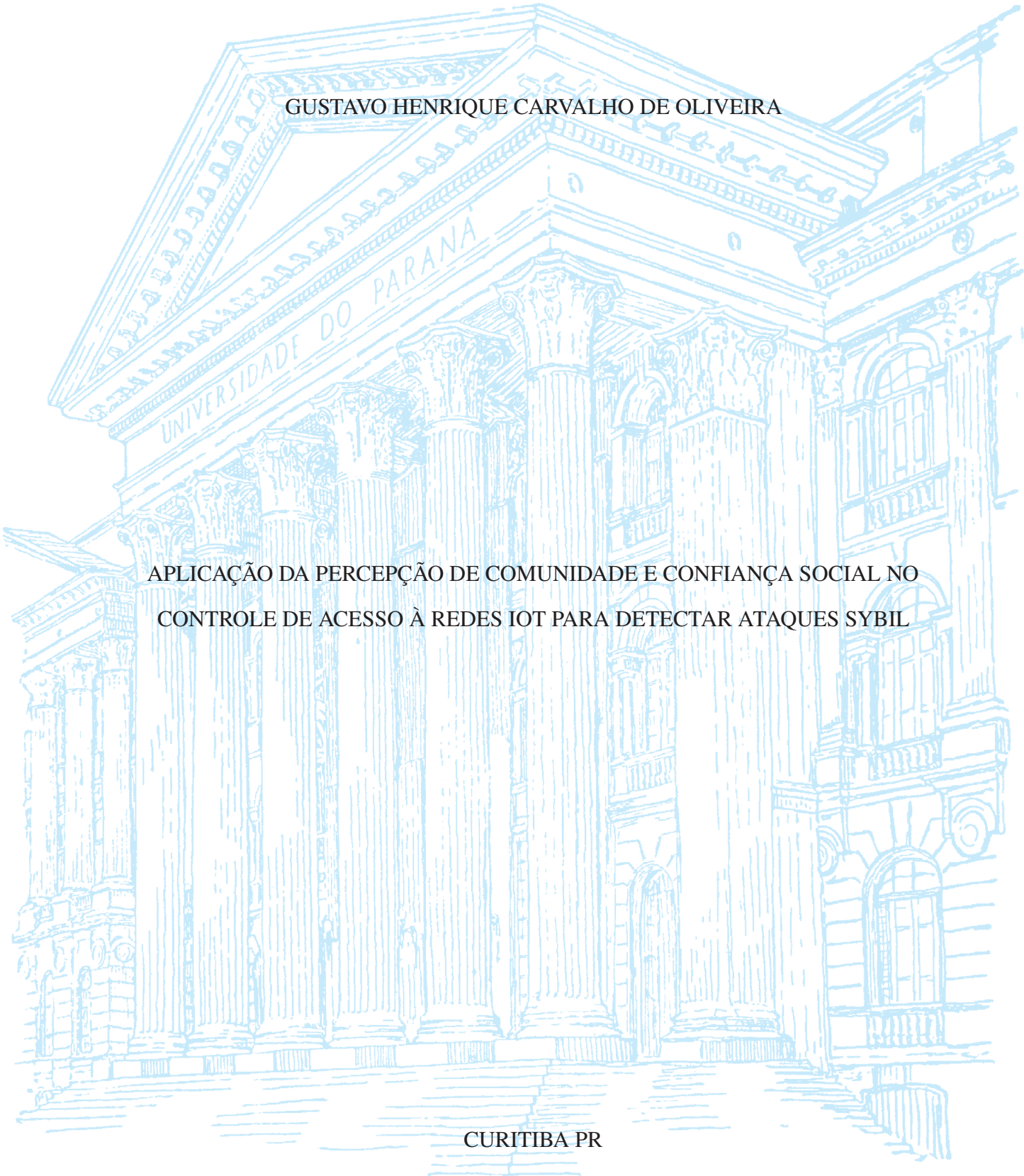
UNIVERSIDADE FEDERAL DO PARANÁ

GUSTAVO HENRIQUE CARVALHO DE OLIVEIRA



APLICAÇÃO DA PERCEPÇÃO DE COMUNIDADE E CONFIANÇA SOCIAL NO CONTROLE DE ACESSO À REDES IOT PARA DETECTAR ATAQUES SYBIL

CURITIBA PR

2019

GUSTAVO HENRIQUE CARVALHO DE OLIVEIRA

APLICAÇÃO DA PERCEPÇÃO DE COMUNIDADE E CONFIANÇA SOCIAL NO CONTROLE DE ACESSO À REDES IOT PARA DETECTAR ATAQUES SYBIL

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

2019

Catalogação na Fonte: Sistema de Bibliotecas, UFPR
Biblioteca de Ciência e Tecnologia

O48a Oliveira, Gustavo Henrique Carvalho de
Aplicação da percepção de comunidade e confiança social no controle de acesso à redes IoT para detectar ataques Sybil [recurso eletrônico] / Gustavo Henrique Carvalho de Oliveira. – Curitiba, 2019.

Dissertação - Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-Graduação em Informática, 2019.

Orientador: Aldri Luiz dos Santos .

1. Internet - Controle de acesso. 2. Computadores - Medidas de segurança. 3. Internet das coisas. I. Universidade Federal do Paraná. II. Santos, Aldri Luiz dos. III.Título.

CDD: 004.678

Bibliotecária: Vanusa Maciel CRB- 9/1928

MINISTÉRIO DA EDUCAÇÃO
SETOR SETOR DE CIENCIAS EXATAS
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO INFORMÁTICA - 40001016034P5

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação em INFORMÁTICA da Universidade Federal do Paraná foram convocados para realizar a arguição da Dissertação de Mestrado de **GUSTAVO HENRIQUE CARVALHO DE OLIVEIRA** intitulada: **Aplicação da Percepção de Comunidade e Confiança Social no Controle de Acesso a Redes IoT Para Detectar Ataques Sybil.**, após terem inquirido o aluno e realizado 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, 11 de Março de 2019.

ALDRI LUIZ DOS SANTOS
Presidente da Banca Examinadora (UFPR)

JOSÉ AUGUSTO MIRANDA NACIF
Avaliador Externo (UFV)

MICHELE NOGUEIRA LIMA
Avaliador Interno (UFPR)

MINISTÉRIO DA EDUCAÇÃO - UNIVERSIDADE FEDERAL DO PARANÁ - Setor de Ciências Exatas - Coordenação de Pós-Graduação em Informática

Dedico este trabalho aquele a quem busco me espelhar para ser uma pessoa melhor a cada dia, exemplo para todos: Jesus. Dedico também aos meus pais que são a minha base e como disse Sir Isaac Newton: se vi mais longe, foi por estar em ombros de gigantes.

AGRADECIMENTOS

O presente trabalho representa um sonho que começou a ser formado na Universidade Tecnológica Federal do Paraná, onde fiz minha graduação e onde a paixão pela área e pelos estudos começou. Seu início em 2016 representava apenas o ponto de partida para um grande desafio, onde muitos finais de semana foram abdicados e muitas reuniões e escrita feitas em feriados. Ao fim, é natural que todo o esforço aplicado neste trabalho seja recompensado na forma de aprendizado e evolução pessoal, além da singela contribuição desta dissertação.

Inicialmente eu gostaria de agradecer a Deus por esta oportunidade e por poder concluí-la. Em seguida eu agradeço a minha família José Carlos, meu pai, Cristiane, minha mãe, e ao meu irmão Gabriel que sempre me apoiaram e me ajudaram, não apenas financeiramente, mas também com concelhos e aconchego para descansar durante a escrita deste trabalho. Também gostaria de agradecer a família Luzza: Isabel, Iara e Wagner que passaram comigo a maior parte deste período me incentivando, aconselhando e me acolhendo durante as várias viagens para Cascavel.

Meus agradecimentos também se estendem aos meus colegas do grupo de pesquisa NR2[1] e CCSC[2] os quais foram fundamentais para conclusão deste trabalho; sempre receptivos, dispostos a ajudar e ensinar. Por isso quero agradecer especialmente ao: Paulo Lenz, Benevid Felix, Carlos Pedroso, Arthur Garcete, Mateus Peloso, Rafael Araújo, Agnaldo, Lígia, Fernando Nakayama, Cainã, Bruno Marques, Euclides, Igor Steuck e Danilo Passati.

Em especial quero agradecer ao meu orientador Aldri Santos por se dedicar todos os dias em formar alunos com excelência em pesquisa e na formação do senso crítico, algo que vou levar comigo para o resto da vida. Obrigado pelos ensinamentos e esforço de me orientar entre as várias tarefas do dia, as inúmeras reuniões e e-mail enviados resultaram nesta contribuição cientifica. Agradeço também a professora Michele Nogueira por fazer parte desta caminhada, ensinando e colaborando para melhorar as discussões e problemas abordados no presente texto.

Agradeço a CAPES e UFPR que fomentaram este estudando, liberando ajuda financeira e infraestrutura para o desenvolvimento de pesquisas essenciais para o futuro deste país.

A todos que estiveram direta ou indiretamente envolvidos com o desenvimento deste trabalho. Meu muito obrigado!

[1] Núcleo de Redes Avançadas

[2] Center for Computational Security sCience

RESUMO

A Internet das Coisas envolve diversos dispositivos conectados entre si, geralmente compreendendo dispositivos pessoais que contém informações como hábitos e comportamentos dos usuários. Esses dispositivos disseminam dados pela rede contendo informações pessoais de seus usuários, bem como de outros usuários. Por esse motivo, muito se tem discutido em como preservar a privacidade em redes não estruturadas e de baixa disponibilidade de recurso, característica encontrada nas redes de borda da IoT. Por consequência, se a rede estiver vulnerável a um invasor mal intencionado, requisitos de segurança como privacidade, integridade e disponibilidade podem ser quebrados. Logo, esses ambientes demandam por soluções que diminuam as vulnerabilidades e aumentem a sua segurança quanto à presença de intrusos. Entre essas medidas de segurança encontra-se o serviço de controle do acesso, responsável em gerenciar quem pode acessar as informações transmitidas na rede. De modo a evitar a presença de intrusos que venham a comprometer a privacidade ou perturbar o funcionamento da rede. Entre os tipos de intrusos destaca-se o atacante Sybil, este tipo de ataque consiste na personificação de identidades roubadas ou fabricadas tal que o atacante se passe por um nó legítimo na rede. Para fornecer proteção contra esses ataques, um serviço de controle de acesso deve ser efetivo a fim de bloquear o acesso não autorizado. Em geral, as técnicas presentes na literatura para realizar esse controle dentro da IoT têm sido baseadas em capacidade, risco e no gerenciamento da confiança. Esta dissertação tem como objetivo criar um controle de acesso à redes IoT que possa detectar atacantes Sybil buscando autenticação. Foram investigados os modelos de controle de acesso propostos para IoT com a finalidade de identificar suas características e possíveis contribuições para este trabalho. Além disso, identificou-se que novos aspectos como a formação de relações sociais entre os dispositivos e a ciência de mudanças no contexto podem proporcionar uma maior resiliência ao serem incorporados nas técnicas de controle de acesso. A inteligência em construir relações sociais encontra-se na *Social Internet of Things* (SIoT) e possibilita que sistemas para o controle de acesso possam agregar contexto de comunidade e informações de sociabilidade dos dispositivos. Assim, este trabalho propõe o mecanismo ELECTRON para o controle de acesso em redes IoT baseado em confiança social entre os dispositivos para proteger a rede de ataques Sybil. ELECTRON utiliza o gerenciamento da confiança através da lógica subjetiva para calcular a confiabilidade dos dispositivos que requisitam acesso a rede e por meio da uma similaridade social, calculada pelo coeficiente de Jaccard, modela uma comunidade na rede. A sociabilidade e a noção de comunidade contribuiem para se obter um valor mais acurado da confiança. Os resultados obtidos no simulador NS-3 mostram a eficácia do ELECTRON em identificar ataques Sybil na IoT que buscam acesso à rede, principalmente em redes de pequeno e médio porte ao comparar com o mecanismo SA²CI. Ele alcançou até 93,5% de identificação e exclusão na melhor comunidade avaliada, e 82,4% na comunidade com taxas de detecção mais baixas, onde a confiança evoluiu com maior facilidade.

