,3, \gamma = 0,5, \delta = 0,5$ e $\alpha = 0,2, \beta = 0,3, \gamma = 0,3, \delta = 0,5$) obtiveram *MEA* = 0, indicando que a médias das confianças nessas configurações atingiu a mesma média do cenário de referência. Isso pode ter ocorrido devido a quantidade de interações ocorridas entre os dispositivos durante a simulação. Por fim, percebe-se que os maiores valores de *MEA* foram atingidos quando se deu mais importância para as relações LOR (balanceada por α) e WOR (balanceada por β) pois elas atingem valores altos e como estão contribuindo mais para a confiança o erro apresenta-se maior.

Configuração				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 5.5: TAP e TCA para o Cenário 1

Configuração				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%	88,90%	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%	88,90%	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%	88,90%	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%	88,90%	93,60%

Tabela 5.6: TAP e TCA para o Cenário 2

Em seguida analisa-se a taxa de aplicação de políticas (*TAP*) e a taxa de compatibilidade (*TCA*). Essas taxas traduzem a influência da variação da confiança na aplicação de políticas e seleção do mecanismo de autenticação. Para o Cenário 1, foi baixa a taxa de aplicação de políticas. A política $\mathcal{P}_3$ foi aplicada em 12 cenários com taxas de compatibilidade em 91%. E a $\mathcal{P}_2$ foi aplicada somente em 6 cenários, com uma taxa de aplicação de políticas de somente 0,07% do total de interações. A política $\mathcal{P}_1$, foi aplicada entre 4,7%, quando a $\mathcal{P}_3$ foi a mais aplicada, e 99,4% das interações nos cenários. Mesmo com a baixa densidade de dispositivo, o que permite menos interações, a *TCA* atingiu valores entre 96% e 99%, demonstrando que a o GALENA conseguiu negociar autonomamente um mecanismo de autenticação adequado a um nível de confiança social. Esses valores se encontram sumarizados na Tabela 5.5. No Cenário 2, com maior quantidade de dispositivos, a *TCA* se mostrou mais alta. Na maior parte dos cenários foi aplicada unicamente a política $\mathcal{P}_1$. Porém, em cerca de 12 deles, foram aplicadas conjuntamente as políticas $\mathcal{P}_2$ e $\mathcal{P}_3$, mostrando que o GALENA é capaz de alterar a política considerada a medida que altera-se a confiança. Nas simulações em que somente $\mathcal{P}_1$ foi aplicada, ela atingiu uma *TAP* de 99%, com *TCA* igual valor. Nas simulações em que $\mathcal{P}_1$ e $\mathcal{P}_2$ foram aplicadas, $TAP_{\mathcal{P}_1} = 98\%$ e $TAP_{\mathcal{P}_2} = 0,02\%$. Por fim, nas simulações em que todas as políticas foram aplicadas, $TAP_{\mathcal{P}_1} = 4\%$ e $TAP_{\mathcal{P}_2} = 0,02\%$ e $TAP_{\mathcal{P}_3} = 89\%$. Para o Cenário 2, em todas as simulações, o GALENA foi capaz de atingir uma *TCA* acima de 93%, chegando a 99% em algumas simulações. Isso demonstra a capacidade do GALENA na adaptação do mecanismo de autenticação empregado pelo dispositivo. Esses valores se encontram sumarizados na Tabela 5.6.

5.4.2 Robustez das recomendações sociais

Esta avaliação tem o objetivo de aferir a influência e os danos do ataque de difamação e seus modos comportamentos nas recomendações recebidas pelos dispositivos IoT, e como esses ataques afetam a aplicação de políticas estabelecidas para a configuração do sistema de autenticação aplicado num dado momento. Analisou-se o impacto e a afetividade da detecção e mitigação do GALENA em relação aos diferentes comportamentos do ataque de difamação ao mensurar as todas métricas mencionadas anteriormente. Assim, foram avaliados nos dois cenários de simulação quatro comportamentos de ataques de difamação: Identificação própria com

Difamação Constante (**DCP**), Identificação Sybil com Difamação Constante (**DSP**), Identificação própria com Difamação Seletiva (**DCS**), Identificação Sybil com Difamação Seletiva (**DSS**). A percentagem de atacantes foi de 20% em todas configurações analisadas

Visto que o ataque de difamação impacta nas recomendações dos dispositivos, os seus efeitos sobre o GALENA tornam-se mais evidentes na manutenção da confiança, na acurácia e na aplicação das políticas. De maneira geral, os gráficos relacionados à *EC* das configurações com ataque mostram-se mais incoerentes, com curvas com grandes variações. Contudo, eles ainda apresentam comportamentos similares aos vistos na Subseção 5.4.1: para valores de γ altos ou tanto maior quanto for δ , o SOR atingiu valores maiores. Por exemplo, para a configuração $\alpha = 0,2$, $\beta = 0,3$, $\gamma = 0,5$ e com $\delta = 0,2$, $\delta = 0,5$, $\delta = 0,8$, o SOR atingiu máximas de 0,6, 0,75 e 0,9, respectivamente.

A *EC* ao longo do tempo exibiu, nos gráficos das Figuras 5.3 e 5.4, valores muito próximos diante dos ataques com os comportamentos de difamação **DCP** e **DCS** no Cenário 1. Isso ocorre devido a baixa quantidade de dispositivos na simulação. Também percebe-se que as curvas de recomendação se aproxima de 0,4, principalmente quando elas têm maior peso (δ). Isso é evidenciado nas médias dos valores de recomendação que variaram entre 0,4 e 0,45. Essa média representa um valor cerca de 0,04, quando dá-se menor peso ao SOR (γ) e/ou recomendações (δ), a 0,09, quando $\gamma = 0,5$ e/ou $\delta = 0,8$, menores que a configuração sem ataque. Os valores de SOR mantiveram a tendência que exibiam antes, tanto maiores quanto o valor de δ . Essa tendência só não se manteve nas configurações $\alpha = 0,2$, $\beta = 0,5$, $\gamma = 0,3$ e $\delta = 0,8$ e $\alpha = 0,3$, $\beta = 0,3$, $\gamma = 0,3$ e $\delta = 0,8$, nos dois comportamentos de ataque, devido a quantidade menor interações nessas configurações. Finalmente, a confiança mostrou-se análoga à configuração de referência, alcançando médias entre 0,86 e 0,91, que significam erros entre 0,01 abaixo da referência a 0,13 acima da referência.

Para os comportamentos **DSP** e **DSS**, percebe-se que as recomendações também se aproximam de 0,4 exibindo um comportamento consistente nas simulações. Isso é demonstrado pelas médias que consistentemente atingiram cerca de 0,44 quando consideradas duas casas decimais. Nesses comportamentos, a recomendação se mostrou 0,05 e 0,04 menores do que o valor de recomendação média das configurações sem ataque, demonstrando a capacidade do GALENA em empregar a *Data Provenance* para filtrar recomendações maliciosas. Aqui a tendência do SOR também se manteve exibindo diferenças nulas ou entre 0,02 a 0,04 menores que o cenário de referência. Por fim, a confiança apresentou ou nenhum erro em relação à configuração sem ataque, ou erros mínimos, da ordem de 0,01 abaixo da referência. O comportamento das recomendações, SOR e Confiança para o Cenário 1 nos diferentes comportamentos de ataque pode ser conferido nos gráficos das Figuras 5.3 a 5.6.

No Cenário 2, o comportamento das recomendações no **DCP** e **DCS** é ainda mais evidente, com seu valor centrando em 0,4 com maior intensidade. Ao contrário do Cenário 1 com esses comportamentos, os *ECs* mostram-se diferentes, principalmente devido a maior quantidade de dispositivos na simulação, e consequentemente a maior possibilidade de interações. Nessas configurações, as recomendações atingiram uma média de 0,39 e 0,44 respectivamente que representam uma diferença de 0,09 e 0,05 em relação a referência. O SOR apresentou o mesmo comportamento geral, alcançando diferenças entre 0,01 e 0,07 entre as médias alcançadas e as da configuração sem ataque. Finalmente, a confiança mostrou-se próxima do cenário de referência variando entre 0,75 e 0,95. Em cerca de 28 configurações, dos comportamentos **DCP** e **DCS**, a confiança superou a média atingida na referência, principalmente devido à quantidade de interações ocorridas. Nesses casos as confianças se apresentaram 0,01 e 0,11 maiores que a referência. Em outras 8 configurações, as diferenças se encontraram entre 0,01 e 0,03 menores que a referência. Por fim, em 6 outras configurações a diferença foi negligível.

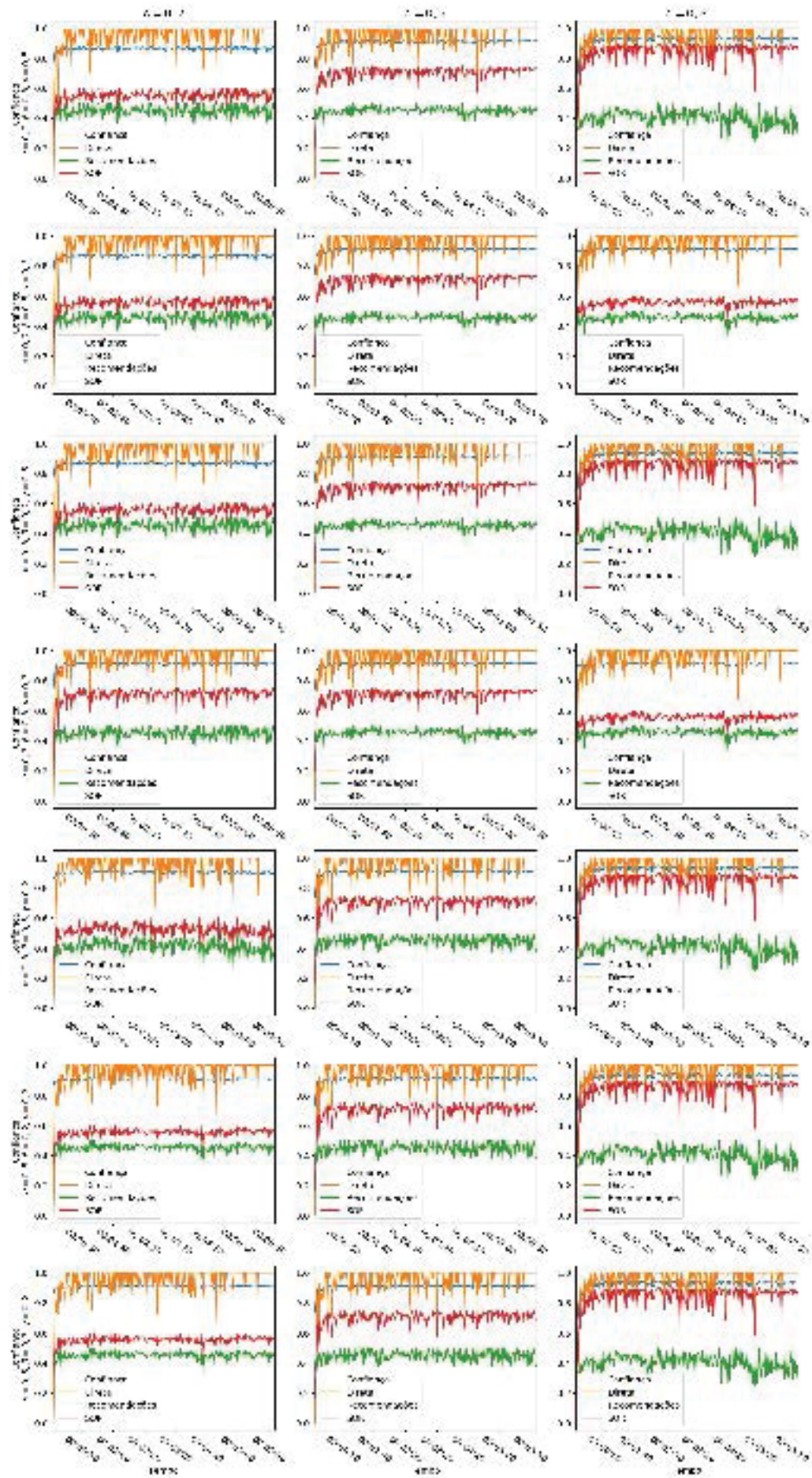


Figura 5.3: EC para o Cenário 1 - DCP

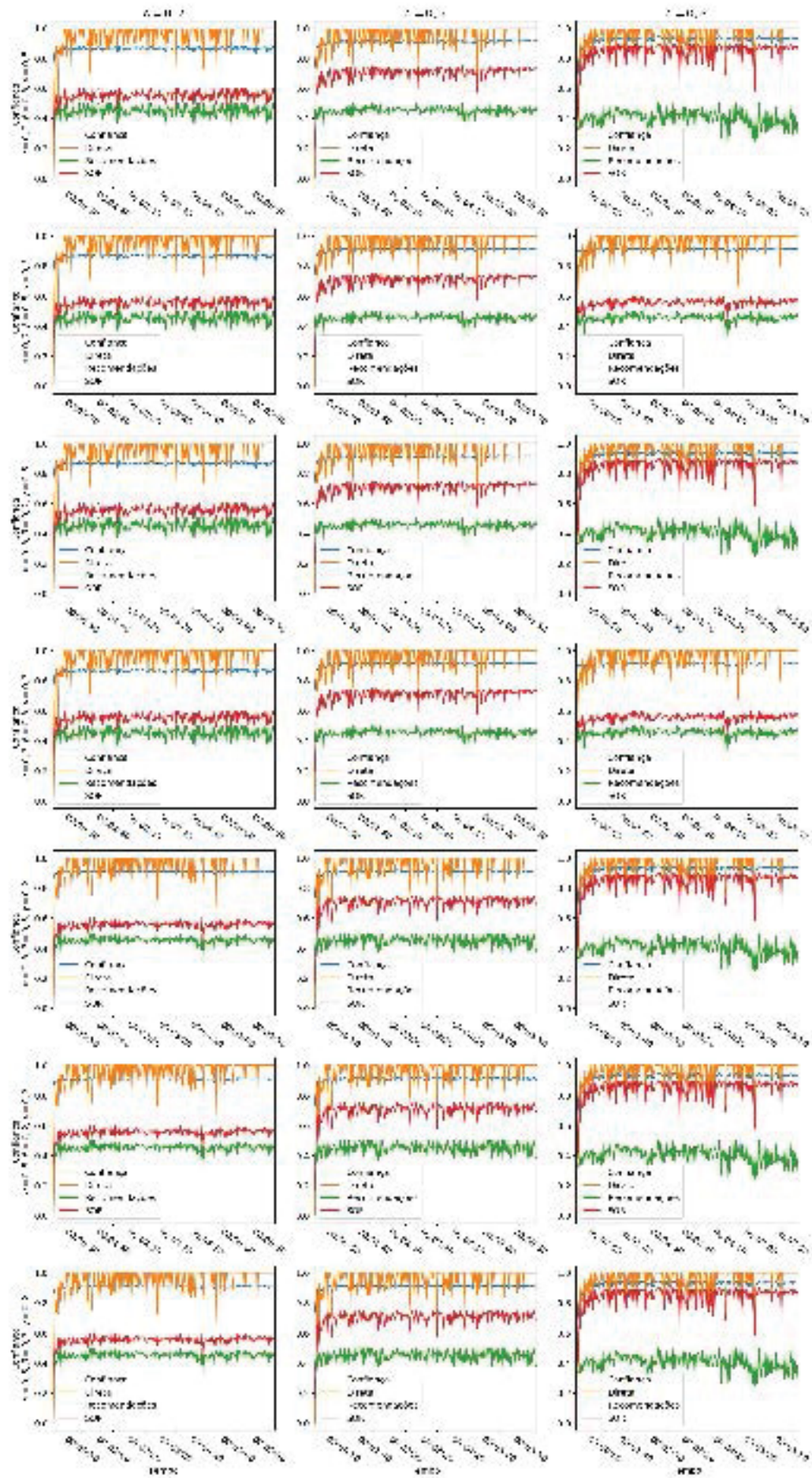


Figura 5.4: EC para o Cenário 1 - DCS

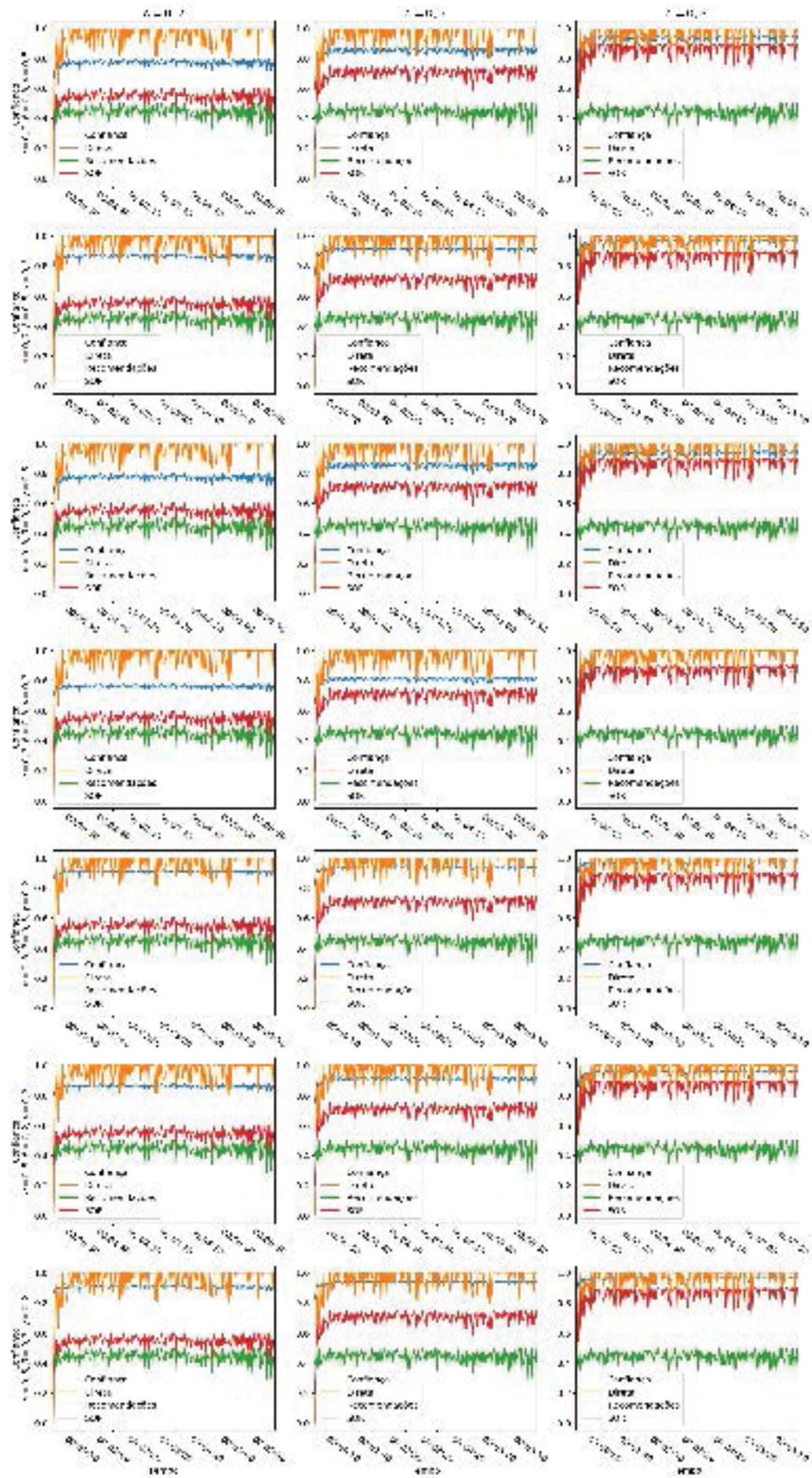


Figura 5.5: EC para o Cenário 1 - DSP

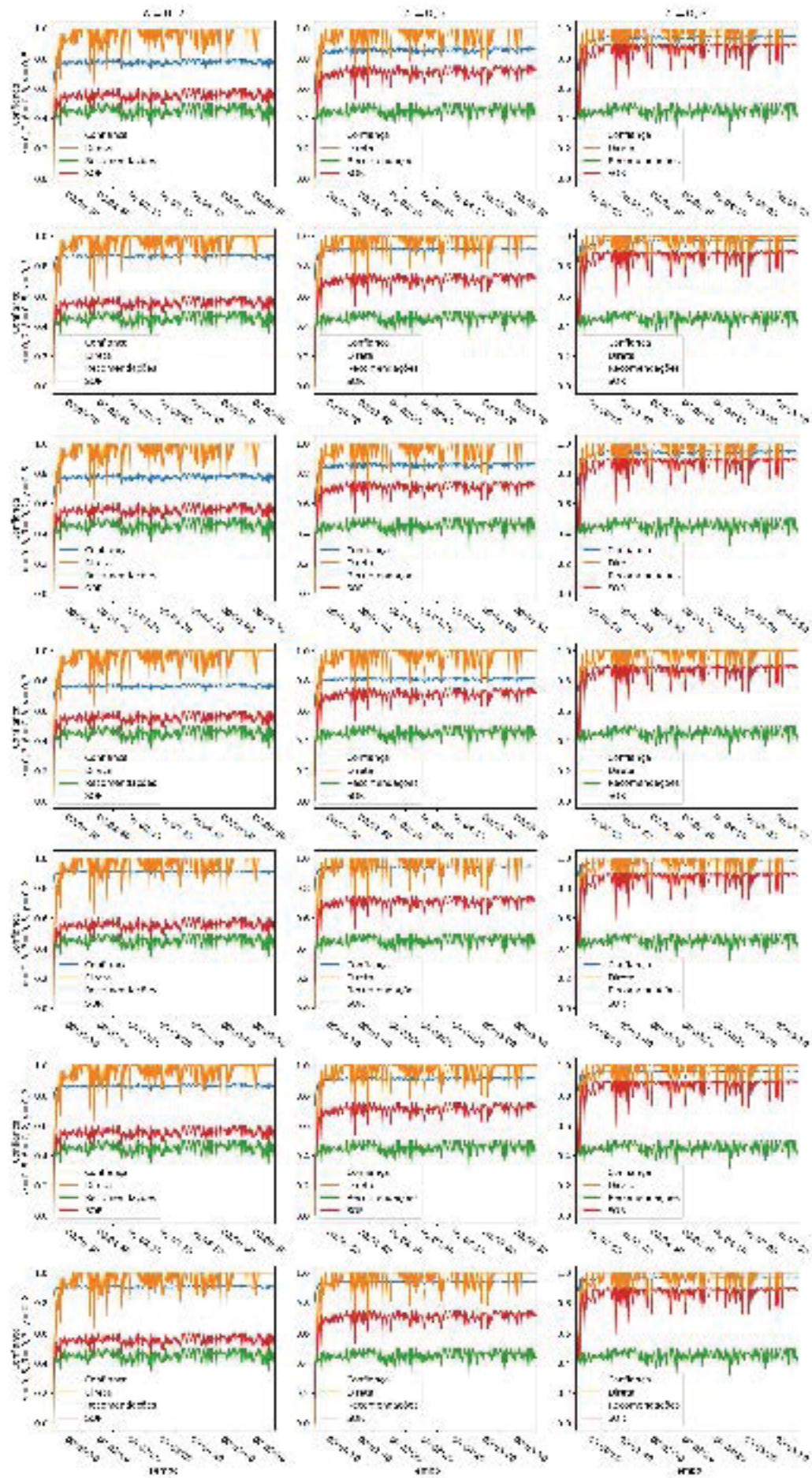


Figura 5.6: EC para o Cenário 1 - DSS

Os comportamentos **DSP** e **DSS** diante de ambos os cenários apresentaram a mesma tendência das outras configurações, com valores de recomendação se elevando um pouco acima do centro de 0,4, atingindo 0,46 consistentemente nas configurações com os dois comportamentos. Do mesmo modo, as diferenças da recomendação mantiveram-se em 0,03 abaixo da referência. Nessas configurações, o SOR exibiu o mesmo comportamento anterior, atingindo valores maiores a medida que δ aumenta. Porém, com as recomendações atingindo valores maiores, o SOR também se eleva e exibe uma tendência mais próxima da configuração de referência. Evidencia-se esse comportamento através das diferenças do SOR, que novamente foram nulas ou entre 0,01 e 0,04 menores que a configuração de referência. O aumento do valor do SOR também proporcionou a confiança atingir valores mais altos. Também nesses comportamentos, em cerca de 28 configurações, a confiança superou a média atingida na referência, principalmente devido à quantidade de interações ocorridas. Nesses casos as confianças se apresentaram 0,02 e 0,11 maiores que a referência. Nas outras duas configurações, as diferenças se encontraram entre 0,01 menores que a referência. As 18 configurações restantes não mostraram diferenças significativas em relação à configuração de referência. Isso deve-se ao emprego da *Data Provenance* que permite ao dispositivo detectar e descartar recomendações difamatórias quando o comportamento da difamação está associado ao ataque Sybil. Os comportamentos do Cenário 2 podem ser conferidos nos gráficos das Figuras B.1 a B.4, localizadas no Apêndice B.