Palavras-chave: Controle de Acesso, Comunidade, Social, Confiança, SIoT, Ataques Sybil

ABSTRACT

The Internet of Things involves a variety of connected devices, usually comprising personal devices that contain information - such as users' habits and behaviors. These devices disseminate data across the network containing personal information from their users as well as from other users. For this reason, much has been discussed on how to preserve privacy in unstructured and resource-poor networks, a feature found in IoT edge networks. As a result, if the network is vulnerable to a malicious attacker, security requirements such as privacy, integrity and availability may be breached. Therefore, these environments demand solutions that mitigate vulnerabilities and increase their security against intruders. Among these security measures is the access control service, which is responsible for managing who can access the information transmitted on the network. In order to prevent intruders from compromising privacy or disrupting network operation. Among the types of intruders stands out Sybil attacker, this type of attack is the impersonation of identities stolen or fabricated such that the attacker impersonates a legitimate node in the network. To provide protection against such attacks, an access control service must be effective to block unauthorized access. In general, the techniques in the literature to perform this control within IoT have been based on capacity, risk, and trust management. This dissertation aims to create an IoT network access control that can detect Sybil attackers seeking authentication. The access control models proposed for IoT were investigated in order to identify their characteristics and possible contributions to this work. In addition, it was identified that new aspects such as the formation of social relations between devices and the science of changes in context can provide greater resilience by being incorporated into access control techniques. Intelligence in building social relationships is found in Social Internet of Things (SIoT) and enables systems for access control to aggregate community context and device sociability information. Thus, this paper proposes the ELECTRON mechanism for access control in IoT networks based on social trust between devices to protect the network from Sybil attacks. ELECTRON uses trust management through subjective logic to calculate the reliability of devices requesting network access and through social similarity, calculated by the Jaccard coefficient, models a community on the network. Sociability and the notion of community contribute to a more accurate value of confidence. The results obtained in the NS-3 simulator show the effectiveness of ELECTRON in identifying Sybil attacks on IoT that seek network access, especially in small and medium networks. compared to the SA²CI engine. It achieved up to 93.5% identification and exclusion in the best community assessed, and 82.4% in the community with the lowest detection rates, where confidence evolved most easily.

Keywords: Access Control, Community, Social, Trust, SIoT, Sybil Attack

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

6LowPAN	*Internet Protocol v6 over Low-Power Wireless Personal Area Networks*
ABAC	*Attribute-Based Access Control*
AdRBAC	*Adaptive Risk-Based Access Control*
AP	*Access Point*
AR	Arquitetura Referencial
ARM	*Architecture Reference Model*
AS	Ataque *Sybil*
CapBAC	*Capacity-Based Access Control*
CI	Interesses em Comum
CNTD	*Clustered Neighbor Based Trust Dissemination*
COCapBAC	*Community Capacity-Based Access Control*
CTMOS-SIoT	*Context-based Trust Managment System for the Social Internet of Things*
C-LOR	*Co-location Object Relationship*
C-WOR	*Co-Work Object Relationship*
DCapBAC	*Distributed Capacity-Based Access Control*
DIS	*DODAG Information Solicitation*
DMAS	*Distributed Multi Agent System*
DODAG	*Destination Oriented Directed Acyclic Graph*
ECC	*Elliptic Curve Cryptography*
ELECTRON	*Access Control Driven on Community and Social Trust of Things*
EU FP7	*European Lighthouse Integrated Project*
EX	*Experience*
FTBAC	*Fuzzy approach to the Trust-based Access Control*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IIRA	*Industrial Internet Reference Architecture*
IoT	*Internet of Things*
IPv6	*Internet Protocol version 6*
KN	*Knowledge*
LS	Lógica Subjetiva
LTE-A	*Long Term Evolution Advanced*
MIMO	*Multiple-Input and Multiple-Output*
MIT	*Massachusetts Intitute of Technology*

MR	Modelo Referencial
NBTD	*Network Based Trust Dissemination*
NFC	*Radio Frequency Identification*
NS-2	*Network Simulator 2*
NS-3	*Network Simulator 3*
OOR	*Ownership Object Relationship*
PDR	*Packet Delivery Ratio*
POR	*Parental Object Relationship*
QoS	*Quality of Service*
RBAC	*Role-Based Access Control*
RC	*Recommendation*
RFID	*Radio-Frequency Identification*
RPL	*Routing Protocol for Low power and Lossy networks*
RSS	*Received Signal Strength*
RSSI	*Received Signal Strength Indication*
SA²CI	*Sybil Attack Association Control for IoT*
SIoT	*Social Internet of Things*
SOR	*Social Object Relationship*
SybM	*Sybil-Mobile Attack*
TACIoT	*Trust-Aware Access Control System for IoT*
TTD	*Tree Based Trust Dissemination*

LISTA DE SÍMBOLOS

N	Conjunto de nós da rede
N_{man}	Conjunto de nós sem restrição de recurso
N_{sub}	Conjunto de nós com restrição de recurso
Id_r	Conjunto de identidades roubadas
Id_f	Conjunto de identidades fabricadas
C	Comunidade
$Similarity_{threshold}$	Limite para similaridade
$S_{i,j}$	Similaridade entre i e j
φ	Importância das métricas A e CI
$A(i,j)$	Similaridade por amizade
$CI(i,j)$	Similaridade por interesses em comum
T_{ij}^{C}	Confiança geral do objeto i em relação ao objeto j dentro da comunidade C
D_{ij}	Confiança direta
R_{ij}	Recomendações
α	Peso para confiança direta
β	Peso para similaridade entre os objetos
γ	Peso para as recomendações
b	Crença (*belief*)
d	Descrença (*disbelief*)
u	Incerteza (*uncertainty*)
$\omega_{C}^{A:B}$	Desconto entre duas opiniões
$\omega_{C}^{A\Diamond B}$	Consenso entre duas opiniões
R_d	Taxa de detecção
R_a	Acurácia
R_{fp}	Falsos Positivos
R_{fn}	Falsos Negativos
P_{ec}	Consumo Energético

SUMÁRIO

1 INTRODUÇÃO

A Internet das Coisas (IoT) proporcionou uma maior troca de dados entre os dispositivos (objetos) computacionais e os objetos do nosso cotidiano. Naturalmente, ela se consolida como a principal aplicação da Internet no futuro para vários aplicativos e serviços (Buyya e Srirama, 2019). A IoT tem sido abordada em diversos contextos, desde empresas ao anunciar novos produtos e serviços baseados na IoT até políticos reconhecendo o grande potencial econômico e oportunidades de negócios, onde estima-se que a IoT pode crescer em um mercado de 7,1 trilhões de dólares até 2025 (Wortmann e Flüchter, 2015). Contudo, pouco se tem falado de seu surgimento e definição. A origem do termo IoT data de mais de 20 anos e vem sendo atribuída a um trabalho do laboratório Auto-ID no Instituto de Tecnologia do Massachusetts (MIT, do inglês *Massachusetts Intitute of Technology*) (Fleisch, 2007). Desde então, várias visões da IoT foram propostas e sua finalidade inicial, limitada em *radio-frequency identification* (RFID), foi expandida para abranger diversos dispositivos computacionais, como sensores, atuadores, celulares e até eletrodomésticos (Atzori et al., 2010), trazendo como suas principais inovações a combinação de componentes físicos e digitais para criar novos produtos e serviços.

A IoT pode ser caracterizada como uma rede híbrida, heterogênea e aberta. A característica híbrida vem das várias redes estruturadas e não estruturadas contidas na IoT. Enquanto a heterogeneidade deve-se a grande diversidade de objetos, que por sua vez, fornecem uma pluralidade de serviços. Além disso, ao permitir que vários sistemas forneçam serviços para diferentes clientes, ela caracteriza-se como uma rede aberta (Al-Fuqaha et al., 2015). Os objetos presentes na IoT possuem uma propriedade chamada *identidade*, que fornece os dados necessários para identificar com quem ou com o que ocorre a comunicação; a propriedade *atributos físicos*, que disponibilizam informações sobre o dispositivo e/ou usuário; e a propriedade *interfaces inteligentes*, que corresponde aos diferentes canais de comunicações disponíveis e que, por serem inteligentes, permitem a personalização pelo usuário de acordo com a preferência. Logo, através da IoT, serviços como a mensuração de temperatura, a localização de objetos e até o monitoramento de funções vitais podem ser oferecidos.

Na medida que novos dispositivos passam a se comunicar pela Internet e novos serviços são oferecidos, novas aplicações para IoT são destacadas. Dentre essas, algumas se sobressaem como mais proeminentes no contexto industrial (Indústria 4.0), no contexto doméstico (*smart home*) e no contexto hospitalar (*eHealth*). Na Indústria 4.0, uma grande rede de sistemas ciber físicos em tempo real interliga fornecedores, indústria e clientes (Wortmann e Flüchter, 2015). O conceito de *smart home* une várias tecnologias interativas, com o objetivo de automatizar e agrupar funções da casa e entregar um controle para o proprietário. Alguns exemplos são as tecnologias de assistentes virtuais VPA (do inglês, *Virtual Personal Assistant*), tais como *Apple HomeKit* e *Alexa*, desenvolvidos pela Apple e Amazon (Gartner, 2017). Enquanto, as aplicações *eHealth* podem ajudar no monitoramento de pacientes a distância, como no uso de redes VANETs (do inglês, *Vehicular Ad hoc Networks*) e WBAN (do inglês, *Wireless Body Area Network*) para monitorar pacientes de longo prazo (diabetes, problemas de pressão sanguínea, idosos e pessoas com deficiência). A aplicação utiliza a rede WBAN para monitorar o paciente e acionar um sistema de alerta para informar ao profissional de saúde qualquer alteração nos dados vitais.

Embora todos os domínios de aplicação tenham seu devido foco dentro das pesquisas, as projeções apontam que as aplicações *eHealth* serão preponderantes na IoT até 2025 (Al-Fuqaha et al., 2015). Espera-se criar cerca de 1,1 a 2,5 trilhões de dólares americanos em crescimento anual com aplicações *healthcare* e serviços relacionados tal como *mobile health (m-Health)*, assim

como reduzir o tempo gasto em processos com a automação da coleta de dados e diagnósticos de prevenção em tempo real para pacientes através de sensores. Por conseguinte, todas essas funções necessitam de um serviço em comum: a disseminação de dados (Gielow et al., 2015). O serviço de disseminação de dados é fundamental para funções como a coleta de dados e a configuração do ambiente (Furlaneto et al., 2012), (Carrero et al., 2015). Por essa razão, a segurança e a privacidade assumem papéis importantes no futuro da IoT (Sicari et al., 2015).

Em um modelo de rede como da IoT, a disseminação de dados deve levar em conta a heterogeneidade dos dispositivos que compõem a rede (Figueiredo et al., 2005). Alguns desses dispositivos apresentam recursos limitados, enquanto outros possuem maior capacidade de processameto e energia. A transmissão de dados em dispositivos com restrição de energia consome cerca de 80% dos recursos da bateria, sendo uma disseminação eficiente e segura vital para o tempo de vida desses objetos (Alduais et al., 2016). Diante disso, a disseminação em uma rede IoT deve ser orientada pela capacidade do dispositivo, isto é, caso um dispositivo não disponha de recursos suficientes, o dispositivo mais próximo com capacidade se encarrega de realizá-la, garantindo a continuidade dos serviços prestados (Le et al., 2012). Como resultado, a disseminação de dados se torna a base para aplicações e serviços na IoT.

1.1 MOTIVAÇÃO

A disseminação de dados segura, tanto de dados pessoais quanto de dados de controle, é fundamental para o sucesso das aplicações nos diferentes domínios da IoT. O primeiro desafio está em diminuir falhas causadas pelas características da rede. As falhas geram erros, podendo ser de transmissão ou perda de pacotes, causados por fatores como mobilidade, limitação de recurso e tecnologia de transmissão (Sethi et al., 2015). Reduzir essas falhas e, consequentemente, os erros contribui para a queda nas taxas de retransmissão, melhorando a qualidade de serviços disponibilizados na rede e o custo para manter o funcionamento destes serviços para os dispositivos. Porém, nem todos os erros são gerados por falhas em componentes ou devido à mobilidade, usuários mal intencionados (atacantes) podem gerar falhas propositalmente nos dispositivos. Aproveitando de vulnerabilidades da rede, os atacantes podem inserir dispositivos com comportamento alterado causando erros na transmissão dos dados e degradando a qualidade do serviço. Todavia, esses atacantes representam uma maior ameaça para a privacidade dos dados disseminados, pois a partir do momento que os dispositivos atacantes têm acesso a rede os dados transmitidos ficam expostos.

Entre os ataques que buscam comprometer a privacidade, a integridade e a disponibilidade das informações encontram-se o *selective forwarding*, *black hole* e Sybil (Pongle e Chavan, 2015). Um ataque *selective forwarding* consiste em encaminhar seletivamente os pacotes, isto é, o dispositivo do atacante faz parte da disseminação, porém só encaminha dados que lhe interessa (geralmente apenas mensagens de controle). Já o *black hole* faz referência aos buracos negros que sugam tudo a sua volta e, da mesma forma, o atacante descarta todos pacotes de dados silenciosamente, fazendo com que todo dado se perca. Por fim, destaca-se o Ataque Sybil (AS) responsável por forjar várias identidades no mesmo nó físico, na tentativa de se passar por um nó legítimo. Para isso, o atacante rouba ou fabrica as identidades, na tentativa de adquirir níveis de controle elevados e comprometer a efetividade da rede e, em conjunto com outros ataques, prejudicar atributos da segurança como a privacidade e a confidencialidade dos dados disseminados.