Pesos Par. Sociais				Cenários	
α	β	γ	δ	1	2
2	3	5	2	51,03%	53,29%
2	3	5	5	50,48%	48,99%
2	3	5	8	44,85%	45,33%
2	5	3	2	51,03%	46,72%
2	5	3	5	50,48%	44,65%
2	5	3	8	49,78%	42,76%
3	2	5	2	51,03%	53,34%
3	2	5	5	50,47%	49,03%
3	2	5	8	44,85%	45,36%
3	3	3	2	49,03%	53,06%
3	3	3	5	50,48%	50,41%
3	3	3	8	49,78%	48,02%
3	5	2	2	43,78%	44,04%
3	5	2	5	49,03%	42,79%
3	5	2	8	44,85%	41,62%
5	2	3	2	49,78%	46,83%
5	2	3	5	49,03%	44,76%
5	2	3	8	44,85%	42,86%
5	3	2	2	49,78%	44,10%
5	3	2	5	49,03%	42,86%
5	3	2	8	44,85%	41,68%

Tabela 5.7: AC - DCP

Pesos Par. Sociais				Cenários	
α	β	γ	δ	1	2
2	3	5	2	51,03%	58,38%
2	3	5	5	50,48%	54,35%
2	3	5	8	44,85%	50,84%
2	5	3	2	51,03%	51,77%
2	5	3	5	50,48%	49,80%
2	5	3	8	49,78%	47,98%
3	2	5	2	51,03%	58,43%
3	2	5	5	50,48%	54,40%
3	2	5	8	44,85%	50,88%
3	3	3	2	51,03%	58,69%
3	3	3	5	50,48%	56,18%
3	3	3	8	49,78%	53,87%
3	5	2	2	49,78%	49,03%
3	5	2	5	49,03%	47,84%
3	5	2	8	44,85%	46,71%
5	2	3	2	49,78%	51,90%
5	2	3	5	49,03%	49,92%
5	2	3	8	44,85%	48,09%
5	3	2	2	49,86%	49,11%
5	3	2	5	49,03%	47,91%
5	3	2	8	44,85%	46,78%

Tabela 5.8: AC - DCS

Pesos Par. Sociais				Cenários	
α	β	γ	δ	1	2
2	3	5	2	57,09%	59,25%
2	3	5	5	52,78%	55,22%
2	3	5	8	49,08%	51,71%
2	5	3	2	50,58%	52,68%
2	5	3	5	48,47%	50,70%
2	5	3	8	46,54%	48,87%
3	2	5	2	57,13%	59,31%
3	2	5	5	52,82%	55,27%
3	2	5	8	49,11%	51,75%
3	3	3	2	57,33%	59,70%
3	3	3	5	54,65%	57,18%
3	3	3	8	52,20%	54,86%
3	5	2	2	47,88%	49,95%
3	5	2	5	46,60%	48,75%
3	5	2	8	45,39%	47,61%
5	2	3	2	50,68%	52,81%
5	2	3	5	48,56%	50,83%
5	2	3	8	46,62%	48,99%
5	3	2	2	47,94%	50,03%
5	3	2	5	46,66%	48,83%
5	3	2	8	45,45%	47,68%

Tabela 5.9: AC - DSP

Pesos Par. Sociais				Cenários	
α	β	γ	δ	1	2
2	3	5	2	57,89%	59,08%
2	3	5	5	53,58%	55,03%
2	3	5	8	49,87%	51,49%
2	5	3	2	51,42%	52,51%
2	5	3	5	49,31%	50,52%
2	5	3	8	47,36%	48,68%
3	2	5	2	57,91%	59,14%
3	2	5	5	53,60%	55,07%
3	2	5	8	49,88%	51,53%
3	3	3	2	58,25%	59,51%
3	3	3	5	55,55%	56,98%
3	3	3	8	53,09%	54,65%
3	5	2	2	48,72%	49,78%
3	5	2	5	47,43%	48,58%
3	5	2	8	46,21%	47,43%
5	2	3	2	51,47%	52,64%
5	2	3	5	49,35%	50,65%
5	2	3	8	47,40%	48,80%
5	3	2	2	48,74%	49,86%
5	3	2	5	47,46%	48,65%
5	3	2	8	46,24%	47,50%

Tabela 5.10: AC - DSS

Enquanto o *EC* demonstra um panorama geral do comportamento da Confiança no decorrer da simulação, o *AC* nos permite verificar o efeito dos ataques em relação a qualidade da confiança. As Tabelas 5.7 e 5.8 apresentam o *AC* para os comportamentos **DCP** e **DCS**. Quando comparados ao resultado com a configuração sem ataque da Seção 5.4.1, percebe-se que as porcentagens tornaram-se menores, atingindo valores tão baixos quanto cerca de 41%. Na configuração sem ataque o distanciamento da confiança em relação a recomendação (representada pelas porcentagens baixas de *AC*) demonstra que a Confiança atingida traduz as relações sociais criadas entre os dispositivos. Porém, nas configurações analisadas aqui, dado que havia um ataque alterando a recomendação, as porcentagens baixas demonstram a efetividade do ataque de difamação. Já nos comportamentos **DSP** e **DSS**, descritos nas Tabelas 5.9 e 5.10, a *AC* apresentou porcentagens compatíveis com os da configuração sem ataque demonstrando que a *Data Provenance* foi capaz de filtrar algumas das recomendações difamatórias.

A Média do Erro Absoluto (*MEA*) demonstra como, a medida que os pesos são alterados e o ataque de difamação tem seus diferentes comportamentos, a confiança se distancia ou se aproxima de um valor considerado como “real”. Para o valor real da confiança, tomou-se o *MEA* da combinação $\alpha = \beta = \gamma = 0,3$ e $\delta = 0,5$, nas configurações sem ataque da Seção 5.4.1 nos Cenários 1 e 2. Esse valor foi escolhido por representar uma configuração neutra em relação a importância de cada componente e considerar de maneira equivalente as recomendações e a experiência própria do dispositivo. As Tabelas 5.11 a 5.14 apresentam os *MEAs* das configurações com ataque, cada cenário foi comparado com seu respectivo *MEA*.

Para os comportamentos **DCP** e **DCS** o *MEA* exibiu o mesmo comportamento geral, tão maior quanto o peso das recomendações, nos dois cenários. Para o Cenário 1, o *MEA* diante dos comportamentos **DCP** e **DCS** apresentou erros de cerca de 0,05 em relação à configuração de referência em algumas configurações e erros compatíveis com aquela em outras configurações. Já nos comportamentos **DSP** e **DSS** o erro mostrou-se baixo com erros de cerca de 0,02 em relação a referência e erro zero em 10 configurações. Isto indica que a *Data Provenance* foi efetiva em

desconsiderar as recomendações difamatórias dado o baixo valor de erro ou sua inexistência em diversas configurações.

Já o Cenário 2 apresentou para os comportamentos **DCP** e **DCS** erros entre 0,03 e 0,08 e somente três configurações em que o erro foi compatível. Isto aponta que a difamação afetou demasiadamente a confiança nesses comportamentos. Para os comportamentos **DSP** e **DSS** no Cenário 2, mostrou-se menor em cerca de metade das configurações, variando entre 0,02 e 0,05. Contudo, na outra metade, ele exibiu erros tão altos quanto nos outros ataques. Diferentemente do Cenário 1, a quantidade de dispositivos permitiu que aqueles com comportamento difamatório se comunicassem para uma maior quantidade de vizinhos.

Pesos Par. Sociais				Cenários	
α	β	γ	δ	1	2
2	3	5	2	0,05	0,05
2	3	5	5	0,09	0,01
2	3	5	8	0,10	0,09
2	5	3	2	0,05	0,03
2	5	3	5	0,09	0,08
2	5	3	8	0,09	0,13
3	2	5	2	0,05	0,06
3	2	5	5	0,09	0,01
3	2	5	8	0,10	0,09
3	3	3	2	0,09	0,06
3	3	3	5	0,09	0,01
3	3	3	8	0,09	0,03
3	5	2	2	0,08	0,08
3	5	2	5	0,09	0,11
3	5	2	8	0,10	0,15
5	2	3	2	0,09	0,03
5	2	3	5	0,09	0,08
5	2	3	8	0,10	0,13
5	3	2	2	0,09	0,08
5	3	2	5	0,09	0,11
5	3	2	8	0,10	0,14

Tabela 5.11: MEA - DCP

Pesos Par. Sociais				Cenários	
α	β	γ	δ	1	2
2	3	5	2	0,05	0,04
2	3	5	5	0,09	0,02
2	3	5	8	0,10	0,09
2	5	3	2	0,05	0,05
2	5	3	5	0,09	0,09
2	5	3	8	0,09	0,13
3	2	5	2	0,05	0,04
3	2	5	5	0,09	0,02
3	2	5	8	0,10	0,09
3	3	3	2	0,05	0,05
3	3	3	5	0,09	0,00
3	3	3	8	0,09	0,03
3	5	2	2	0,09	0,09
3	5	2	5	0,09	0,12
3	5	2	8	0,10	0,15
5	2	3	2	0,09	0,04
5	2	3	5	0,09	0,09
5	2	3	8	0,10	0,13
5	3	2	2	0,09	0,09
5	3	2	5	0,09	0,12
5	3	2	8	0,10	0,15

Tabela 5.12: MEA - DCS

Pesos Par. Sociais				Cenários	
α	β	γ	δ	1	2
2	3	5	2	0,04	0,03
2	3	5	5	0,03	0,03
2	3	5	8	0,10	0,10
2	5	3	2	0,04	0,05
2	5	3	5	0,09	0,09
2	5	3	8	0,13	0,13
3	2	5	2	0,04	0,03
3	2	5	5	0,03	0,03
3	2	5	8	0,10	0,10
3	3	3	2	0,05	0,04
3	3	3	5	0,00	0,00
3	3	3	8	0,03	0,03
3	5	2	2	0,09	0,09
3	5	2	5	0,12	0,12
3	5	2	8	0,15	0,15
5	2	3	2	0,04	0,05
5	2	3	5	0,09	0,09
5	2	3	8	0,13	0,13
5	3	2	2	0,09	0,09
5	3	2	5	0,12	0,12
5	3	2	8	0,15	0,15

Tabela 5.13: MEA - DSP

Pesos Par. Sociais				Cenários	
α	β	γ	δ	1	2
2	3	5	2	0,03	0,03
2	3	5	5	0,03	0,03
2	3	5	8	0,10	0,10
2	5	3	2	0,05	0,05
2	5	3	5	0,09	0,09
2	5	3	8	0,13	0,13
3	2	5	2	0,04	0,03
3	2	5	5	0,03	0,03
3	2	5	8	0,10	0,10
3	3	3	2	0,05	0,04
3	3	3	5	0,00	0,00
3	3	3	8	0,03	0,03
3	5	2	2	0,09	0,09
3	5	2	5	0,12	0,12
3	5	2	8	0,15	0,15
5	2	3	2	0,04	0,05
5	2	3	5	0,09	0,09
5	2	3	8	0,13	0,13
5	3	2	2	0,09	0,09
5	3	2	5	0,12	0,12
5	3	2	8	0,15	0,15

Tabela 5.14: MEA - DSS

As métricas *TAP* e *TCA* traduzem a influência do ataque na aplicação de políticas e seleção do mecanismo de autenticação. Para o Cenário 1, com os comportamentos de difamação **DCP** e **DCS**, que são sumarizados nas Tabelas 5.15 e 5.16 respectivamente, o GALENA aplicou a política $\mathcal{P}_2$ em 5 cenários com *TAP* de 0,14%. A $\mathcal{P}_3$, dessa vez, foi aplicada em 18 das configurações, porém com taxas de compatibilidade baixas. Por fim, a política $\mathcal{P}_1$ foi aplicada em todas as configurações, com *TAPs* variando de 2,93% a 99,6%. Nessas configurações, porém, o *TCA* apresentou grande variações, entre 69,22% e 99,66%, diferentemente da configuração sem ataque que exibiu *TCAs* 96,3% e 99,4%. Os maiores valores de *TCA* foram atingidos quando o valor de γ era baixo e δ baixo, ou quando os valores de α e β eram altos. Para os comportamentos **DSP** e **DSS** no Cenário 1, exibidos nas Tabelas 5.17 e 5.18 respectivamente, a política $\mathcal{P}_1$ também foi aplicada em todas as configurações, variando entre 3,05% e 98,55%. $\mathcal{P}_2$ foi aplicada em 6 configurações, com valores de 0,09%. Por fim, $\mathcal{P}_3$ foi aplicada em 12 cenários com valores de 71,81% no comportamento DSP e 73,82%. Nesses comportamentos os *TCAs* variaram entre 74,96% e 98,65%. Apesar de apresentar variações de valores em relação a *TAP* e *TCA*, pode-se verificar que nesses comportamentos as políticas foram aplicadas nas mesmas configurações em relação às configurações sem ataque, visto na Tabela 5.5, demonstra que a técnica de *Data Provenance* aplicada foi eficaz em filtrar as recomendações maliciosas.

No Cenário 2, nos comportamentos de difamação **DCP** e **DCS**, encontrados respectivamente nas Tabelas B.1 e B.2 no Apêndice B, em 5 configurações, foi aplicada unicamente a política $\mathcal{P}_1$ com *TAPs* da ordem de 99,67% e *TCA* com o mesmo valor. A política $\mathcal{P}_2$ foi aplicada em 6 das configurações com *TAPs* da ordem de 0,31% (DCP) e 0,23% (DCS). Por fim, a política $\mathcal{P}_3$ foi aplicada em 12 cenários com *TAPs* tão baixos quanto 47,45% e atingindo máximas de

89,59%. Os TCAs variaram entre 66,37% e 99,89%. Como no Cenário 1, os maiores valores de TCA foram atingidos quando eram γ e δ baixos, ou quando os valores de α e β eram altos. Para os comportamentos **DSP** e **DSS** no Cenário 2, exibidos respectivamente nas Tabelas B.3 e B.4 também do Apêndice B, a política $\mathcal{P}_2$ foi aplicada em 6 configurações, com TAP de 0,28% (DSP) e 0,31% (DSS), e a política $\mathcal{P}_3$ foi aplicada em 12 configurações, com TAPs variando entre 76,63% e 90,02%. Por fim a política $\mathcal{P}_1$ foi aplicada em todas as configurações com TAPs variando entre 4,36% e 98,07%. Assim como no Cenário 1, o uso de *Data Provenance* proporcionou TCAs mais altos, próximos da configuração sem ataque, atingindo valores entre 82,39% e 99,62%. Porém, dado a baixa densidade de atacantes, o efeito da difamação não se mostra tão pronunciado quando no 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	99,66%	00,00%	00,00%	99,66%
2	3	5	5	05,31%	00,00%	63,91%	69,22%
2	3	5	8	02,93%	00,14%	72,24%	75,31%
2	5	3	2	99,66%	00,00%	00,00%	99,66%
2	5	3	5	05,31%	00,00%	63,91%	69,22%
2	5	3	8	07,64%	00,00%	59,87%	67,52%
3	2	5	2	99,66%	00,00%	00,00%	99,66%
3	2	5	5	05,31%	00,00%	63,90%	69,22%
3	2	5	8	02,93%	00,14%	72,24%	75,31%
3	3	3	2	04,24%	00,00%	73,69%	77,93%
3	3	3	5	05,31%	00,00%	63,91%	69,22%
3	3	3	8	07,64%	00,00%	59,87%	67,52%
3	5	2	2	13,65%	00,00%	55,86%	69,52%
3	5	2	5	04,24%	00,00%	73,69%	77,93%
3	5	2	8	02,93%	00,14%	72,24%	75,31%
5	2	3	2	07,64%	00,00%	59,87%	67,52%
5	2	3	5	04,24%	00,00%	73,69%	77,93%
5	2	3	8	02,93%	00,14%	72,24%	75,31%
5	3	2	2	07,64%	00,00%	59,87%	67,52%
5	3	2	5	04,24%	00,00%	73,69%	77,93%
5	3	2	8	02,93%	00,14%	72,24%	75,31%

Tabela 5.15: TAP e TCA do DCP - 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	99,66%	00,00%	00,00%	99,66%
2	3	5	5	05,31%	00,00%	63,91%	69,22%
2	3	5	8	02,93%	00,14%	72,24%	75,31%
2	5	3	2	99,66%	00,00%	00,00%	99,66%
2	5	3	5	05,31%	00,00%	63,91%	69,22%
2	5	3	8	07,64%	00,00%	59,87%	67,52%
3	2	5	2	99,66%	00,00%	00,00%	99,66%
3	2	5	5	05,31%	00,00%	63,91%	69,22%
3	2	5	8	02,93%	00,14%	72,24%	75,31%
3	3	3	2	99,66%	00,00%	00,00%	99,66%
3	3	3	5	05,31%	00,00%	63,91%	69,22%
3	3	3	8	07,64%	00,00%	59,87%	67,52%
3	5	2	2	07,64%	00,00%	59,87%	67,52%
3	5	2	5	04,24%	00,00%	73,69%	77,93%
3	5	2	8	02,93%	00,14%	72,24%	75,31%
5	2	3	2	07,64%	00,00%	59,87%	67,52%
5	2	3	5	04,24%	00,00%	73,69%	77,93%
5	2	3	8	02,93%	00,14%	72,24%	75,31%
5	3	2	2	08,31%	00,00%	58,88%	67,19%
5	3	2	5	04,24%	00,00%	73,69%	77,93%
5	3	2	8	02,93%	00,14%	72,24%	75,31%

Tabela 5.16: TAP e TCA do DCS - 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	98,55%	00,09%	00,00%	98,65%
2	3	5	5	98,55%	00,09%	00,00%	98,65%
2	3	5	8	03,05%	00,09%	71,81%	74,96%
2	5	3	2	99,73%	00,00%	00,00%	99,73%
2	5	3	5	04,12%	00,00%	71,81%	75,94%
2	5	3	8	03,94%	00,00%	93,20%	97,14%
3	2	5	2	98,55%	00,09%	00,00%	98,65%
3	2	5	5	98,55%	00,09%	00,00%	98,65%
3	2	5	8	03,05%	00,09%	71,81%	74,96%
3	3	3	2	99,73%	00,00%	00,00%	99,73%
3	3	3	5	99,73%	00,00%	00,00%	99,73%
3	3	3	8	99,73%	00,00%	00,00%	99,73%
3	5	2	2	04,12%	00,00%	71,81%	75,94%
3	5	2	5	04,12%	00,00%	71,81%	75,94%
3	5	2	8	03,94%	00,00%	93,20%	97,14%
5	2	3	2	99,90%	00,00%	00,00%	99,90%
5	2	3	5	04,27%	00,00%	71,81%	76,09%
5	2	3	8	04,09%	00,00%	93,20%	97,29%
5	3	2	2	04,27%	00,00%	71,81%	76,09%
5	3	2	5	04,27%	00,00%	71,81%	76,09%
5	3	2	8	04,09%	00,00%	93,20%	97,29%

Tabela 5.17: TAP e TCA do DSP - 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	98,08%	00,25%	00,00%	98,34%
2	3	5	5	98,08%	00,25%	00,00%	98,34%
2	3	5	8	02,66%	00,25%	73,82%	76,74%
2	5	3	2	99,55%	00,00%	00,00%	99,55%
2	5	3	5	03,85%	00,00%	73,82%	77,68%
2	5	3	8	03,66%	00,00%	93,02%	96,68%
3	2	5	2	98,08%	00,25%	00,00%	98,34%
3	2	5	5	98,08%	00,25%	00,00%	98,34%
3	2	5	8	02,66%	00,25%	73,82%	76,74%
3	3	3	2	99,55%	00,00%	00,00%	99,55%
3	3	3	5	99,55%	00,00%	00,00%	99,55%
3	3	3	8	99,55%	00,00%	00,00%	99,55%
3	5	2	2	03,85%	00,00%	73,82%	77,68%
3	5	2	5	03,85%	00,00%	73,82%	77,68%
3	5	2	8	03,66%	00,00%	93,02%	96,68%
5	2	3	2	99,77%	00,00%	00,00%	99,77%
5	2	3	5	04,05%	00,00%	73,82%	77,88%
5	2	3	8	03,86%	00,00%	93,02%	96,89%
5	3	2	2	04,05%	00,00%	73,82%	77,88%
5	3	2	5	04,05%	00,00%	73,82%	77,88%
5	3	2	8	03,86%	00,00%	93,02%	96,89%

Tabela 5.18: TAP e TCA do DSS - Cenário 1

As métricas relacionadas a efetividade da detecção do ataque estão sumarizadas na Tabela 5.19. Somente os comportamentos **DSP** e **DSS** foram escolhidos para análise pois são aqueles em que a *Data Provenance* mostra-se mais relevante. A primeira métrica a ser

destacada é a Taxa de Falsos Positivos (T_{fp}), que mensura dispositivos que eram atacantes e foram incorretamente classificados como não atacantes. Observa-se que essa taxa manteve-se em zero. Isso ocorre devido ao uso da *Data Provenance* para verificação criptográfica da integridade das recomendação, ou seja, mostra-se improvável que uma verificação possa ser forjada ou validada. Contrariamente, a Taxa de Falsos Negativos (T_{fn}) mensura a quantidade de dispositivos que eram não atacantes mas não foram incorretamente classificados como atacantes. Percebe-se que no Cenário 1 essa métrica exibiu valores baixos, não ultrapassando cerca de 10%. Já no Cenário 2 esse erro mostrou-se maior, variando entre 25% e 31%. Isso acarreta no descarte de recomendações que eram legítimas e na alteração da confiança percebida por um dispositivo sobre o outro, o que impacta na TAP das políticas e na TCA.

Cenário	Comportamento da Difamação	T_{fp}	T_{fn}	T_{acc}	T_{det}
1	DSP	0	09,95%	91,42%	90,62%
1	DSS	0	10,58%	90,42%	89,41%
2	DSP	0	31,43%	76,08%	68,56%
2	DSS	0	25,23%	79,85%	74,76%

Tabela 5.19: T_{fp} , T_{fn} , T_{acc} , T_{det} para os Comportamentos **DSP** e **DSS**

Ainda, a Acurácia da Detecção (T_{acc}) quantifica a precisão da detecção do ataque. O GALENA foi capaz de atingir valores da ordem de cerca de 90% no Cenário 1. Porém, no Cenário 2 o GALENA não atingiu uma acurácia no mesmo patamar, reflexo direto da taxa de falsos positivos elevada, se restringindo entre 76% e 79%. Por fim, a Taxa de Detecção (T_{det}) quantifica quão efetivo o GALENA foi na detecção do ataque de difamação com esses comportamentos. No Cenário 1 ele atingiu valores entre 89% e 90% que pode ser percebido principalmente ao analisar-se os TAPs e TCA desses comportamentos contra o configuração sem ataque, demonstrando a efetividade do GALENA na detecção e mitigação do efeito desse ataque. No Cenário 2, porém, a detecção mostrou-se baixa, variando entre cerca de 68% e 74%. Novamente isso reflete diretamente nas TAPs e TCA desses comportamentos que não se assemelham à configuração sem ataque.

Assim, a análise dos resultados obtidos a partir da simulação do GALENA nos permite concluir que a percepção social pode ser incorporada aos Sistemas de Autenticação Adaptativa como fatores de adaptação. Ainda, os fatores sociais possibilitam uma flexibilidade na avaliação de confiança ao proporcionar a mudança dos pesos de cada fator social considerado e, assim, influenciar na seleção do mecanismo de autenticação. O fator SOR, por levar em consideração as experiências passadas, mostrou-se como o fator de maior impacto no cálculo da confiança. Por fim, em relação à proteção das recomendações sociais trocadas pelos dispositivos, a técnica de *Data Provenance* baseada em códigos de verificação autenticados (HMAC) mostrou-se promissora na proteção das recomendações sociais trocadas entre os dispositivos IoT, garantindo sua origem e integridade, principalmente em cenários em que o ataque de difamação empregava identidades fabricadas (*Sybil*).