A disseminação pode ser preservada implementando contramedidas para garantir a segurança aos dispositivos e usuários. Dentre essas medidas, evidencia-se o controle de acesso, tendo como principal função restringir o acesso a recursos da rede como os dados transmitidos e

os serviços disponíveis. As tecnologias de controle de acesso são elementos centrais para abordar problemas de segurança e privacidade em redes de computadores (Liu et al., 2012), prevenindo que usuários não autorizados tenham acesso aos recursos, certificando que usuários legítimos não acessam os recursos de maneira não autorizada e possibilitando que usuários legítimos acessem os recursos de modo autorizado. A IoT é o ambiente com maior demanda de escalabilidade e gerenciabilidade se comparado com os ambientes anteriores, por exemplo os baseados em serviços SOA (do inglês, *Service-oriented architecture (SOA)*) dinamicamente orquestrados, devido a dois fatores: o potencialmente ilimitado número de objetos e o suporte para orquestrar e integrar os diferentes serviços (Gusmeroli et al., 2012). Estes aspectos específicos da IoT implicam que o controle de acesso pode se tornar um verdadeiro pesadelo se não for empregado com novas abordagens e mecanismos de controle de acesso mais complexos e eficientes.

Novas formas de se estabelecer o controle de acesso foram então propostas, levando em consideração as restrições da IoT. Entre essas técnicas, destacam-se o controle de acesso baseado em: **(i)** capacidade (*Capability Based Access Control - CapBAC*) (Hernández-Ramos et al., 2016; Hussein et al., 2017), **(ii)** risco (*Risk Based Access Control - RiskBAC*) (Alenezi et al., 2017) e **(iii)** confiança (*Trust Based Access Control - TBAC*) (Mahalle et al., 2013; Bernal Bernabe et al., 2016; Khan e Herrmann, 2017). No controle de acesso CapBAC, uma entidade autenticadora recebe a requisição de acesso de um requisitante externo. A entidade avalia o dispositivo requisitante e devolve uma chave indicando seus níveis de permissão dentro da rede. Essa chave será verificada por outros dispositivos dentro da rede de forma a garantir que existe permissão para as informações acessadas. Enquanto no RiskBAC, um gerenciador de risco avalia vários fatores para permitir o acesso na rede. Esses fatores incluem indícios de ameaças, contexto, histórico, entre outros e no final são quantificados em um valor de risco, que determina o acesso. Por outro lado, o gerenciamento da confiança avalia o quanto um dispositivo é confiável através da análise do seu comportamento por interações.

A confiança tem sido aplicada em vários domínios da computação e com diversos propósitos (Cho et al., 2015), (Mannes et al., 2012b), (Mannes et al., 2012a). Pesquisas em Inteligência Artificial (IA) têm estudado como a confiança pode ajudar a modelar agentes. Assume-se que os agente devem ser inteligentes, cooperativos e independentes, então considera-se a confiança um fator chave para as relações entre os agentes em sistemas multiagentes distribuídos (DMASs) (Hang e P Singh, 2012). A fusão de dados (*data fusion*) é outra área que emprega confiança para a tomada de decisão no processo de escolha entre as várias técnicas de fusão (Yang et al., 2010). A fusão de dados consiste no processo de combinar múltiplos registros em um, na presença de incerteza, incompletude e conflito de evidências. A mineração de dados (*data mining*) também utiliza avaliação de confiança em várias de suas aplicações: para preservar a privacidade ao analisar quantidades massivas de dados (*big data*); identificar confiança, desconfiança, e/ou fatores de privacidade em redes sociais; e analisar relações confiáveis em *big data* gerados por redes sociais (*Facebook*, *Twitter*) (Bachi et al., 2012).

Embora as soluções CapBAC, RiskBAC e TBAC demonstrem ser promissoras para o controle de acesso na IoT, elas ainda se baseiam nas características dos dispositivos ou necessitam estabelecer confiança dentro de um domínio de hardware, sem empregar inteligência sobre as relações dos objetos (inteligência social). E isso nem sempre reforça a verdadeira interação, isto é, relação de conexões entre indivíduos construída no dia-a-dia e, portanto, de confiança entre os dispositivos; assim como acorre em relações humanas em suas comunidades, como família, trabalho, escola, entre outros. Tais relações nos permitem estabelecer níveis de confiança mais fortes e utilizá-los para restringir o acesso aos lugares e aos dados privados das pessoas e dispositivos (Abderrahim et al., 2017); formando uma inteligência social. O uso de aspectos subjetivos em dispositivos IoT vai de encontro ao paradigma *Social Intenet of Things*

(SIoT) (Atzori et al., 2012), que consiste na evolução das associações dos dispositivos na IoT baseada nas relações humanas para disseminar dados na rede.

1.2 DEFINIÇÃO DO PROBLEMA

A concretização da IoT ainda cria muito expectativa principalmente pelos serviços e domínios de aplicação oferecidos. Automação de tarefas e criação de serviços como o monitoramento remoto de pacientes são algumas propostas para revolucionar o modo como interagimos com os objetos. Entretanto, para a real implementação deste cenário, medidas de segurança devem certificar que somente pessoas autorizadas obtenham acesso as informações trafegadas na rede. Mantendo a privacidade de seus usuários contra potenciais ameaças, dentre elas o ataque Sybil. Este tipo de ataque, em especial, chama a atenção pela sua capacidade de comprometer atributos da segurança como a privacidade (Evangelista et al., 2016a). O comportamento Sybil é o primeiro passo para uma sucessão de ataques, onde um atacante Sybil autenticado pode adiquirir níveis desproporcionais de controle, obter informações vitais e afetar a privacidade dos dados, o consumo de recursos, o desempenho em geral da rede e possivelmente até a integridade dos dados (Rajan et al., 2017; Evangelista et al., 2016b), se mostrando uma real ameaça para redes IoT. O principal problema abordado nesta dissertação consiste em: **como oferecer um ambiente seguro à disseminação de dados, que dê suporte a outros serviços essenciais dentro de um ecossistema IoT, diante da ameaça da presença de atacantes que buscam comprometer a privacidade dos dados.**

Para aumentar a segurança nas redes, contramedidas têm sido aplicadas na identificação e isolamento de atacantes Sybil. As atuais técnicas de detecção dividem-se em três estratégias: *(i)* baseadas em ferramentas da rede, *(ii)* certificação confiável e *(iii)* relacionamento entre vizinhos (Sicari et al., 2015; Alaba et al., 2017; Fernandez-Gago et al., 2017). As relações sociais propostas pela SIoT estão sendo aplicadas no contexto de segurança para ajudar na identificação de ataques. Embora existam diferentes estratégias para encontrar e impedir a associação de invasores Sybil, elas apresentam desvantagens que somam um alto custo computacional, baixa eficácia e necessidade de treinamento *offline*. Logo, este problema tem incentivado a pesquisa de novos métodos de detecção para preencher as lacunas em aberto na segurança e privacidade da disseminação de conteúdo na IoT. Considerando o problema levantado, esta dissertação busca explorar e responder as seguintes questões de pesquisa:

- *As relações sociais entre os dispositivos dentro da rede SIoT podem contribuir para aumentar a segurança no controle de acesso?*
  Permitir que os dispositivos construam relações entre si cria novos aspectos que podem ser explorados por novos modelos de segurança. Esses aspectos estão sendo explorados em pesquisas para facilitar a modelagem acurada da confiança em sistemas de recomendação e em outros tipos de ataque na IoT.

- *As relações sociais da SIoT influenciam na construção da confiança social?*
  As relações sociais dentro da SIoT são divididas pelo tipo dos dispositivos, sua localização, finalidade de aplicação e pelo comportamento social de seu usuário. Dentre essas relações, níveis de importância podem ser estipulados a fim de priorizar as relações mais íntimas.

- *A confiança social pode ser utilizada de modo eficaz para identificar atacantes Sybil?*
  A confiança baseia-se no comportamento observável de um dispositivo requisitante em questão. Proporcionar que os objetos possam se relacionar e esses relacionamentos

influenciarem a confiança verificada, pode contribuir para a identificação de possíveis atacantes que buscam se identificar com identidades falsas.

1.3 OBJETIVO

Esta dissertação busca como objetivo criar um controle de acesso à rede seguro, que leve em conta a percepção do contexto e da sua confiança social. Ao permitir que o mecanismo tenha ciência do contexto, parâmetros para o cálculo da confiança podem ser ajustados, a fim de se obter valores mais precisos. Ao passo que a confiança baseada na sociabilidade permite que dispositivos com relações mais significativas e, consequentemente, com maior interação conquistem maior confiabilidade. Ao cogitar o resultado do serviço de controle de acesso como restringir o acesso à rede para dispositivos não autorizados, conceder mais capacidade para este serviço remete em maior proteção para a privacidade dos dados. Por conseguinte, este trabalho propõem um mecanismo de controle de acesso denominado ELECTRON (*acc***E***ss contro***L** *driv***E***n on* **C***ommunity and social* **TR***ust* **O***f thi***N***gs*). Logo, o princípio para modelar este serviço na rede consiste na confiança estabelecida nas relações sociais dos dispositivos, e assim identificar atacantes Sybil. Além disso, ele deve ser distribuído, escalável, sensível ao contexto e energicamente factível, tal que atenda aos requisitos para um controle de acesso em uma rede com as características da IoT.

Para atingir o objetivo geral, os seguintes objetivos específicos foram definidos:

- Investigar os modelos de controle de acesso propostos para IoT e propor uma taxonomia.
- Projetar um modelo de controle de acesso baseado no relacionamento dos objetos com percepção de comunidades, que possa atender aos requisitos levantados.
- Implementar o modelo proposto e o SA²CI em um simulador de rede com a finalidade de analisar a real viabilidade da proposta, comparando os resultados obtidos dos dois modelos.
- Analisar os resultados obtidos via simulação para validar se o modelo atende aos requisitos levantados, e identificar as vantagens e limites da abordagem aplicada.

1.4 CONTRIBUIÇÕES

O desenvolvimento desta dissertação resultou em contribuições científicas na área de computação, com ênfase na segurança dentro de redes IoT através do controle de acesso e na construção de relações sociais dos dispositivos. As seguintes contribuições foram obtidas:

- *Um estudo do estado da arte da literatura*. O estudo apresenta uma classificação dos modelos de controle de acesso para redes IoT, levando em consideração aspectos como histórico, contexto, características do objeto, regras e sociabilidade. As técnicas apresentadas permitem estabelecer maior segurança na rede, restringindo o acesso a dispositivos não autorizados.
- *A proposição de um mecanismo, chamado ELECTRON, para o controle de acesso em redes IoT*. Este mecanismo baseia-se na percepção de comunidade e resistente a ataques Sybil. Ele emprega a confiança social para permitir a identificação de atacantes requisitando acesso à rede, contribuindo para manter a privacidade dos dados disseminados.

1.5 ESTRUTURA

Esta dissertação de mestrado está estruturada em seis capítulos. O Capítulo 2 apresenta a fundamentação de conceitos de IoT, a inclusão do aspecto social aos dispositivos e a composição de comunidades em grafos e em redes sociais. O Capítulo 3 discute os trabalhos da literatura que buscam resolver o problema e os modelos tradicionais na construção da confiança. O Capítulo 4 descreve o mecanismo ELECTRON para o controle de acesso baseado em confiança social e contexto de comunidades. O Capítulo 5 apresenta uma avaliação dos mecanismos ELECTRON e SA²CI dividida em duas partes: avaliação dos aspectos sociais e avaliação dos aspectos de segurança do mecanismo. O Capítulo 6 conclui este trabalho apontando também para as direções futuras desta pesquisa.

2 FUNDAMENTOS

Este capítulo descreve os principais fundamentos necessários à compreensão do problema de pesquisa, das perguntas de pesquisa levantadas e da proposta de um mecanismo para controle de acesso a IoT. A Seção 2.1 descreve sobre a formação da Internet das Coisas e sua evolução ao longo do tmepo. Ela também aborda as aplicações que se destacam na IoT, as tecnologias envolvidas e sua arquitetura. A Seção 2.2 aponta os principais requisitos de segurança para sd redes sem fio, o funcionamento do ataque Sybil e as técnicas de detecção existentes. A Seção 2.4 descreve como o gerenciamento da confiança vem sendo empregada para segurança em ambientes distribuídos como a IoT. A Seção 2.5 detalha o paradigma *Social Intenet of Things*, responsável por estabelecer a noção de relacionamentos sociais entre os objetos; bem como os conceitos de formação de comunidades e o seu uso para o oferecimento de serviços em redes de computadores.

2.1 INTERNET DAS COISAS

Kevin Ashton, pesquisador do *Massachusetts Institute of Technology* (MIT) e considerado o pai do termo "Internet das Coisas" (IoT do inglês, *Internet of Things*) cunhou o conceito em 1999 (Parwekar, 2011). Em sua definição para o que seria esse novo termo, Ashton citou: todas as coisas estão conectadas pela Internet via dispositivos sensores tais como os proporcionados pela tecnologia RFID (do inglês, *Radio-Frequency Identification*) para atingir uma inteligência de identificação e gerenciamento. Ainda, alguns anos antes, o livro The Power to Predict (O Poder de Prever) fez uma contribuição pioneira para cenários de aplicações da IoT em 1995. Conforme novas pesquisas e tecnologias foram surgindo, novos dispositivos passaram a comunicar-se através da Internet incorporando inteligência em seu comportamento. A IoT foi então genericamente definida como "uma infraestrutura de rede global dinâmica com a capacidade de autoconfiguração e baseada em padrões e protocolos de comunicações interoperáveis" (Li et al., 2015). As "coisas" dentro da rede possuem identidades, atributos e utilizam interfaces inteligentes sendo integrada como uma rede de informação. A identidade fornece dados necessários para identificar com qual usuário ocorre a comunicação ou, se for caso, com qual dispositivo na rede. Os atributos disponibilizam informações sobre o dispositivo e/ou usuário, enquanto as interfaces inteligentes consistem nas diferentes formas para que o sistema/pessoa interaja com a rede e que, por serem inteligentes, permitem a personalização pelo usuário de acordo com a preferência. Porém, conforme as pesquisas avançam, o termo IoT tem representado um macro domínio, enquanto outros subdomínios são criados de acordo com sua aplicação.