5.5 RESUMO

Esse capítulo apresentou a metodologia de avaliação e a discussão dos resultados obtidos a partir da simulação do sistema GALENA. Os resultados demonstram a eficiência do GALENA na adaptação do mecanismo de autenticação empregado pelo dispositivo e a eficácia em mitigar os efeitos do ataque de difamação. Os cenários foram avaliados de modo que o sistema pudesse ser testado diante de diferentes configurações e comportamentos do ataque de difamação.

6 CONCLUSÕES

A autenticação nas redes IoT é uma etapa importante à prestação de serviços em redes, pois ela garante a segurança da comunicação e da troca de informações entre os dispositivos, e consequentemente da robustez dos serviços providos aos usuários ou outros dispositivos. O gerenciamento dos mecanismos de autenticação empregados pelos dispositivos IoT possibilita que estes mecanismos sejam utilizados conforme o ambiente e a compatibilidade do ambiente em que os dispositivos se encontram e sua relação com outros dispositivos, para garantir o nível adequado de segurança. Assim, os sistemas de autenticação adaptativos (SAAs) buscam para gerenciar dinamicamente o mecanismo de autenticação a ser empregado.

Apesar da literatura apresentar várias soluções voltadas a prover adaptabilidade ao serviço de autenticação, essas soluções exibem algumas fragilidades como a necessidade de pré-treinamento dos dados do sistema para determinar um comportamento, uma complexidade computacional para alcançar uma tomada de decisão, e muitas das vezes são desenvolvidas numa arquitetura centralizada, tendo dificuldades de escalabilidade diante de redes massivas e abertas com múltiplos proprietários. Além disso, elas possuem a limitação de normalmente apenas empregarem de fatores de adaptação não diversificados. Por outro lado, a percepção social, obtida a partir das relações sociais entre dispositivos, tem sido empregada na IoT para apoiar o serviço de controle de acesso, especificamente a autorização, na seleção e composição de serviços, visto que a percepção social proporciona um meio de selecionar com assertividade o dispositivo mais confiável entre os vizinhos próximos para a tomada de serviços. Portanto, ela também pode ser empregada em SAAs na medida que esses sistemas podem se beneficiar dessa percepção como fator de adaptação. No entanto, a utilização de confiança social traz também seus desafios, dentre eles a presença de ataques que visam alterar a confiança percebida entre ou pelos os dispositivos, como o ataque de difamação.

Esta dissertação investigou meios de incorporar a confiança social como fator de adaptação em SAAs a fim de que eles sejam robustos na seleção do mecanismo de autenticação adequado e flexíveis ao se adaptarem aos diferentes ambientes, bem como torná-los resilientes aos ataques de difamação que prejudicam os sistemas baseados em confiança social. Desta forma, propôs-se o sistema GALENA (*manaGement of Adaptive authentication based on poLiciEs aNd sociAl trust*), para gerenciar a autenticação de sistemas IoT baseado em confiança social para avaliar com assertividade o comportamento dos dispositivos vizinhos numa percepção social conforme o ambiente em que eles se encontram. Além disso, para mitigar o efeito de possíveis ataques de difamação sobre as recomendações trocadas pelo serviço de interação social, o GALENA emprega uma técnica *Data Provenance* que garante a origem dessas recomendações. Além disso, o uso de políticas apoia a adaptação visando a adequação do sistema aos dispositivos com restrições computacionais da IoT.

Avaliou-se através do simulador NS-3 a eficácia da adaptação do GALENA sobre o mecanismo de autenticação aplicado pelos dispositivos na transição pelos vários ambientes, bem com a sua eficiência na detecção do ataque de difamação que venham a comprometer o seu funcionamento. As avaliações levaram em conta um ambiente urbano e um modelo realístico de mobilidade dos dispositivos, e para a análise da robustez do GALENA considerou-se quatro comportamentos do ataque de difamação. Em relação ao desempenho da adaptação da autenticação, o GALENA atingiu taxas de compatibilidade de autenticação de cerca de 97% no cenário com 200 dispositivos e de 98% com 400 dispositivos. As avaliações demonstraram a capacidade do GALENA em adaptar o mecanismo de autenticação empregado e negociá-lo

com compatibilidade a depender da percepção social exibida pelos dispositivos. Já em relação à análise da robustez do GALENA contra o ataque de difamação, o sistema atingiu taxas de detecção para o ataque de difamação DSP (Identificação Sybil com Difamação Constante) de cerca de 90% em algumas configurações mostrando assim a eficácia na detecção do ataque de difamação e na mitigação do seu efeito.

Em relação as análises efetuadas para a validação do GALENA, foi escolhido um ambiente com poucos dispositivos e homogêneos devido à complexidade de tempo exigida da simulação conforme o número de dispositivos aumenta. As configurações com 200 dispositivos demoraram cerca de 10 horas de simulação para a sua conclusão na infraestrutura de processamento empregada, e as de 400 dispositivos, cerca de 12 horas. Uma vez que as configurações são numerosas, 21 com 200 e mais 21 com 400 dispositivos nas configurações sem ataque e mais 4 variações de comportamento do ataque de difamação para cada configuração de quantidade de dispositivos, atingindo o total de cerca de 2310 horas de execução contínua. Para mitigar um pouco da demora, optou-se por executar a simulação através de multiprocessamento (uma simulação para cada *core* do processador das máquinas disponíveis) e não realizar uma análise com métricas estatísticas agregadas.

Dessa maneira, este trabalho contribuiu com um estudo das principais abordagens empregadas na literatura para a autenticação adaptativa na IoT, como a confiança social tem sido usada na IoT e quais as técnicas empregadas para lidar com o ataque de difamação. Ele também explorou como a confiança social pode ser incorporada aos SAAs para os dispositivos IoT.

6.1 QUESTÕES DE PESQUISA

- **Múltiplos fatores sociais e da percepção do ambiente podem ser incorporados aos SAAs?** Eles podem ser incorporados como fatores de adaptação dado que possibilitam aos SAAs tornarem-se mais capazes na avaliação dos dispositivos, e, portanto, uma avaliação mais assertiva para selecionar o mecanismo de autenticação adequado.
- **Qual é o impacto da influência de cada fator social na confiança final estabelecida entre os dispositivos IoT?** Os pesos de cada fator social afetam diretamente a confiança social final, alterando seu valor para mais ou para menos e influenciando na aplicação de políticas, e portanto podendo ocasionar a não aplicação de uma dada política. A relação social SOR se mostrou a mais forte em termos de contribuição para o valor final da confiança.
- **Como proteger as recomendações sociais entre os dispositivos IoT diante de ataques de difamação nos ambientes?** A técnica de *Data Provenance* baseada em códigos de verificação autenticados (HMAC) mostrou-se efetiva na manutenção da integridade e garantia da origem das recomendações sociais, principalmente quando o ataque de difamação emprega diversas identidades.

6.2 TRABALHOS FUTUROS

Durante o desenvolvimento da pesquisa, novas questões surgiram e outras podem ser melhor aprofundadas. Manter a privacidade dos dispositivos a medida que eles transitam entre diversos ambientes e tomam e proveem serviços para dispositivos desconhecidos é uma tarefa de constante evolução. Portanto os sistemas empregados na IoT devem acompanhar a evolução também das ameaças. A evolução da pesquisa dessa dissertação possibilita a investigação

de novas questões a serem avaliadas, principalmente em relação a adaptação e mitigação da difamação. A seguir são detalhadas as direções para os trabalhos futuros.

1. **Análise da variação do peso da recomendação para uma maior efetividade da adaptação:** Investigar a importância do peso do valor da recomendação, estabelecida a partir de δ , durante a simulação para melhorar a avaliação das recomendações e mitigar o efeito do ataque de difamação. Desse modo, pode-se avaliar de forma mais efetiva um determinado dispositivo e aumentar a robustez do sistema contra o ataque de difamação ao empregar uma coleção de técnicas para mitigar seu efeito.
2. **Investigação de outras técnicas para garantir integridade:** Desenvolvimento de estudo e análise comparativa de outras técnicas de garantia de integridade das recomendações recebidas como alternativa para mitigação dos efeitos do ataque de difamação. Assim, pode-se obter uma menor taxa de falsos negativos, melhorando a detecção do ataque.
3. **Robustez a comportamentos de difamação em conluio:** Avaliar o desempenho do GALENA diante de o ataque de difamação com comportamento em conluio, onde um grupo de dispositivos emite má-recomendações contra um dispositivo visando sua remoção da rede. Esse comportamento representa um grande desafio, pois trata-se de um ataque coordenado.

REFERÊNCIAS

- Aalibagi, S., Mahyar, H., Movaghar, A. e Stanley, H. E. (2019). A matrix factorization model for hellinger-based trust management in social internet of things. *arXiv:1909.12432*.
- Abderrahim, O. B., Elhdhili, M. H. e Saidane, L. (2017a). Tmcoi-siot: A trust management system based on communities of interest for the social internet of things. Em *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, páginas 747–752. IEEE.
- Abderrahim, O. B., Elhdhili, M. H. e Saidane, L. (2016). Dtms-iot: A dirichlet-based trust management system mitigating on-off attacks and dishonest recommendations for the internet of things. Em *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, páginas 1–8. IEEE.
- Abderrahim, O. B., Elhdhili, M. H. e Saidane, L. (2017b). Ctms-siot: A context-based trust management system for the social internet of things. Em *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, páginas 1903–1908. IEEE.
- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. e Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys and Tutorials*, 17(4):2347–2376.
- Al-Hamadi, H., Chen, I.-R. e Cho, J.-H. (2019). Trust Management of Smart Service Communities. *IEEE Access*, 7:26362–26378.
- Alam, M. e Wang, W. (2021). A Comprehensive Survey on the State-of-the-art Data Provenance Approaches for Security Enforcement. 29(4).
- Aman, W. e Kausar, F. (2019). Towards a gateway-based context-aware and self-adaptive security management model for IoT-based eHealth systems. *International Journal of Advanced Computer Science and Applications*, 10(1).
- Aman, W. e Sneekenes, E. (2015). EDAS: An evaluation prototype for autonomic event-driven adaptive security in the internet of things. *Future Internet*, 7(4):225–256.
- Arfaoui, A., Kribeche, A., Senouci, S. M. e Hamdi, M. (2018). Game-based adaptive risk management in wireless body area networks. Em *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE.
- Arias-Cabarcos, P., Krupitzer, C. e Becker, C. (2019). A survey on adaptive authentication. *ACM Computing Surveys*, 52(4):1–30.
- Ashton, K. et al. (2009). That ‘internet of things’ thing. *RFID journal*, 22(7):97–114.
- Assis, M. V. O. D., Hamamoto, A. H., Abrao, T. e 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.
- Atzori, L., Iera, A. e Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15):2787–2805.