Basicamente, a IoT consiste de sensores e pequenos dispositivos (atuadores) embutidos em objetos físicos como carros, eletrodomésticos e maquinas industriais ligados através de redes cabeadas ou sem fio (*wireless*), empregando, em sua maioria, protocolos que os conectam a Internet (Vasseur e Dunkels, 2010). Ao juntar as palavras "Internet" e "coisas" semanticamente significa "uma rede mundial de objetos conectados e unicamente endereçados", compreendendo objetos físicos capazes de receber sensores e tecnologias de comunicação. Os objetos passam a ter a capacidade de sensorear o ambiente e comunicar-se, gerando um imenso volume de dados analisados por computadores. O aspecto revolucionário está na implantação em curso desses sistemas físicos de informação e alguns deles podendo operar largamente sem a intervenção humana (ETSI, 2017). Esta revolução surge para melhor servir a sociedade moderna, que sofre com restrição de recursos nos campos de energia, transporte, logística e financeira enquanto, simultaneamente, existe um crescimento na demanda por saúde e serviços de tratamento médico.

Com a inserção de inteligência em vários objetos, muitas aplicações para a IoT puderam ser viabilizadas. Em aplicações *eHealth*, micro câmeras em forma de pílulas mandam imagens para identificar fontes de doenças no trato digestivo. Na agricultura de precisão, conexões *wireless* ligam equipamentos com dados de satélites e sensores espalhados pelo campo. Essas informações fazem com que o maquinário adapte em tempo real o cultivo - como por exemplo aplicando mais fertilizante em áreas com maior falta de nutrientes. *Outdoors* com propagandas no centro de grandes cidades podem analisar os pedestres caminhando na calçada e, baseado no perfil do pedestre, instantaneamente adaptar os anúncios. Processos industriais integrados com sensores podem ser controlados com maior precisão, elevando a eficiência. Ainda, com o contínuo monitoramento dos ambientes de produção, objetos aplicam medidas corretivas para evitar riscos e diminuir custos (ETSI, 2017). Entretanto, espera-se que aplicações no domínio de *eHealth* representem a maior porcentagem do mercado até 2025, seguido logo após por aplicações voltadas para a indústria (Al-Fuqaha et al., 2015).

Para entregar serviços inteligentes, os objetos heterogêneos conectados devem possuir tecnologias para comunicação. Comumente, os nós na IoT operam em um ambiente usando baixo consumo de energia e na presença de *links* com perda e ruído (Al-Fuqaha et al., 2015). Dentro desse contexto, algumas tecnologias possibilitam essa comunicação, entre elas estão: o padrão IEEE 802.11, mais conhecido como WiFi; o padrão 802.15.1, conhecido também como *Bluetooth*, foi inicialmente criado pela IEEE, mas atualmente é gerenciado pela *Bluetooth Special Interest Group* (SIG); o padrão 802.15.4 define a operação em redes sem fio de baixa taxa e que posteriormente foi em englobado pelas redes 6LowPAN (do inglês, *Internet Protocol v6 over Low-Power Wireless Personal Area Networks*). O 6LowPAN é um trabalho desenvolvido pela IETF (do inglês, *Internet Engineering Task Force*) e pode ser encarado como uma evolução do padrão 802.15.4, operando sobre o protocolo de comunicação IPv6 (do inglês, *Internet Protocol v6*); LTE-A (do inglês, *Long Term Evolution Advanced*) é a tecnologia de comunicação utilizada pelas operadores de telecomunicação em dispositivos móveis e representa uma evolução do anterior LTE, trazendo como principal vantagem o aumento da taxa de transferência e o uso de antenas MIMO (do inglês, *Multiple-Input and Multiple-Output*) (Berardinelli et al., 2009); Zigbee, utilizado também em comunicação em redes PAN e baseado no padrão 802.15.4; RFID; e, por fim, o NFC (do inglês, *Near Field Communication*). Todavia, nem todas essas tecnologias têm a capacidade de se comunicar entre si. Para que haja essa comunicação, arquiteturas integrando a heterogeneidade são necessárias.

2.1.1 Arquitetura

Embora nenhuma arquitetura padrão tenha sido definida para a IoT (Nath, 2017), duas arquiteturas propostas se destacam na literatura: IIRA (do inglês, *Industrial Internet Reference Architecture*) e IoT-A (do inglês, *Internet of Things Architecture*) (Weyrich e Ebert, 2016). As duas arquiteturas podem ser comparadas considerando três perspectivas. A primeira perspectiva consiste da *orientação semântica* - interpretação dos dados e informações para criar conhecimento em casos de uso. A IIRA tem seu foco em indústrias, lidando com funcionalidades como negócios, operação (prognóstico, monitoramento, otimização), informação (análise de dados) e aplicação. Enquanto a IoT-A se concentra nos aspectos genéricos da informação, ao invés de se ater a semântica. A segunda perspectiva compreende a *orientação para internet*, com aspectos para serviços *middleware* de suporte a gerenciamento de dados. As duas arquiteturas cobrem extensivamente modelos e estruturas para processos de negócios IoT, serviços IoT, organização para cruzamento de serviços e informação. Porém a IIRA permanece fechada para negócios e casos de uso. A terceira perspectiva constitui a *orientação para coisas*, que se concentra em aspectos como sensores, atuadores e *tags*, as quais são cruciais às duas arquiteturas. Ambas

arquiteturas possuem mecanismos de gerenciamento e segurança entre as camadas e proveem modelos descritivos de como dispositivos e humanos interagem e processam dados, contudo tendo diferentes perspectivas e granularidade em descrever a IoT.

Em especial, a IoT-A foi desenvolvida pelo projeto EU FP7 (do inglês, *European Lighthouse Integrated Project*) e representa a principal iniciativa de uma visão harmonizada da IoT. Seu principal resultado sucedeu na definição do modelo ARM (do inglês, *Architecture Reference Model*) para sistemas IoT, com a ideia central de prover uma estrutura comum e diretrizes para lidar com aspectos centrais de desenvolvimento, usando e analisando sistemas IoT (Meissner e Walewski, 2013). O modelo ARM consiste de três partes interconectadas e baseadas nas boas práticas da engenharia de software, sendo elas: o Modelo Referencial (MR), a Arquitetura Referencial (AR) e o conjunto de Orientação. O MR prove os conceitos e definições nos quais a arquitetura IoT pode ser construída e é a primeira grande contribuição do ARM. Além disso, o MR consiste de vários submodelos como: modelo de domínio; modelo de informação; modelo de comunicação; modelo funcional; e *modelo para segurança, confiança e privacidade*. Baseado nos submodelos descritos no MR, a AR apresenta um conjunto de visões e perspectivas, empregados para representar aspectos estruturais e focar na qualidade do sistema. Por fim, o conjunto de Orientação define o processo, que baseado no MR e AR, comandam a geração da arquitetura IoT (Krco et al., 2014).

2.1.2 Disseminação de dados

A computação ubíqua proporciona aos dispositivos se comunicarem em qualquer lugar e a qualquer momento (Atzori et al., 2010). Como resultado, ela trouxe benefícios para a implementação da IoT, visto que os modelos dos serviços necessitam de uma comunicação pervasiva entre os dispositivos. Nesse sentido, as informações coletadas por dispositivos com restrição de recurso (isto é, sensores, termômetros, atuadores, etc.) precisam ser transmitidas para dispositivos com maior poder de processamento, para que esses possam processar e/ou encaminhar essa informação. Este processo denomina-se disseminação de dados.

O ambiente em que a rede IoT está inserida determina o tipo de informação disseminada. Esse conteúdo pode variar entre: texto, áudio, vídeo e informações de controle. Em redes inseridas em indústrias ou em rodovias inteligentes, o maior fluxo de informação trafegada será de texto, enquanto em uma rede inserida em comércios ou em casas inteligentes, o fluxo representativo será de áudios e vídeos, tendo em vista que esses ambientes exploram mais serviços de *streaming* de vídeos e o compartilhamento de áudio e imagens. Portanto, o tipo de informação está associado ao ambiente e ao poder de processamento dos dispositivos presentes.

Com tanta informação trafegando pela rede, classificar esses dados coletados de acordo com a criticidade, a emergência e a periodicidade da coleta mostra-se um serviço importante nas futuras aplicações. Em ambientes como hospitais, rodovias e indústrias as informações trafegadas são críticas, emergenciais e necessitam de coleta constante, o que torna essas informações pessoais e sigilosas, necessitando uma maior segurança. Enquanto em ambientes domésticos, tipicamente, os dados transmitidos não apresentam essas características. Porém, outro tipo de cenário seria um ambiente doméstico com o monitoramento de sinais vitais de pessoas idosas ou enfermas, na qual a classificação dos dados ajuda a priorizar os dados de sinais vitais sobre os dados de entretenimento, mantendo o serviço em tempo real e podendo garantir uma maior segurança e privacidade. Logo, esse tipo de serviço de classificação traz benefícios para a disseminação, adequando o funcionamento de serviços em relação aos ambientes no qual operam.

2.2 PRINCÍPIOS DE SEGURANÇA PARA REDE SEM FIO

As redes que utilizam a tecnologia de transmissão sem fio (*wireless*) para comunicação entre os dispositivos possuem características específicas. Ao contrário das rede cabeadas, a transmissão nesse tipo de rede se distingue por não ser guiada, e acessível a qualquer receptor dentro do raio de alcance do ponto de acesso (AP, do inglês *Access Point*) (Ferreira, 2014). Neste cenário, caso não haja nenhuma medida de segurança, o acesso a informação fica imediatamente disponível a quem esteja perto das antenas. A fim de tentar proteger essas informações, mecanismos de segurança devem garantir três atributos na disseminação: confidencialidade, integridade e disponibilidade (Lima et al., 2009). A confidencialidade garante o acesso as informações apenas a quem tem o direito de recebê-las. Enquanto a integridade refere-se à ausência de alterações na informação original. Por fim, a disponibilidade consiste na garantia de acesso a informação em qualquer momento. Juntos, esses atributos garantem a segurança dos dados transmitidos na rede.

Da mesma forma, a IoT baseia-se em tecnologias *wireless*, herdando os mesmos problemas de redes tradicionais no padrão 802.11 e adicionando ainda mais desafios a segurança. Como por exemplo, a falta de recursos computacionais (poder de processamento, armazenamento e restrição de energia) e sendo composta por redes *ad hoc* (ou seja, rede não estruturada), onde a falta de uma autoridade central para gerenciar o tráfego dificulta a garantia de segurança (Sicari et al., 2015). Considerando esses fatores, a segurança vem ganhando principal foco em pesquisas na IoT, a qual ainda permanece desprovida de soluções que atendam a todos os princípios de segurança.

2.3 ATAQUE SYBIL NA IOT

O ataque Sybil se caracteriza pela manipulação de identidades falsas ou roubadas, onde o atacante através de escutas na rede (*sniffers*) pode clonar as identidades ou fabricá-las com base nas identidades fornecidas ao serviço de autenticação. Ao lançar um ataque Sybil em uma rede distribuída, o atacante considera o tipo de comunicação entre os nós legítimos e os maliciosos. Quando o atacante se comunica diretamente com os nós legítimos, chama-se ataque direto. Já se o atacante necessita de uma identidade legítima para se comunicar com os nós legítimos, e a partir de então, entregar dados provenientes do atacante aos nós legítimos, denomina-se ataque indireto (Valarmathi et al., 2016). Ademais, outras características sobre o ataque podem ser destacadas.

Em um sistema distribuído todas identidades Sybil podem participar simultaneamente do ataque ou as identidades são utilizadas isoladamente, enquanto sua maioria permanece em estado ocioso. Essencialmente, a seleção desses dois esquemas depende de quão custoso pode ser para o atacante obter uma identidade no sistema. Quando um atacante consegue facilmente muitas identidades, manter algumas em estado ocioso faz o ataque parecer mais real, considerando que os nós legítimos saem e voltam para o sistema muitas vezes. A Figura 2.1 retrata alguns dos comportamentos Sybil destacados no texto. Nela é possível identificar uma *região Sybil* (à direita) onde os nós Sybil conluiem para o ataque e um nó Sybil detentor de uma identidade legítima (à esquerda) injetando dados do atacante na *região honesta*.

A forma como o atacante autentica uma identidade roubada/fabricada na rede também deve ser destacada. Um adversário pode acionar simultaneamente todas as identidades para alcançar o acesso na rede, ou acioná-las uma por uma em um tempo maior de ataque. Porém, conforme novas identidades são ativadas e maior o tempo de duração do ataque, maior a complexidade para o atacante lidar com os mecanismos de segurança. E por fim, a última

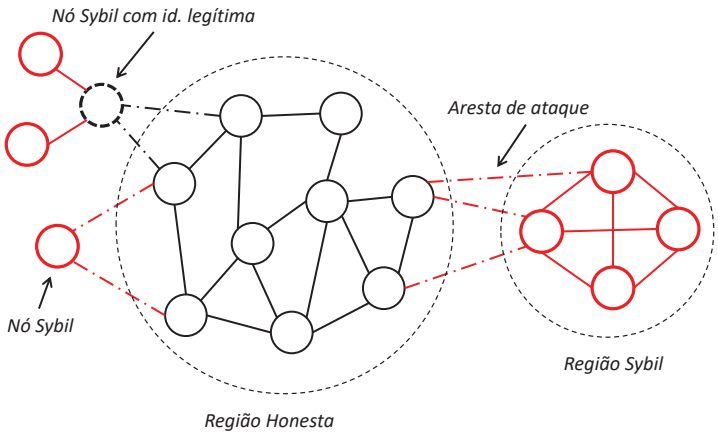


Figura 2.1: Diferentes comportamentos Sybil

característica do ataque é o posicionamento dos nós Sybil em relação ao acesso à rede. O impacto do ataque depende se os nós Sybil podem autenticar ou não na rede. No momento que o atacante possui pelo menos uma identidade real adquirida da rede, denomina-se que o atacante está dentro da rede. Se o mesmo não possuir nenhuma identidade, então assume-se que ele está fora.

2.3.1 Ataque Sybil no RPL

O serviço de roteamento provê uma atividade fundamental dentro das redes de computadores e na IoT da mesma forma. Compete a ele a função de proporcionar que um *host* remetente consiga encaminhar as informações para um *host* destinatário, acontecendo assim a disseminação de dados. Por esta razão, garantir a segurança desse serviço mostra-se relevante para assegura a disseminação. Devido a estrutura da IoT também abranger redes *ad hoc*, protocolos de roteamento especiais para estas redes precisaram ser elaborados para atender suas características. Pensando nessas redes não estruturadas e com baixa taxa de transferência, o protocolo de roteamento RPL (do inglês, *Routing Protocol for Low power and Lossy networks*) foi criado e padronizado como o protocolo de roteamento da IoT (Wallgren et al., 2013). O RPL forma um grafo acíclico direcionado (DAG, do inglês *Direct Acyclic Graph*) com sua fonte no nó *sink* - atuando como um *gateway* e conectando toda a rede 6LowPAN com a internet. As arestas para formar o caminho são calculadas por vários atributos - tais como taxa de transferência, latência e até energia restante - que calculam o custo do link. O RPL divide o DAG em um ou mais DODAGs (do inglês, *Destination Oriented DAGs*) por nó *sink*. A Figura 2.2 exemplifica um DODAG em que cada nó possui um endereço único IPv6.

Especialmente para a IoT, defender o protocolo RPL de ataques significa manter a disseminação de dados. Por essa razão, uma avaliação de desempenho do protocolo RPL foi conduzida em um ambiente com ataque Sybil móvel (Medjek et al., 2017). Os autores investigaram o comportamento do RPL na presença de atacantes Sybil móveis, nomeado pelos autores como SybM (do Inglês, *Sybil-Mobile Attack*). O SybM se caracteriza pela combinação do comportamento Sybil e da mobilidade aleatória dos atacantes, a qual se divide em dois tipos: micro mobilidade e macro mobilidade. Na micro mobilidade os nós se movem dentro do mesmo domínio, enquanto na macro mobilidade o movimento acorre entre domínios, ou seja, entre redes. Contudo, os autores consideram apenas o movimento de micro mobilidade dos atacantes.

No modelo do ataque, os nós Sybil se comunicam diretamente com os nós legítimos, operando independentemente e sem cooperação entre os atacantes. Cada nó da rede é alocado aleatoriamente e manda periodicamente pacotes de dados para o nó borda. Os nós atacantes

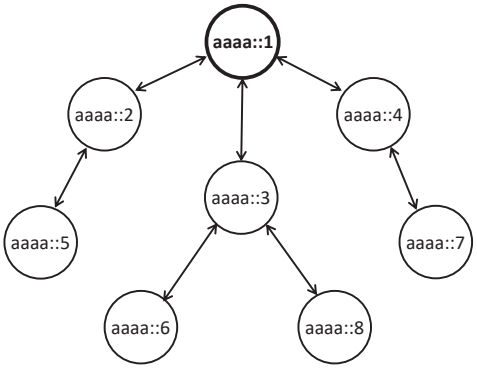


Figura 2.2: Exemplo de um DODAG no protocolo RPL

pausam por um período de tempo, assim como os nós legítimos. Após o período de pausa os nós maliciosos escolhem uma nova localização na vizinhança e se movem fisicamente para o novo local. Ao chegar ao destino, eles repetem o processo de pausa e escolhem uma nova localização. Para realizar a avaliação, os autores criaram o ambiente no simulador Cooja-Contiki-2.7, emulando 50 nós TelosB (uma plataforma de código aberto, utiliza o sistema *TinyOS* e IEEE 802.15.4 para comunicação de rádio), com uma duração de 330s em uma área de 300x300m². Durante os experimentos, quatro cenários foram montados. O primeiro sem atacante e mobilidade, no segundo apenas a mobilidade foi adicionada. Já no terceiro cenário um ataque DIS (do Inglês, *DODAG Information Solicitation*) foi implementado. O ataque consiste de nós Sybil transmitindo mensagens DIS com novos endereços IPv6, correspondendo as novas identidades Sybil. Por fim, no quarto cenário o ataque SybM foi adicionado.

Os resultados encontrados pelos autores demonstram que quando o número de nós Sybil aumenta, a sobrecarga com mensagens de controle aumenta junto. Comparando os ataques DIS e SybM, a sobrecarga no ataque SybM praticamente dobra em relação ao ataque DIS. Conforme o número de atacantes na rede cresce, o valor da sobrecarga do SybM triplica comparado com o DIS. Essa diferença no ataque deve-se ao ambiente estático no ataque DIS, contrastando com o ambiente dinâmico do SybM, no qual confirma que em um ambiente móvel, o ataque Sybil pode ser ainda mais nocivo.

Além disso, observa-se que na presença de atacantes SybM, o consumo de energia aumenta enquanto a taxa de pacotes entregues reduz notavelmente. Este comportamento pode ser atribuído ao crescente número de nós afetados na rede. Consequentemente, o número de mensagens de controle aumenta, crescendo a probabilidade de colisão e retransmissão dos pacotes, levando inevitavelmente ao aumento do custo energético e a redução de pacotes entregues. É importante salientar também que os danos causados por um ataque SybM ultrapassam em 33% os do ataque DIS, em termos de consumo de energia e de taxa de pacotes entregues.

2.3.2 Ataque Sybil na disseminação de dados

Com o propósito de analisar a influência de um Ataque Sybil (AS) na disseminação de conteúdo da IoT, o trabalho (Evangelista et al., 2016a) implementou um cenário e coletou dados da disseminação em meio ao ataque. O cenário para a avaliação consistiu de um ambiente residencial, ondem os nós compreenderam objetos como refrigerador, fogão, televisores e computadores. Os nós agem sequencialmente transmitindo o fluxo de dados para o destino. O fluxo de dados consiste em mensagens de coleta com tamanhos de 256 *bytes*. A escolha da origem e destino dos dados acontece aleatoriamente, sendo eles nós diferentes. O nó origem dissemina os dados para seus vizinhos encaminharem para o destino, repetindo apenas a disseminação quando os dados

em tráfego forem entregues ao destino. Por fim, os atacantes operam com identidades roubadas e fabricadas para solicitar associação na rede, dividindo-se em dois tipos de comportamento: *churn*, o comportamento de entrar e sair várias vezes da rede; ou múltiplas identidades, um comportamento mais estático o qual utiliza duas ou mais identidades para a associação.

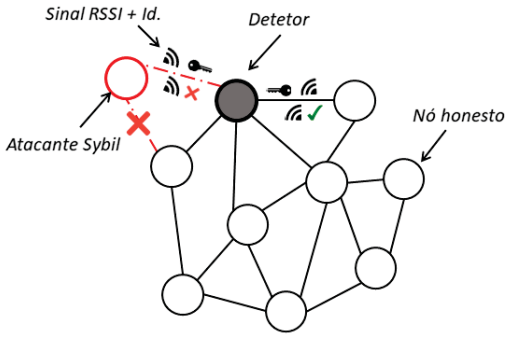
O ambiente da simulação levou em conta a quantidade de nós variando entre 20, 40 e 60, onde nós podiam ser fixos ou móveis. Além disso, 25% dos nós eram fixos e os demais móveis. Eles também emitem uma RSS (do inglês, *Received Signal Strength*) por 100s e se movimentam pela rede de modo aleatório com uma velocidade entre 0.2m/s até 2 m/s. A comunicação foi definida com o padrão IEEE 802.15.4. Os resultados foram obtidos com rodadas de 30 simulações com um intervalo de confiança de 95%, constituindo o número de atacantes como 10% do total.

Os resultados evidenciam o impacto causado por um ataque Sybil na performance da disseminação de conteúdo. Entre os resultados obtidos, não houve uma diferença significativa entre os dois tipos de identidades. Contudo, as identidades fabricadas causaram um aumento no tempo de disseminação, se comparadas com as identidades roubadas. Os resultados demonstram a maior efetividade do ataque em redes com menos dispositivos, onde as taxas na simulação com 20 nós foram consideravelmente inferiores as simulações com o número maior de nós. Também pode-se observar que o comportamento *churn* foi mais danoso, pois causou uma sobrecarga maior e aumentou o custo da disseminação. Isso mostra que o comportamento *churn* reduz a eficiência da disseminação, causando redução na qualidade do serviço.

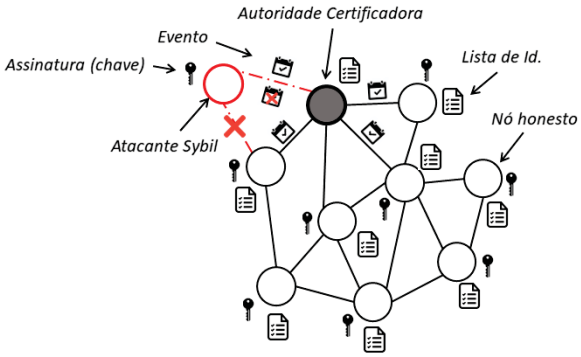
2.3.3 Detecção de ataques Sybil

As técnicas atuais para detecção de ataques Sybil se dividem em três estratégias: baseadas no RSSI (do inglês, *Received Signal Strength Indication*), criptografia e em sistemas de reputação (Evangelista et al., 2016a), como mostra a Figura 2.3. Porém essas técnicas mostram vantagens e desvantagens ao serem aplicadas na IoT (Zhang et al., 2014). Em geral, as técnicas baseadas no RSSI consideram a mobilidade e área de cobertura. Esses parâmetros são avaliados e determinam um comportamento Sybil da rede (Abbas et al., 2013). Mecanismos baseados nessa estratégia apresentam a vantagem de consumirem pouco recurso, tornando-os atrativos para IoT. Contudo, ao mesmo tempo apresentam a desvantagem de terem pouca eficiência na detecção de AS, gerando muitos falsos-positivos.

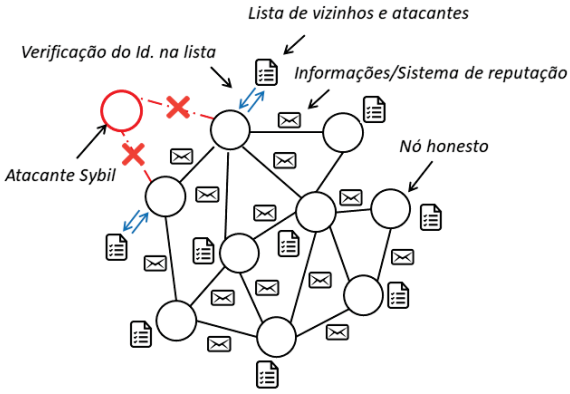
A detecção baseada em criptografia se divide em duas categorias, assimétrica e simétrica. A criptografia assimétrica requer um alto custo computacional para gerar as chaves de segurança, por esse modo são mais indicadas para dispositivos sem restrições de recurso (Lin, 2013). Enquanto a simétrica necessita de uma troca de mensagem segura para garantir o não repúdio, se tornando um gargalo. Por fim, a estratégia baseada em sistemas de reputação mantém uma lista de identidades sobre nós legítimos e atacantes. Então, os nós trocam informação sobre o comportamento de seus vizinhos, gerando um sistema de reputação dentro da rede, onde nós que não cooperam tem sua reputação diminuída (Quercia e Hailes, 2010). As abordagens baseadas neste tipo de estratégia não envolvem o contexto SIoT, nem dados de redes sociais. Como vantagem encontra-se a alta precisão na detecção. Entretanto, as desvantagens somam a sobrecarga de mensagens de controle, a possibilidade de o atacante enganar o sistema de reputação com bom comportamento e a necessidade de treinamento *offline* do mecanismo para identificar comportamentos maliciosos. Baseado nas técnicas apresentadas, existe um *tradeoff* entre segurança e desempenho na escolha de uma solução sobre a outra.