- Atzori, L., Iera, A. e Morabito, G. (2017). Understanding the internet of things: definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, 56:122–140.
- Atzori, L., Iera, A., Morabito, G. e Nitti, M. (2012). The social internet of things (SIoT) - When social networks meet the internet of things: Concept, architecture and network characterization. *Computer Networks*, 56(16):3594–3608.
- Bahga, A. e Madiseti, V. K. (2016). Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications*, 09(10):533–546.
- Bao, F. e Chen, I.-R. (2012). Trust management for the internet of things and its application to service composition. Em *2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE.
- Bernabe, J. B., Ramos, J. L. H. e Gomez, A. F. S. (2015). TACIoT: multidimensional trust-aware access control system for the internet of things. *Soft Computing*, 20(5):1763–1779.
- Chen, I.-R., Bao, F. e Guo, J. (2016). Trust-based service management for social internet of things systems. *IEEE Transactions on Dependable and Secure Computing*, 13(6):684–696.
- Chen, I.-R., Guo, J., Wang, D.-C., Tsai, J. J., Al-Hamadi, H. e You, I. (2018). Trust as a Service for IoT Service Management in Smart Cities. Em *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, páginas 1358–1365. IEEE.
- Chen, R., Guo, J. e Bao, F. (2014). Trust management for soa-based iot and its application to service composition. *IEEE Transactions on Services Computing*, 9(3):482–495.
- Cho, J.-H., Chan, K. e Adali, S. (2015). A survey on trust modeling. *ACM Computing Surveys*, 48(2):1–40.
- da Costa Júnior, E. P., da Silva, C. E., Pinheiro, M. e Sampaio, S. (2018). A new approach to deploy a self-adaptive distributed firewall. *Journal of Internet Services and Applications*, 9(1).
- Datamation (2022). Iot in smart cities in 2022. <https://www.datamation.com/networks/iot-in-smart-cities/>. [Online; Acessado em 17-03-2022].
- de Moraes, Y. U. (2022). Gerenciamento e Proteção do Serviço de Autenticação Adaptativa Social para Ambientes IoT Contra Ataques de Difamação - Dataset. <https://doi.org/10.5281/zenodo.6654129>.
- Denis, F. e Contributors (2013). The sodium cryptography library. <https://doc.libsodium.org/>.
- El-hajj, M., Fadlallah, A., Chamoun, M. e Serhrouchni, A. (2019). A survey of internet of things (IoT) authentication schemes. *Sensors*, 19(5):1141.
- Elkhodr, M. e Mufti, Z. B. (2019). On the challenges of data provenance in the internet of things. *International Journal of Wireless & Mobile Networks*, 11(3):43–52.
- Fang, H., Wang, X. e Hanzo, L. (2020). Adaptive trust management for soft authentication and progressive authorization relying on physical layer attributes. *IEEE Transactions on Communications*, 68(4):2607–2620.

- Farris, I., Bernabe, J. B., Toumi, N., Garcia-Carrillo, D., Taleb, T., Skarmeta, A. e Sahlin, B. (2017). Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems. Em *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE.
- Fedrechski, G., De Biase, L. C. C., Calcina-Ccori, P. C. e Zuffo, M. K. (2019). Attribute-Based Access Control for the Swarm with Distributed Policy Management. *IEEE Transactions on Consumer Electronics*.
- Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J. e Shu, L. (2017). Authentication Protocols for Internet of Things: A Comprehensive Survey. *Security and Communication Networks*, 2017:1–41.
- Gardašević, G., Veletić, M., Maletić, N., Vasiljević, D., Radusinović, I., Tomović, S. e Radonjić, M. (2016). The IoT architectural framework, design issues and application domains. *Wireless Personal Communications*, 92(1):127–148.
- Gebrie, M. T. e Abie, H. (2017). Risk-based adaptive authentication for internet of things in smart home ehealth. Em *Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings*, páginas 102–108.
- Guo, J., Chen, I.-R. e Tsai, J. J. (2017). A survey of trust computation models for service management in internet of things systems. *Computer Communications*, 97:1–14.
- Gwak, B., Cho, J. H., Lee, D. e Son, H. (2018). TARAS: Trust-Aware Role-Based Access Control System in Public Internet-of-Things. *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, páginas 74–85.
- Hamdi, M. e Abie, H. (2014). Game-based adaptive security in the internet of things for eHealth. Em *2014 IEEE International Conference on Communications (ICC)*. IEEE.
- Hamme, T. V., Preuveneers, D. e Joosen, W. (2018). Managing distributed trust relationships for multi-modal authentication. *Journal of Information Security and Applications*, 40:258–270.
- Hayashi, E., Das, S., Amini, S., Hong, J. e Oakley, I. (2013). Casa: context-aware scalable authentication. Em *Proceedings of the Ninth Symposium on Usable Privacy and Security*, páginas 1–10.
- Hellaoui, H., Bouabdallah, A. e Koudil, M. (2016). Tas-iot: trust-based adaptive security in the iot. Em *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, páginas 599–602. IEEE.
- Hintze, D., Füller, M., Scholz, S., Findling, R. D., Muaaz, M., Kapfer, P., Koch, E. e Mayrhofer, R. (2019). CORMORANT. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(3):1–23.
- Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K. et al. (2013). Guide to attribute based access control (abac) definition and considerations (draft). *NIST special publication*, 800(162).

- Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R. e Scarfone, K. (2014). Guide to attribute based access control (ABAC) definition and considerations. Relatório técnico, National Institute of Standards and Technology.
- ITUNews (2018). Arm predicts 1 trillion iot devices by 2035 with new end-to-end platform. <https://news.itu.int/arm-pelion-iot-end-to-end-platform/>. [Online; Acessado em 17-03-2022].
- Jafarian, B., Yazdani, N. e Haghighi, M. S. (2020). Discrimination-aware trust management for social internet of things. *Computer Networks*, 178:107254.
- Jaigirdar, F. T., Rudolph, C. e Bain, C. (2019). "can i Trust the Data i See?" A Physician's Concern on Medical Data in IoT Health Architectures. *ACM International Conference Proceeding Series*, páginas 1–10.
- Jøsang, A. e Bhuiyan, T. (2008). Optimal trust network analysis with subjective logic. Em *2008 Second International Conference on Emerging Security Information, Systems and Technologies*, páginas 179–184. IEEE.
- Josang, A. e Ismail, R. (2002). The beta reputation system. Em *Proceedings of the 15th bled electronic commerce conference*, volume 5, páginas 2502–2511.
- Katsikogiannis, G., Kallergis, D., Garofalaki, Z., Mitropoulos, S. e Douligeris, C. (2018). A policy-aware service oriented architecture for secure machine-to-machine communications. *Ad Hoc Networks*, 80:70–80.
- Khan, Z. A., Ullrich, J., Voyiatzis, A. G. e Herrmann, P. (2017). A trust-based resilient routing mechanism for the internet of things. Em *Proceedings of the 12th International Conference on Availability, Reliability and Security*, páginas 1–6.
- Khani, M., Wang, Y., Orgun, M. A. e Zhu, F. (2018). Context-aware trustworthy service evaluation in social internet of things. Em *International Conference on Service-Oriented Computing*, páginas 129–145. Springer.
- Kowshalya, A. M. e Valarmathi, M. (2018). Dynamic trust management for secure communications in social internet of things (siot). *Sādhanā*, 43(9):136.
- Li, W., Song, H. e Zeng, F. (2018). Policy-Based Secure and Trustworthy Sensing for Internet of Things in Smart Cities. *IEEE Internet of Things Journal*.
- Malik, M., Dutta, M. e Granjal, J. (2019). A Survey of Key Bootstrapping Protocols Based on Public Key Cryptography in the Internet of Things. *IEEE Access*, 7:27443–27464.
- Marche, C., Atzori, L. e Nitti, M. (2018). A dataset for performance analysis of the social internet of things. Em *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, páginas 1–5. IEEE.
- Marche, C., Atzori, L., Pilloni, V. e Nitti, M. (2020). How to exploit the social internet of things: Query generation model and device profiles' dataset. *Computer Networks*, página 107248.
- McKinsey (2015). By 2025, internet of things applications could have \$11 trillion impact. <https://www.mckinsey.com/mgi/overview/in-the-news/by-2025-internet-of-things-applications-could-have-11-trillion-impact>. [Online; Acessado em 26-11-2019].

- Morabito, R. e Jimenez, J. (2020). IETF protocol suite for the internet of things: Overview and recent advancements. *IEEE Communications Standards Magazine*, 4(2):41–49.
- Park, T., Kim, Y., Park, J., Suh, H., Hong, B. e Shin, S. (2016). QoSE: Quality of security a network security framework with distributed NFV. Em *2016 IEEE International Conference on Communications (ICC)*. IEEE.
- Pasquier, T., Singh, J., Powles, J., Eysers, D., Seltzer, M. e Bacon, J. (2018). Data provenance to audit compliance with privacy policy in the Internet of Things. *Personal and Ubiquitous Computing*, 22(2):333–344.
- Pinel, E. C., Long, A. E., Landau, M. J., Alexander, K. e Pyszczynski, T. (2006). Seeing i to i: a pathway to interpersonal connectedness. *Journal of personality and social psychology*, 90(2):243.
- Premarathne, U. S. (2017). Mag-siot: A multiplicative attributes graph model based trust computation method for social internet of things. Em *2017 IEEE International Conference on Industrial and Information Systems (ICIIS)*, páginas 1–6. IEEE.
- Putra, G. D., Dedeoglu, V., Kanhere, S. S. e Jurdak, R. (2019). Trust management in decentralized iot access control system. arXiv:1912.10247.
- Qin, W., Chen, S. e Peng, M. (2020). Recent advances in industrial internet: insights and challenges. *Digital Communications and Networks*, 6(1):1–13.
- Reddy, V. B., Negi, A., Venkataraman, S. e Venkataraman, V. R. (2019). A similarity based trust model to mitigate badmouthing attacks in internet of things (iot). Em *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, páginas 278–282. IEEE.
- Riley, G. F. e Henderson, T. R. (2010). The ns-3 network simulator. Em *Modeling and Tools for Network Simulation*, páginas 15–34. Springer Berlin Heidelberg.
- Saarinen, M.-J. e Aumasson, J.-P. (2015). The blake2 cryptographic hash and message authentication code (mac). RFC 7693, RFC Editor.
- Silva, E. F., Muchaluat-Saade, D. C. e Fernandes, N. C. (2018). ACROSS: A generic framework for attribute-based access control with distributed policies for virtual organizations. *Future Generation Computer Systems*, 78:1–17.
- Suhail, S., Hong, C. S., Ahmad, Z. U., Zafar, F. e Khan, A. (2017). Introducing secure provenance in IoT: Requirements and challenges. *Proceedings - 2016 International Workshop on Secure Internet of Things, SIoT 2016*, páginas 39–46.
- Suryani, V., Sulistyono, S. e Widyawan, W. (2017). Contrast: A trust model to enhance the privacy in internet of things. *Int. J. Intell. Eng. Syst*, 10(3):30–37.
- Suryani, V., Sulistyono, S. e Widyawan, W. (2018). Simulation of trust-based attacks in internet of things. *MATEC Web of Conferences*, 154:03014.
- Sylla, T., Chalouf, M. A., Krief, F. e Samaké, K. (2020). Towards a context-aware security and privacy as a service in the internet of things. Em *Information Security Theory and Practice*, páginas 240–252. Springer International Publishing.

- Sánchez, P. M. S., Celdrán, A. H., Maimó, L. F. e Pérez, G. M. (2020). Authcode: A privacy-preserving and multi-device continuous authentication architecture based on machine and deep learning. *arXiv:2004.07877*.
- Tan, S., Liu, Y., Li, X. e Dong, Q. (2016). A similarity-based indirect trust model with anti-spoofing capability. *Security and Communication Networks*, 9(18):5868–5881.
- Tripathy, B. K., Das, D. P., Jena, S. K. e Bera, P. (2018). Risk based security enforcement in software defined network. *Computers & Security*, 78:321–335.
- Ud Din, I., Guizani, M., Kim, B.-S., Hassan, S. e Khurram Khan, M. (2019). Trust Management Techniques for the Internet of Things: A Survey. *IEEE Access*, 7(c):29763–29787.
- Waldbusser, S., Perry, J., Herzog, S., Carlson, M. A., Schnizlein, D. J. M., Quinn, B., Scherling, M., Westerinen, A., Huynh, A. e Strassner, J. (2001). Terminology for Policy-Based Management. RFC 3198.