(a) Baseado em RSSI



(b) Criptografia



(c) Relacionamento entre Vizinhos

Figura 2.3: Técnicas de detecção de ataques Sybil

2.4 O CONCEITO CONFIANÇA

A confiança (*trust*) representa um conceito subjetivo para medir a confiabilidade em um indivíduo/sistema para realizar uma tarefa. Mais especificamente, trata-se de uma medida psicológica subjetiva para ajudar um fiduciante (*trustor*) a decidir quando se colocar em uma situação de risco, caso a confiança no fiduciário (*trustee*) esteja mal interpretada e este não complete a tarefa (Truong et al., 2017). Entretanto, mensurar quando deve-se assumir o risco e confiar em uma pessoa ou objeto não se trata de uma tarefa simples, principalmente pela sua subjetividade. Por isso, a confiança não necessariamente requer uma observação do comportamento no passado, diferentemente da confiabilidade no qual consiste de uma confiança verificada por evidencias observadas. Sendo assim, a composição da confiança inclui ambos, comportamento observado e recomendações (Solhaug et al., 2007).

Em um sistema computacional, esses fatores são definidos como confiança direta e indireta. A confiança direta refere-se ao comportamento observável do objeto na rede, se tratando das experiências/interações com outros dispositivos, sendo elas positivas ou negativas. Por outro lado, a confiança indireta representa o comportamento não observável, consistindo de recomendações e/ou reputação. Essas recomendações representam as experiências de outros objetos, compartilhadas na forma de uma opinião (Cho et al., 2015). A fim de determinar valores para confiança direta e indireta, diferentes escalas foram propostas: escala binária, discreta, nominal e valores contínuos (Marsh, 1994). Dentre essas escalas, a binária vem sendo adotada amplamente entre os trabalhos baseados em confiança na IoT.

A confiança possui propriedades chaves consideradas ao criar modelos de confiança, sendo elas: subjetividade, dinamicidade, assimetria, transitividade e dependência do con-

texto (Cho et al., 2015). A subjetividade consiste da natureza inerente na avaliação da confiança, implicando que a confiança subjetiva estima a confiança baseada em evidencias locais, incertas e/ou incompletas. A dinamicidade da confiança está intrínseca em sua natureza. A confiança evolui ao longo do tempo, baseada nos tipos de experiências e interações. A assimetria da confiança aborda como duas entidades não possuem necessariamente o mesmo grau de confiança em relação de uma a outra, sendo uma extensão da reciprocidade das relações. A transitividade reflete uma corrente de confiança entre entidades, a qual pode ser incompleta. A transitividade incompleta assume que em uma corrente onde "A" confia em "B" e "B" confia em "C", não indica que "A" confia em "C", visto que a base de observação não é mesma. A dependência de contexto ajuda a derivar fatores críticos ao estimar a confiança em um determinado contexto. Considerar o contexto para a avaliação da confiança tem sido destacado em pesquisas como essencial para melhor acurácia da confiança (Fernandez-Gago et al., 2017). Logo, considerar o contexto conforme a comunidade em que a pessoa/objeto está inserida garante a aplicação desta propriedade.

Apesar de sua natureza subjetiva, a confiança vem ganhando destaque no desenvolvimento da segurança em contexto heterogêneo, restrito de recurso e não estruturada. O desenvolvimento da confiança e o gerenciamento da reputação em tais ambientes tem o objetivo de atingir alta performance e segurança (Alaba et al., 2017). Além disso, a confiança é usada como uma abordagem suave, identificando dispositivos maliciosos ou usuários egoístas. Vários serviços utilizam a confiança para detectar intrusos, roteamento seguro, gerenciamento de chaves e *controle de acesso* (Cho et al., 2011b).

2.5 SOCIAL INTERNET OF THINGS

A possibilidade de os objetos criarem e gerenciarem relações sociais, abriu novas possibilidades de serviços dentro da IoT, propiciando funções de disseminação de dados, descoberta, seleção e composição de serviços (Atzori et al., 2011, 2012). Com base nessa integração, alguns indicadores da confiança podem ser determinados baseados em interações sociais dentro do ambiente SIoT (Truong et al., 2017). Esclarece-se que a confiança se origina de um aspecto fundamental das relações sociais humanas, e portanto, quando aplicada na SIoT deve-se observar na perspectiva do fiduciário (*trustor*) em correlação a um conjunto de indivíduos. O objetivo da SIoT é trazer as relações humanos para os objetos, de forma que eles possam imita-las. O estabelecimento e gerenciamento dessas relações acontece sem a intervenção humana, gerando uma espécie de "inteligência artificial social" entre os objetos.

De acordo com o modelo SIoT, as relações entre os objetos não são todas idênticas. Os objetos podem estabelecer cinco tipos diferentes de relação (Atzori et al., 2012), como mostra a Figura 2.4. A primeira **relação de objeto parental** (ROP) criada entre objetos produzidos no mesmo período e pelo mesmo fabricante, sendo tipicamente objetos homogêneos. A **relação de objeto de propriedade** (ROPR) é estabelecida entre objetos heterogêneos os quais pertencem ao mesmo dono, isto é, celulares, computadores, *tablets*. Não traz uma abordagem inovadora, porém o conceito é aprimorado com um perfil mais rico de objetos.

A **relação de objeto por localização** (ROL) formada-se entre objetos homogêneos e heterogêneos e que estão sempre no mesmo lugar, como o caso de sensores, atuadores e objetos de grande porte (geladeiras, televisões) em um mesmo ambiente, tais como *smart homes* e *smart city*. Além disso, em certos casos esta relação pode ocorrer entre objetos improváveis de cooperar um com o outro para atingir um objetivo em comum. Mesmo assim, a formação desta relação é útil para criar vários links "curtos" na rede. A **relação de objeto para trabalho** (ROT) começa sempre que objetos colaboram para prover uma aplicação em comum na IoT, como por exemplo

visando atender aplicações de emergência ou telemedicina. Esses dois tipos de relação social estão muito associadas, visto que há uma grande chance de se estabelecerem ao mesmo tempo.

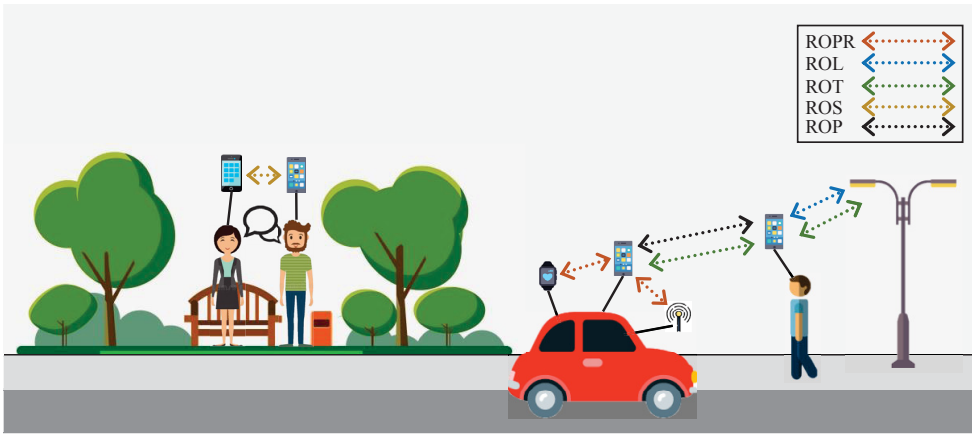


Figura 2.4: Relações na SIoT

Enfim, a **relação de objeto social** (ROS) inicia-se quando os objetos entram em contato, seja esporadicamente ou continuamente, por razões unicamente ligadas aos relacionamentos de seus donos. Da mesma forma que humanos trocam contatos, seja através de telefone, e-mail, entre outras, os objetos nesta relação trocam dados sobre seu perfil social. A ideia principal consiste que os objetos de características similares possam compartilhar boas práticas para resolver problemas comuns, do modo como eles fariam aos "amigos". Logo, espera-se que estas relações sejam responsáveis em gerar um conjunto de regras, interações sociais e serviços para os objetos. Por seguir abordagens inspiradas em relações sociais humanas e modelos de relacionamentos, os objetos agregam o comportamento humano apenas com a finalidade de se obter melhor efetividade nos serviços disponibilizados, com uma clara vantagem de poder estender para a comunidade de objetos os modelos e princípios dos estudos em redes sociais humanas, o qual já obtiveram a comprovada efetividade.

Essas relações desempenham um papel chave na criação de modelos mais escaláveis e seguros para a IoT. Como os trabalhos (Bernal Bernabe et al., 2016; Jayasinghe et al., 2016) utilizaram as relações de sociabilidade dos objetos como fator compositivo para a confiança. Entretanto, o objetivo deste trabalho foca em conferir uma maior importância ao aspecto social na composição do mecanismo, não apenas como fator compositivo. Extraindo os benefícios descritos anteriormente da SIoT para integrar um serviço de controle de acesso mais eficiente.

2.6 COMUNIDADE INTELIGENTE

O conceito de Comunidade Inteligente (*Smart Community*) foi primeiramente descrito em (Li et al., 2011), onde consiste em um ambiente virtual composto por redes domésticas (*smart homes*) localizadas em uma mesma região. Esta rede multi-saltos se interconecta por uma frequência de rádio, seguindo os padrões 802.11 (*wifi*) e a terceira geração da telefonia móvel (3G). Tendo como principal objetivo realizar o contínuo monitoramento da comunidade em vários aspectos, a fim de encontrar ameaças. Quando necessário, *feedbacks* automáticos ou gerados fisicamente por humanos contribuem para melhorarias no sistema. Além disso, suas aplicações vão além de *smart home* e se estende para cuidados com a saúde. Por exemplo, pessoas idosas, com necessidades especiais e crianças podem receber serviços a qualquer momento, por meio do monitoramento com sensores corporais, sistema de vigilância ou pessoas por perto.

No entanto, com o advento da sociabilidade dos objetos (SIoT) houve a necessidade de estender este conceito para se obter uma melhor definição de comunidades inteligentes nos moldes atuais. Para isso, é necessário apresentar como uma comunidade é definida e como denota-se seu comportamento social. A forma tradicional de representação de comunidade consiste da utilização de grafos, onde em um grafo $G(V, E)$, o conjunto V representa os dispositivos na rede e o conjunto E as relações criadas entre os dispositivos.

Em recentes pesquisas como em (Chakraborty et al., 2017), percebe-se que o conceito de comunidade ainda é *ill-defined* (Fortunato, 2010). Um consenso geral sugere que as comunidades possuem estruturas compostas de nós em grupos, no qual dentro desse grupo os nós são altamente conectados e entre os grupos a conexão é menor (Girvan e Newman, 2002). Como um fator agrupador, dentro do contexto de SIoT, a formação desses *clusters* (comunidades) acontece pela similaridade entre os vértices (Fortunato, 2010). Logo, o entendimento do comportamento dos nós proporciona uma melhor visão da formação das comunidades, através das interações dos nós de natureza similares. Tal similaridade vem sendo aplicada em diferentes áreas e tem sido modelada em diferentes formas. Para computar a similaridade de usuários em aplicações *online*, popularmente utilizou-se o coeficiente de correlação de Pearson (Breese et al., 1998). Na qual se obtém através da equação abaixo:

$$Similarity_{rating}(\alpha, \beta) = \frac{\sum_{i \in G}(r_{\alpha,i} - r_{\alpha})(r_{\beta,i} - r_{\beta})}{\sqrt{\sum_{i \in G}(r_{\alpha,i} - r_{\alpha})^2 \sum_{i \in G}(r_{\beta,i} - r_{\beta})^2}} \tag{2.1}$$

Onde, α e β correspondem a dois usuários diferentes e i é qualquer usuário $\in G$, que significa todos os usuários do sistema, exceto os usuários α e β. A função $r(\alpha, i)$ refere-se a taxa avaliada pelo α sobre o usuário i. Em redes sociais, frequentemente calcula-se a similaridade baseada no conhecimento que os vizinhos possuem. Então em (Liben-Nowell e Kleinberg, 2003), os autores definiram a similaridade utilizando a intersecção de dois nós vizinhos, como:

$$Similarity_{neighborhood}(i, j) = |N(i) \cap N(j)| \tag{2.2}$$

A similaridade também foi abordada dentro do particionamento de grafos, onde os vértices formam comunidades com base em suas similaridades. Uma função de modularidade sobre grafos sintéticos pode separar e agrupar os vértices do grafo formando *clusters* (Feng et al., 2007). A Figura 2.5 mostra o grafo resultante com vértices de graus $K_{in} : K_{out} = 15{:}1$. Este grafo contém 124 vértices divididos igualmente em quatro *clusters*. As arestas conectadas entre vértices da comunidade (K_{in}) e as conectadas para fora (K_{out}), são formadas pela probabilidade $P_{out} < P_{in}$.

Entretanto, essas abordagens não envolvem um contexto social, como o encontrado na SIoT. A fim de modelar uma similaridade envolvendo esse contexto social, o coeficiente de similaridade de Jaccard foi utilizado para compor uma similaridade social (Abderrahim et al., 2017). O método estatístico compara à similaridade e a diversidade de uma amostra de conjunto, definido como o tamanho da intersecção, dividida pelo tamanho da união das amostras dos conjuntos. O tipo de dados utilizado nos conjuntos do coeficiente pode variar conforme o contexto estudado, como por exemplo lista de amizade, lista de interesses em comum e a lista de perfis do objeto - referindo-se a informações de fabricante, dono e condições de trabalho.

Uma comunidade inteligente dentro de uma SIoT se forma pela similaridade social dos dispositivos membros da comunidade. Compondo sua inteligência encontram-se aspectos como o gerenciamento das relações na comunidade, o controle de acesso a informação disseminada e

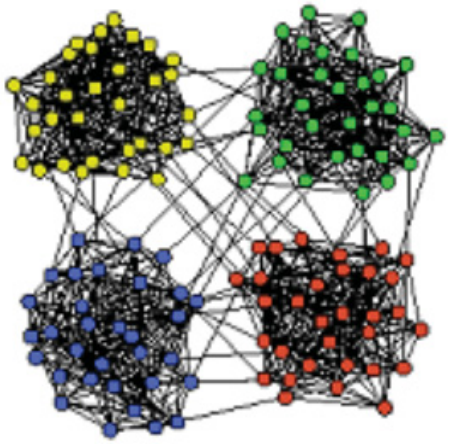


Figura 2.5: Grafo sintético 15:1 (Feng et al., 2007)

em como esse comportamento social pode aprimorar a detecção de nós maliciosos na rede. As comunidades inteligentes criam uma certa estrutura na IoT, onde trabalhos anteriores tratavam o encontro dos dispositivos para troca de dados ao mero acaso (Evangelista et al., 2016b). Agora, a descoberta de serviços e dispositivos passa a ser mais objetiva, pois as comunidades podem ser vistas como representação de determinados serviços e conteúdo.

2.7 RESUMO

Este capítulo expôs os fundamentos sobre Internet das Coisas, apontando exemplos de aplicações, passando por tecnologias possibilitadoras, propostas de arquiteturas para reduzir problema de interoperabilidade dos dispositivos até chegar na disseminação de conteúdo dentro da IoT. Além disso, foram descritos requisitos de segurança em redes sem fio e como eles afetam a IoT. Também foi exposto o modo como atacantes exploram as vulnerabilidades da rede para executar ações maliciosas, a fim de quebrar a confiabilidade, a disponibilidade e a confidencialidade da informação. As técnicas de detecção dos ataques Sybil também foram apresentadas e como a abordagem de confiança pode ajudar a combater esse tipo de ataque. Por fim, destalhou-se o novo paradigma SIoT, discutindo suas definições de relações dos objetos e como ele está mudando a maneira dos objetos se comportarem.

3 ESTADO DA ARTE DOS MODELOS DE CONTROLE DE ACESSO PARA IOT

Este capítulo apresenta os principais trabalhos na literatura que tratam da questão do provimento do controle de acesso na IoT. A Seção 3.1 introduz como o tema tem sido tratado, partindo para as principais técnicas empregadas para adaptar o serviço as característica da IoT; bem como o aspecto social tem atuado na modelagem de novas abordagens. Uma tabela comparativa resume as vantagens e desvantagens das abordagens presentes na literatura. A Seção 3.2 destaca os trabalhos cujo o foco está no gerenciamento da confiança na IoT, e como novas abordagens utilizam a sociabilidade neste serviço.

3.1 O CONTROLE DE ACESSO NA IOT

Uma maneira de lidar com os ataques na rede consiste em efetuar o controle de acesso, que trata em disponibilizar os recursos da rede, como os serviços e dados disseminados, apenas aos usuários ou dispositivos autorizados. Particularmente, as abordagens de controle de acesso têm considerado aspectos como características do objeto, histórico, contexto, e regras criadas pelos administradores. Para facilitar a compreensão do leitor, a Figura 3.1 apresenta na forma de um fluxograma os aspectos e técnicas aplicados pelos sistemas de controle de acesso para IoT encontrados na literatura. Esses aspectos têm sido incorporados as principais técnicas para o controle de acesso existentes como as técnicas baseadas em regras (*Rule Based Access Control* - RBAC), atributo (*Attribute Based Access Control* - ABAC), capacidade (*Capability capability* - CapBAC), risco (*Risk Based Access Control* - RBAC) e confiança (*Trust Based Access Control* - TBAC) (Ouaddah et al., 2017). Além de novas técnicas com criptografia menos complexas e, logo, mais adequadas para os ambientes com restrição de recurso. Como demonstra o mecanismo SA²CI (do inglês, *Sybil Attack Association Control for IoT*), o qual faz um controle de associações para prevenção de atacantes Sybil (Evangelista et al., 2016b). O mecanismo emprega a criptografia de curva elíptica (ECC, *Elliptic Curve Cryptography*) para distribuir, de forma segura, chaves simétricas entre os nós. A fim de assegurar a comprovação da identidade e garantir a irretratabilidade do nós, o mecanismo leva em conta funções não clonáveis (PUF), extraindo informações do *hardware* dos dispositivos e associando com as identidades. Desse modo, o SA²CI mostrou-se capaz de identificar atacantes Sybil e ser eficiente energeticamente.

Entretanto, (Atzori et al., 2011) introduz uma inovadora rede social formada pelos objetos, no qual estes imitam as relações sociais humanas, que pode trazer novas oportunidades para a segurança. Esse novo aspecto social introduziu uma nova visão nas abordagens de controle de acesso. A partir disso, microrregiões começam a ser definidas dentro da IoT, o que possibilita uma melhor delegação de funções e consequentemente um melhor controle no acesso. Com isso, as técnicas trabalhadas no controle de acesso precisaram ser remodeladas para se adequar ao novos aspectos, criando assim, uma diferenciação entre trabalhos que consideram o aspecto social e os que não consideram, tendo como principal diferença, a melhor definição de escopo nos trabalhos sociais. Os trabalhos introduzem conceitos embrionários de comunidades, o que diminui o grande escopo da IoT para microrregiões. Abordagem que permite um melhor gerenciamento de serviços e um melhor controle. A seguir, são apresentados os principais trabalhos propostos baseados em cada aspecto, e são discutidas suas vantagens e limitações quando aplicados ao contexto de SIoT.

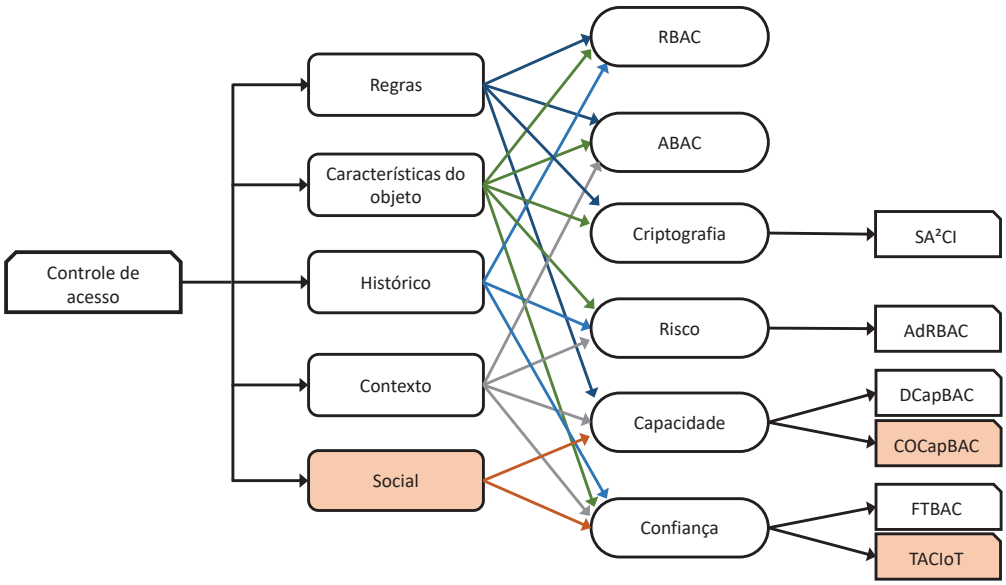


Figura 3.1: Classificação dos aspectos e técnicas para o CA na IoT

3.1.1 Controle de acesso baseado em capacidade

O CapBAC consiste de três serviços fundamentais: avaliação para o acesso, emissão das chaves e validação das chaves. A avaliação para o acesso confere as regras e os parâmetros configurados para regular o acesso. Ao adquirir o acesso através da validação das regras, outro serviço se encarrega na emissão da chave contendo as capacidades do dispositivo na rede; restando ao serviço de validação conferir as capacidades do dispositivo e o tempo de expiração da chave. Os trabalhos baseados em CapBAC se dividem em duas abordagens: centralizada ou distribuída. Na abordagem centralizada, um ponto central se encarrega de todas os serviços fundamentais, concentrando toda a lógica e requisições neste dispositivo da rede. Com a abordagem distribuída, dividem-se os serviços com outros dispositivos na rede, sendo possível que dispositivos com diferentes capacidade computacionais atuam em cada serviço. Em virtude de seu design, a abordagem centralizada mostra sérios problemas em seu modelo (isto é, ponto único de falha e a incompatibilidade com diferentes implementações de segurança), tornando a abordagem distribuída uma opção de maior viabilidade para a IoT.

Entre os trabalhos que usam a abordagem distribuída, (Hernández-Ramos et al., 2016) propuseram o mecanismo DCapBAC (do Inglês, *Distributed Capability-based Access Control Approach*), no qual consiste da evolução da proposta de (Gusmeroli et al., 2013) responsável pela introdução do CapBAC para um cenário IoT em um gerenciamento centralizado. No DCapBAC, os autores estenderam o conceito para atuar em um ambiente distribuído e com restrição de recurso. Feito alcançado e atribuído a implementação de técnicas de criptografia como a PKC (do Inglês, *Public Key Cryptography*) e ECC (do inglês, *Elliptic-Curve Cryptography*), que possibilitaram obter segurança em redes totalmente distribuídas. Contudo, por mais que a solução apresente ferramentas para escalabilidade e interoperabilidade, questões como a granulosidade e consciência do contexto não foram abordadas. Além disso, o DCapBAC possui um foco grande na execução da autorização, enquanto processos como início do *handshake* (abertura do canal de comunicação) para avaliação do acesso e como acontece o processo de geração da chave de capacidade permanecem sem maiores detalhamentos.

O aspecto social veio a ser integrado apenas no *framework* COCapBAC (*Community capability-based access control*), o qual foi modelado orientado a comunidades (Hussein et al.,

2017). O *framework* consiste das seguintes entidades: Servidor de Autorização (SA), Ponto de Decisão de Políticas (PDP), Autoridade Certificadora (AC), Ponto de execução de políticas (PEP) e *Gatekeeper*. O SA possui a responsabilidade de analisar regras e parâmetros e decidir sobre o acesso a rede, enquanto a AC prove asserções (isto é, restrições ou privilégios na rede) para dispositivo requisitante. O PDP e PEP executam funções para auxiliar ao SA e ao *Gatekeeper* respectivamente. No PDP avaliam-se as políticas de aplicações e renderização das chaves de capacidade, enquanto o PEP impõem a execução das políticas do PDP e validade das chaves. Por fim, o *Gatekeeper* encarrega-se de assegurar o comprimentos das regras estabelecidas pelo SA.

Contudo, o sentido de comunidade aplicado no COCapBAC não está relacionado com o paradigma SIoT. As comunidades surgem para a criação de objetivos e missões, políticas de direitos e deveres, bem como facilitar a navegabilidade e a descoberta de serviços. Porém, num ambiente dinâmico onde os objetos constroem relações sociais entre si, este o conceito de comunidade possui desvantagens. Por exemplo, a falta de autonomia dos objetos em aplicar características da comunidade para a avaliação de acesso. Além disso, não é descrito o modo como os aspectos influenciam na criação de novas chaves de acesso.

3.1.2 Controle de acesso baseado em risco

O RiskBAC tem sido outra técnica empregada para o controle de acesso na IoT. Nela, define-se o risco como uma possibilidade de perda ou prejuízo, associado com algum evento que pode ocorrer no futuro. Um exemplo ligado ao risco consiste no vazamento de informações sensíveis por usuários. Logo, o gerenciamento do risco habilita o serviço de controle de acesso a empregar estimativas de risco em cada requisição (Shaikh et al., 2012). Realiza-se a estimativa em cada requisição de acesso dos dispositivos para tomar-se a decisão. Comumente, denota-se a estimativa ao risco através da fórmula: $Q_R = Probabilidade \times Impacto$. Onde a probabilidade representa as chances de um incidente acontecer, enquanto o impacto simboliza a estimativa para os danos causados por esse incidente (Cheng et al., 2007). As abordagens baseadas em RiskBAC são divididas em dois tipos: não adaptativas e adaptativas. O modelo não adaptativo calcula o risco apenas em sua inicialização, enquanto o modelo adaptativo atualiza informações dos aspectos, para o calculo do risco, em tempo real.