APÊNDICE A – METODOLOGIA DO LEVANTAMENTO BIBLIOGRÁFICO

Neste apêndice apresenta-se a metodologia empregada ao levantamento bibliográfico que deu suporte ao desenvolvimento desta pesquisa. Esta metodologia resultou no estado-da-arte apresentado Capítulo 3, assim como as técnicas encontradas na literatura para a adaptação, mitigação do ataque de difamação. Além disso, a metodologia auxiliou com subsídios para a estruturação do GALENA, descrito no Capítulo 4 e a definição dos formalismos necessários a sua definição. Ainda, o levantamento do estado-da-arte auxiliou com as definições de métricas para definição da metodologia de avaliação presente no Capítulo 5. A descrição do levantamento inclui as *strings* de busca e os critérios de inclusão e exclusão. Para o levantamento relacionado a Autenticação Adaptativa, foram empregadas as seguintes *strings* no buscador *Google Scholar*:

- “adaptive authentication” (“iot” OR “WSN” or “internet of things”)
- “adaptive authentication” (“iot” OR “WSN” or “internet of things”) (“M2M” or “machine to machine” OR “machine-to-machine” OR “autonomous”)
- + (“adaptive authentication” OR “adaptive security”) + (“SDN” or “software defined network”)

Para esse levantamento, foram excluídos os trabalhos anteriores a 2015 e aqueles que não envolviam sistemas de autenticação adaptativa, ainda foram excluídas quaisquer patentes e artigos com texto completo inacessível. Para a última *string* de busca, priorizou-se trabalhos que envolviam IoT. Ainda, empregou-se uma estratégia de *snowball* em relação aos trabalhos de (Hayashi et al., 2013) e de (Hamdi e Abie, 2014). À época do levantamento, foram encontradas 154 citações do primeiro trabalho, que foram refinadas utilizando-se a *string* ("adaptive authentication" OR "adaptive security") e incluindo resultados a partir de 2015, resultando em 14 trabalhos. Do segundo trabalho, foram encontrados 31 citações, também refinadas com "adaptive authentication" e incluindo resultados a partir de 2015, resultando em 7 trabalhos. O conjunto de referências resultou em 21 trabalhos e após leitura do texto completo dos artigos, 15 deles foram selecionados para constituir o *corpus* considerado para a Tabela 3.2 no Capítulo 3.

Por sua vez, o levantamento relacionado à confiança e confiança social, auxiliou na definição dos comportamentos sociais a serem considerados pelo GALENA, nas métricas de avaliação relacionadas a confiança, bem como na definição do comportamento do ataque de difamação e formas de mitigação. Nesse levantamento, foram empregadas as seguintes *strings* no buscador *Google Scholar*:

- (“iot” OR “internet of things”) (“trust management systems” OR “trust and reputation management systems”) - “survey”
- (“iot” OR “internet of things”) (“trust management systems” OR “trust and reputation management systems”)
- +IoT +social + (“bad mouthing” OR “bad-mouthing” OR “badmouthing”)

Também foram excluídos os trabalhos anteriores a 2015 e aqueles que não envolviam sistemas de gerenciamento de confiança e/ou relacionados a mitigação do ataque de difamação, novamente, foram excluídos também quaisquer patentes e trabalhos com textos inacessíveis. O conjunto de referências resultou em 31 trabalhos, e, após leitura dos textos completos, 18 foram considerados no *corpus* para as Tabelas 3.3 e 3.4 do Capítulo 3.

APÊNDICE B – RESULTADOS DA AVALIAÇÃO DE SEGURANÇA

Neste apêndice encontram-se os resultados completos das simulações relacionadas a segurança do GALENA. Em razão do volume e tamanho dos gráficos gerados, nem todos os gráficos foram apresentados no Capítulo 5. As Tabelas B.1 a B.4 contêm os *TAPs* e *TCA*s para o Cenário 2, com 400 dispositivos. Por sua vez, os gráficos das Figuras B.1 a B.4 compreendem a Evolução da Confiança nos quatro comportamentos de ataque para esse cenário.

B.1 *TAP* E *TCA* PARA OS ATAQUES NO CENÁRIO 2

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	97,76%	00,31%	00,00%	98,08%
2	3	5	5	97,77%	00,31%	00,00%	98,09%
2	3	5	8	05,30%	00,31%	74,17%	79,80%
2	5	3	2	99,68%	00,00%	00,00%	99,68%
2	5	3	5	14,90%	00,00%	51,34%	66,24%
2	5	3	8	05,18%	00,00%	89,59%	94,77%
3	2	5	2	97,77%	00,31%	00,00%	98,09%
3	2	5	5	97,73%	00,31%	00,00%	98,05%
3	2	5	8	05,41%	00,34%	73,75%	79,51%
3	3	3	2	99,68%	00,00%	00,00%	99,68%
3	3	3	5	99,69%	00,00%	00,00%	99,69%
3	3	3	8	99,69%	00,00%	00,00%	99,69%
3	5	2	2	18,19%	00,00%	48,07%	66,26%
3	5	2	5	07,01%	00,00%	73,75%	80,77%
3	5	2	8	05,18%	00,00%	89,59%	94,77%
5	2	3	2	99,80%	00,00%	00,00%	99,80%
5	2	3	5	15,84%	00,00%	50,00%	65,84%
5	2	3	8	05,28%	00,00%	89,59%	94,88%
5	3	2	2	18,91%	00,00%	47,45%	66,37%
5	3	2	5	07,36%	00,00%	72,86%	80,23%
5	3	2	8	05,28%	00,00%	89,59%	94,88%

Tabela B.1: *TAP* e *TCA* do **DCP** - Cenário 2

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	98,27%	00,23%	00,00%	98,51%
2	3	5	5	98,27%	00,23%	00,00%	98,51%
2	3	5	8	04,13%	00,23%	88,61%	92,99%
2	5	3	2	99,67%	00,00%	00,00%	99,67%
2	5	3	5	09,62%	00,00%	65,53%	75,16%
2	5	3	8	05,24%	00,00%	89,18%	94,43%
3	2	5	2	98,27%	00,23%	00,00%	98,51%
3	2	5	5	98,27%	00,23%	00,00%	98,51%
3	2	5	8	04,13%	00,23%	88,61%	92,99%
3	3	3	2	99,67%	00,00%	00,00%	99,67%
3	3	3	5	99,67%	00,00%	00,00%	99,67%
3	3	3	8	99,67%	00,00%	00,00%	99,67%
3	5	2	2	12,52%	00,00%	59,19%	71,72%
3	5	2	5	05,34%	00,00%	88,61%	93,96%
3	5	2	8	05,24%	00,00%	89,18%	94,43%
5	2	3	2	99,89%	00,00%	00,00%	99,89%
5	2	3	5	10,49%	00,00%	63,69%	74,18%
5	2	3	8	05,42%	00,00%	89,18%	94,60%
5	3	2	2	13,24%	00,00%	57,44%	70,69%
5	3	2	5	05,52%	00,00%	88,61%	94,13%
5	3	2	8	05,42%	00,00%	89,18%	94,60%

Tabela B.2: *TAP* e *TCA* do **DCS** - Cenário 2

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	98,07%	00,28%	00,00%	98,36%
2	3	5	5	98,07%	00,28%	00,00%	98,36%
2	3	5	8	05,19%	00,28%	76,63%	82,11%
2	5	3	2	99,61%	00,00%	00,00%	99,61%
2	5	3	5	06,49%	00,00%	76,63%	83,12%
2	5	3	8	05,04%	00,00%	89,45%	94,50%
3	2	5	2	98,07%	00,28%	00,00%	98,36%
3	2	5	5	98,07%	00,28%	00,00%	98,36%
3	2	5	8	05,19%	00,28%	76,63%	82,11%
3	3	3	2	99,61%	00,00%	00,00%	99,61%
3	3	3	5	99,61%	00,00%	00,00%	99,61%
3	3	3	8	99,61%	00,00%	00,00%	99,61%
3	5	2	2	06,49%	00,00%	76,63%	83,12%
3	5	2	5	06,49%	00,00%	76,63%	83,12%
3	5	2	8	05,04%	00,00%	89,45%	94,50%
5	2	3	2	99,80%	00,00%	00,00%	99,80%
5	2	3	5	06,65%	00,00%	76,63%	83,28%
5	2	3	8	05,20%	00,00%	89,45%	94,66%
5	3	2	2	06,65%	00,00%	76,63%	83,28%
5	3	2	5	06,65%	00,00%	76,63%	83,28%
5	3	2	8	05,20%	00,00%	89,45%	94,66%

Tabela B.3: *TAP* e *TCA* do **DSP** - Cenário 2

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	97,97%	00,31%	00,00%	98,29%
2	3	5	5	97,97%	00,31%	00,00%	98,29%
2	3	5	8	04,36%	00,31%	76,48%	81,16%
2	5	3	2	99,62%	00,00%	00,00%	99,62%
2	5	3	5	05,75%	00,00%	76,48%	82,24%
2	5	3	8	04,73%	00,00%	90,02%	94,75%
3	2	5	2	97,97%	00,31%	00,00%	98,29%
3	2	5	5	97,97%	00,31%	00,00%	98,29%
3	2	5	8	04,36%	00,31%	76,48%	81,16%
3	3	3	2	99,62%	00,00%	00,00%	99,62%
3	3	3	5	99,62%	00,00%	00,00%	99,62%
3	3	3	8	99,62%	00,00%	00,00%	99,62%
3	5	2	2	05,75%	00,00%	76,48%	82,24%
3	5	2	5	05,75%	00,00%	76,48%	82,24%
3	5	2	8	04,73%	00,00%	90,02%	94,75%
5	2	3	2	99,81%	00,00%	00,00%	99,81%
5	2	3	5	05,90%	00,00%	76,48%	82,39%
5	2	3	8	04,87%	00,00%	90,02%	94,89%
5	3	2	2	05,90%	00,00%	76,48%	82,39%
5	3	2	5	05,90%	00,00%	76,48%	82,39%
5	3	2	8	04,87%	00,00%	90,02%	94,89%

Tabela B.4: *TAP* e *TCA* do **DSS** - Cenário 2

B.2 EC PARA OS ATAQUES NO CENÁRIO 2

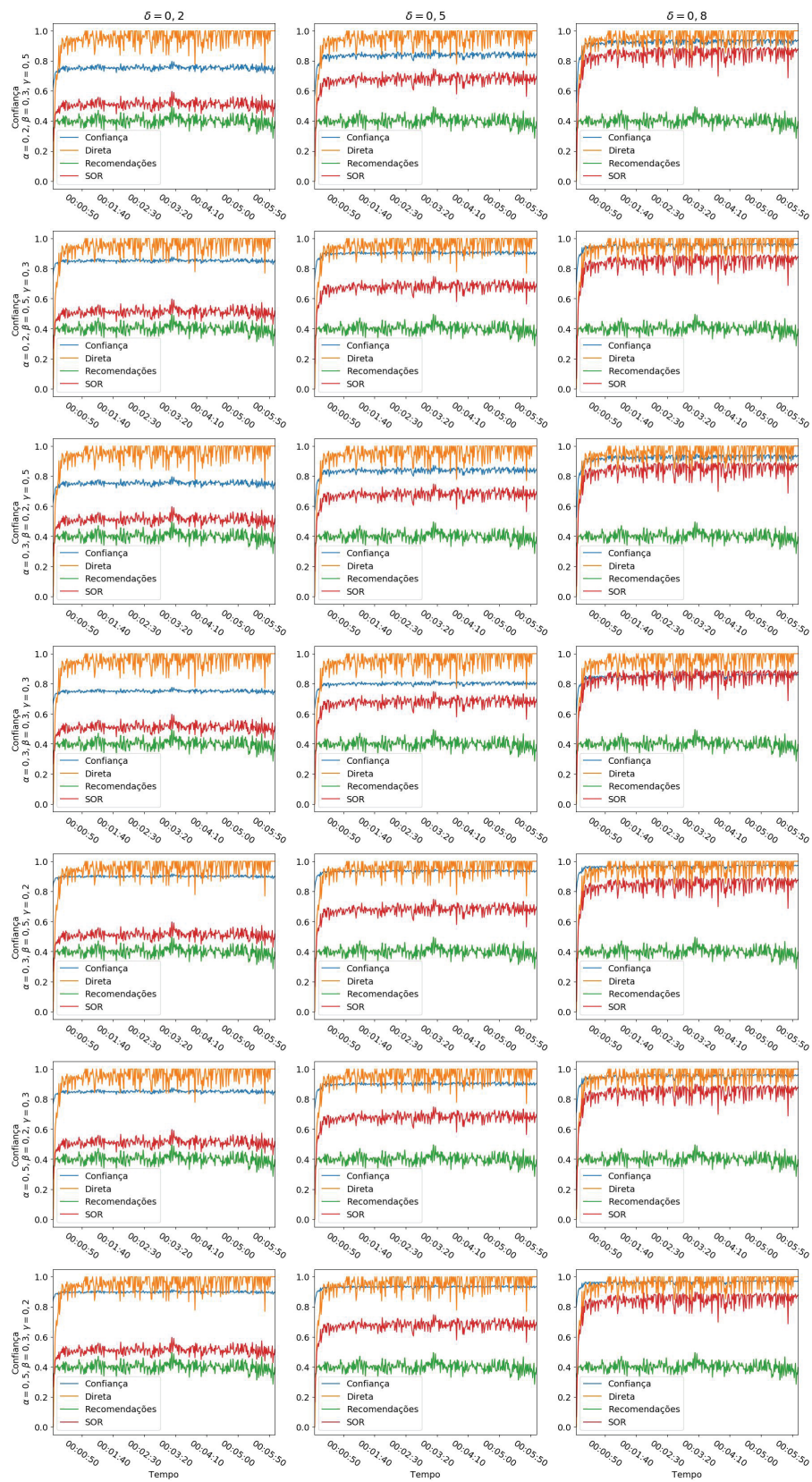


Figura B.1: EC para o Cenário 2 - DCP

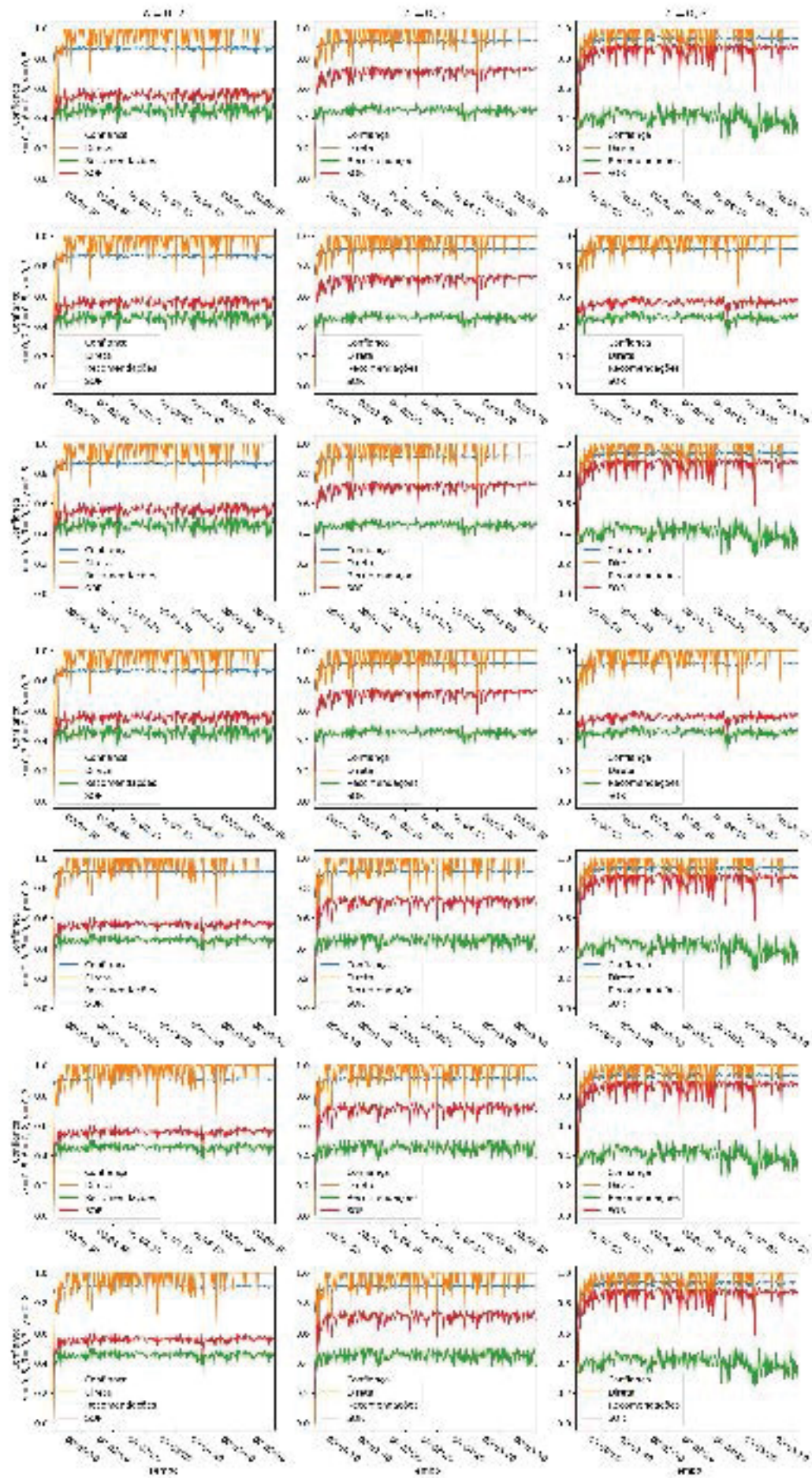


Figura B.2: EC para o Cenário 2 - DCS

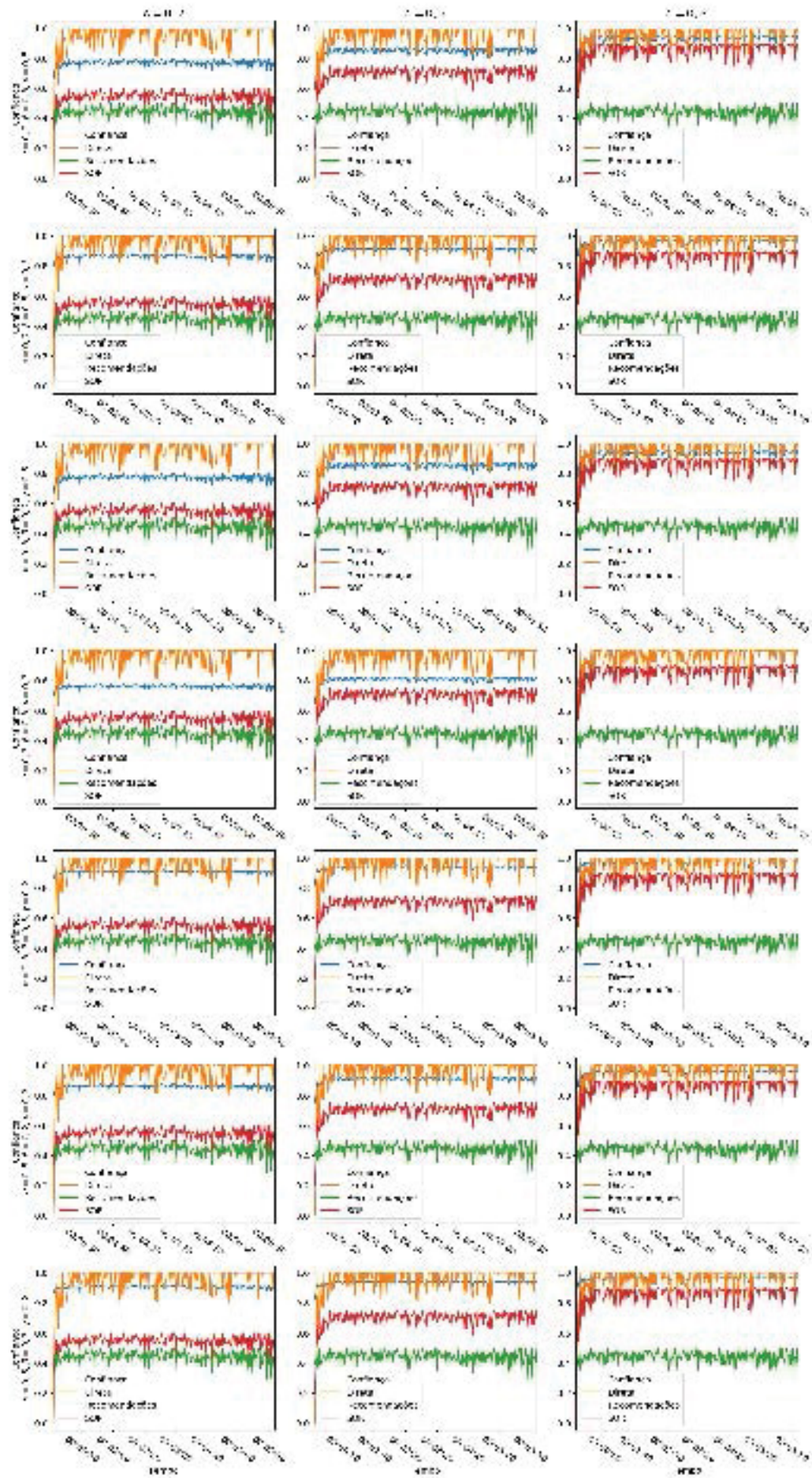


Figura B.3: *EC* para o Cenário 2 - DSP

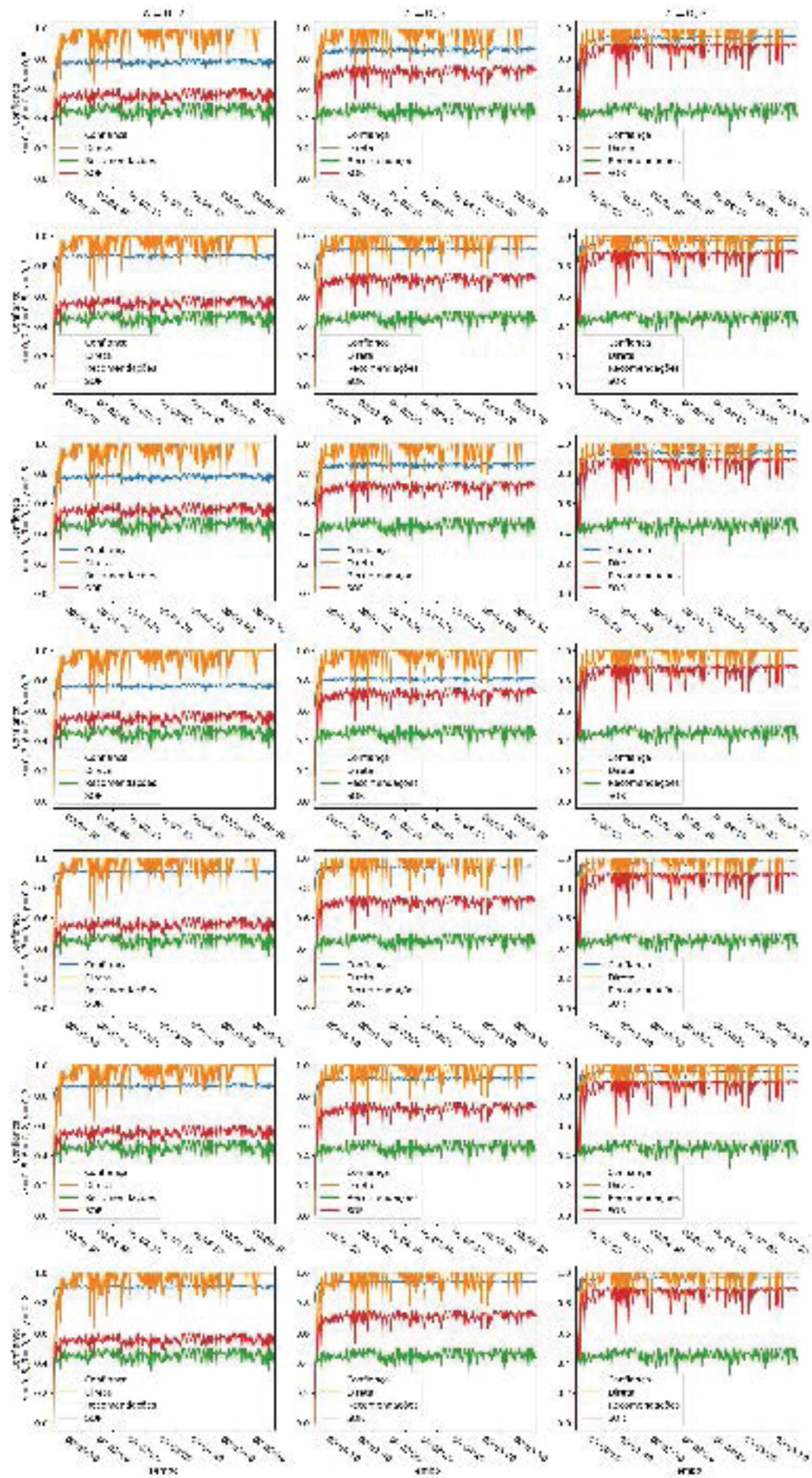


Figura B.4: *EC* para o Cenário 2 - DSS