Devido a dinamicidade da IoT, modelos adaptativos se adéquam melhor ao contexto da rede. Seguindo essa linha, (Alenezi et al., 2017) trouxeram o modelo adaptativo AdRBAC (do inglês, *Adaptive Risk-Based Access Control*) para o gerenciamento do risco na IoT. Fatores como contexto (lugar e horário), sensibilidade do recurso, gravidade da ação e histórico compõem as entrada no modelo. Esses fatores de risco são então utilizados para estimar um valor de segurança associado com cada requisição. Ainda na estimativa de risco, o modelo prevê um módulo para monitoramento das atividades dos usuários, para entregar maior flexibilidade ao modelo e a estimativa do risco melhor se adaptar ao comportamento do usuário. Compara-se então o valor final do risco com as políticas de segurança para tomar a decisão do acesso.

Por fim, o modelo considera aspectos importantes para um ambiente dinâmico e heterogêneo, mesmo deixando de apresentar uma implementação e avaliação. Entretanto, seu principal problema está em não considerar o aspecto social dos objetos, o que o deixa em desvantagem em um ambiente onde os nós se relacionam entre si, trocando informações importantes enquanto estabelecem as relações sociais. Além da necessidade de uma análise cuidadosa sobre o custo de monitorar as atividades dos usuários em tempo real em uma rede IoT.

3.1.3 Controle de acesso baseado em confiança

Os conceitos de controle de acesso e confiança possuem um grande vínculo, ao considerar que o nível de acesso a informação privadas entre dois dispositivos depende do nível de confiança estabelecido entre os objetos (Conti et al., 2018). Pensando nisso, (Mahalle et al., 2013) propuseram o *framework* FTBAC (do Inglês, *Fuzzy approach to the Trust-based Access Control*), ao utilizar a confiança como ferramenta para tomar decisões de controle de acesso. As propriedades da confiança analisadas constituem a experiência (EX), conhecimento (KN) e recomendação (RC). Após o cálculo de cada propriedade, os resultados são transformados em valores linguísticos compreensíveis para lógica Fuzzy e mapeadas em permissões de acesso. Para avaliar a abordagem, implementou-se o FTBAC no simulador *Network Simulator 2* (NS-2) com a quantidade de nós variando entre 100 e 250 e um total de três rodadas de simulação. Os resultados demonstraram a eficiência energética do *framework*, além de uma melhor flexibilidade e escalabilidade. Porém, o trabalho ainda não engloba uma real implementação e integração com um controle de acesso adequado, deixando métricas como computação de falsos positivos/negativos sem serem avaliadas.

Ao considerar aspectos sociais para o TBAC, destaca-se o sistema TACIoT (*Trust-Aware Access Control System for IoT*) (Bernal Bernabe et al., 2016). Os autores propõem um sistema de controle de acesso à IoT multidimensional com o objetivo de ser leve, flexível e adaptativo. As dimensões se dividem em quatro áreas de avaliação: QoS (*Quality of Service*), segurança, reputação e relações sociais. A dimensão de QoS se refere a avaliação da qualidade do serviço, analisando parâmetros de disponibilidade, taxa de transferência, atraso e interações com êxito. Na dimensão da segurança, controles nas requisições avaliam características do dispositivo requisitante como: mecanismo de autenticação, protocolos de comunicação, confiabilidade, benevolência e a capacidade de processamento do dispositivo. A dimensão da reputação recebe as recomendações de todos os nós da rede, agregando-as para gerar uma reputação universal. O cálculo da reputação acontece pela equação $R^i_j = O^i_j * Cr_i$, onde O^i_j representa a opinião de i relativa a j, e Cr_i a credibilidade da informação recebida.

A dimensão de relação social, baseada no paradigma SIoT, considera que os dispositivos podem ser agrupados em bolhas (*bubbles*) ou comunidades de acordo com sua relação social. As bolhas são ponderadas e devem satisfazer uma escala de importância, partindo como maior nível a bolha pessoal, família, amigos e assim por diante. No caso dos objetos não pertencerem a mesma bolha, características como interesses e amigos em comum podem ser avaliados. Depois de coletar as informações das quatro dimensões, o sistema utiliza um *fuzzificador singleton* para gerar um valor final nítido e uma sequências de regras definem se o acesso é concedido. Dessa maneira, mesmo que o trabalho tenha considerado a dimensão social na solução, alguns pontos permanecem indeterminados como o caso do gerenciador de contexto, como também o processo de formação das comunidades entre os objetos carece de um maior detalhamento, adicionando como os aspectos de interesses em comum e amizade compõem a avaliação da confiança.

3.2 GERENCIAMENTO DA CONFIANÇA NA INTERNET DAS COISAS

A literatura fornece uma ampla variedade de trabalhos focados no gerenciamento da confiança para a Internet das Coisas (Yan et al., 2014). Por esse motivo, destacam-se algumas das propostas mais relevantes, focando no gerenciamento da confiança em ambientes distribuídos ou para a detecção de nós maliciosos na rede. Apesar de não configurarem em um contexto de controle de acesso, esses trabalhos apresentam características e aspectos importantes na construção da confiança, os quais podem integrar posteriormente trabalhos focados no serviço de

controle de acesso. Logo, os aspectos subjetivos considerados nestas propostas contribuem para que mais segurança possa ser alcançada dentro da IoT.

Com a ideia de trazer mais subjetividade em sua avaliação, (Son et al., 2017) fundamentaram sua solução na psicologia, ao considerar estereótipos não pessoais. O trabalho alia o gerenciamento da confiança aos estereótipos junto com um histórico de interações. Os esteriótipos contribuem ao fornecer ao gerenciador da confiança valores iniciais em situações onde não existe contato prévio. A avaliação da confiança começa quando os dispositivos se encontram e o esquema captura os estereótipos da situação atual. Entre os estereótipos envolvidos, estão o tipo do dispositivo (categoria, fabricante, modelo), o papel desempenhado pelo dispositivo (tarefas a desempenhar) e o ambiente. Uma vez extraídos os estereótipos da situação atual, o esquema procura no histórico situações que ocorreram com o mesmo tipo de dispositivo. A partir dessas informações, um algoritmo de árvore de aprendizagem M5 analisa as associações entre as situações. A Figura 3.2 mostra uma árvore treinada, onde os nós intermediários e as arestas representam características situacionais. Ao utilizar a situação atual como entrada, o algoritmo faz as associações até chegar ao modelo linear correspondente. Este modelo é então utilizado como base histórica para calcular a confiança pessoal no próximo passo.

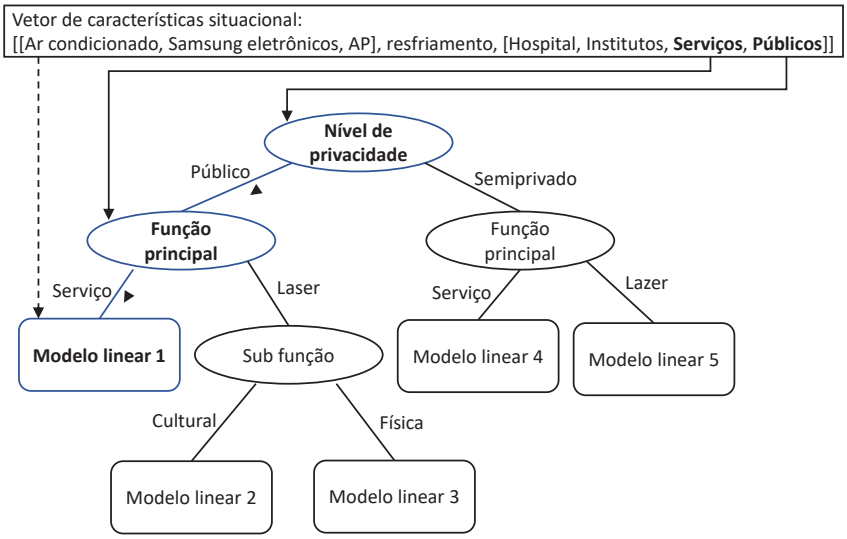


Figura 3.2: Traduzido: Instância da árvore de aprendizagem M5 (Son et al., 2017)

Para conciliar valores pessoais e não pessoais, a fim de formar um único valor, os autores aplicaram a Lógica Subjetiva (LS) (Jøsang, 1997) de forma a entregar dinamicidade. Para isso, eles estenderam a LS de forma que o valor final represente a convicção de que determinado dispositivo terá um comportamento positivo, observada na Equação 3.1a. Na equação, x representa um usuário na rede, y um dispositivo alvo que será avaliado e $P(w_y^x)$ a confiança do usuário que o dispositivo alvo terá um comportamento positivo. As variáveis v_y^x, u_y^x e a_y^x representam respectivamente a confiança pessoal, incerteza e confiança não pessoal. O estereótipo coletado do dispositivo alvo incorpora-se no valor da confiança não pessoal, como mostra a Equação 3.1b. Enquanto r_y^x reflete os interações positivas com y.

$$P(w_y^x) = r_y^x \times u_y^x \times v_y^x + u_y^x \times a_y^x \quad (3.1a) \qquad a_y^x = \frac{\sum_{p \in R_x} c_p t_y^p}{\sum_{p \in R_x} c_p} \quad (3.1b)$$

Na Equação 3.1b, p representa outro usuário dentro do conjunto R_x e c_p descreve a convicção na confiança "estereótipal" t_y^p em y. Assim que estipulada a confiança em um determinado dispositivo, um usuário pode decidir se interage com ele. Se o usuário escolhe

interagir, o esquema atualiza o número de interações positivas. Logo, (Son et al., 2017) apresentaram aspectos interessantes como a avaliação por estereótipo, a qual permite obter um valor inicial para confiança quando não existe evidências. Entretanto, para o esquema funcionar corretamente a árvore M5 deve ser treinada previamente. Além do não envolver a automação entre os objetos, deixando muito das decisões para o usuário humano resolver. O que não se adequada a um ambiente SIoT, onde relações e decisões são tomadas autonomamente.

Ademais, um mecanismo distribuído para detecção de intrusão baseado em confiança foi proposto em (Khan e Herrmann, 2017). A solução combate ataques que tentam omitir comunicação crucial entre os nós. Ao se concentrar em ataques no protocolo RPL, especificamente os ataques: *Selective-Forwarding*, *Sinkhole Attack*, *Version Number Attack*. Para identificar os nós maliciosos, o mecanismo também computa a confiança através da LS. Em contraste, os autores adicionaram a constante k, com valores variando entre 1 e 2 para determinar quão rápido se constrói a confiança em outro dispositivo. A computação da confiança na solução acontece através da *confiança direta* e *confiança indireta*. Na confiança direta, um dispositivo avaliador verifica o comportamento do outro dispositivo avaliado, checando informações como encaminhamento, ranque e número de versão; todos relativos ao protocolo RPL. A confiança indireta neste trabalho representa uma reputação, onde uma entidade dentro da rede concentra todas as opiniões. Para isso, todos os nós da rede enviam suas informações da confiança direta em relação a seus vizinhos para o nó *sink* (nó responsável em conectar a rede 6LowPAN com a Internet). Então o nó *sink*, ao utilizar uma operação de agregação, faz a reputação de cada nó na rede.

Os autores ainda desenvolveram três algoritmos diferentes para gerenciar a reputação. O primeiro algoritmo chamado NBTD (do Inglês, *Network Based Trust Dissemination*), centraliza a computação da confiança, onde o nó da borda executa uma função de agregação para gerar a reputação. Calcula-se o valor da confiança periodicamente, baseado nas entradas de confiança recebidas de outros nós. O segundo algoritmo CNTD (do Inglês, *Clustered Neighbor Based Trust Dissemination*) calcula a confiança de uma maneira distribuída. O algoritmo divide a DODAG em vários *clusters* e dentro de cada *clusters* criado, um *cluster-head* (líder) coleta os valores da confiança e calcula a reputação dos nós do *cluster* com a função de agregação. Por fim, o algoritmo TTD (do Inglês, *Tree Based Trust Dissemination*) opera da mesma forma que o CNTD, entretanto o nível de vigilância dos nós é reduzido, no qual o TTD apenas vigia os nós pais dentro da árvore criada pelo protocolo RPL, ao deixar de vigiar os filhos em ordem de reduzir a sobrecarga de mensagens de controle na rede.

Os resultados foram gerados em cima da avaliação dos três algoritmos e análise de parâmetros como falsos-positivos, falsos-negativos, número de intrusos detectados e número de mensagens de controle enviadas. Com base nos resultados, os autores concluíram que cada algoritmo deve ser usado para diferentes situações. Os algoritmos NBTD e CNTD têm uma maior eficiência para detectar intrusos e são indicados para uma rede maior. Porém, os mesmos acabam causando uma maior sobrecarga na rede, devido ao grande número de dados de controle transferidos. Além disso, o algoritmo NBTD trata de uma abordagem centralizada, que gera problemas como ponto único de falha, sobrecarga do nó *sink* e escalabilidade. Por outro lado, o algoritmo TTD mantém uma baixa sobrecarga na rede, mas ao custo de uma baixa eficiência na detecção. Outro ponto a ser considerado refere-se a falta de informação sobre a mobilidade dos nós na rede e sobre a entrada e a saída contínua de nós legítimos. Essas questões podem afetar os resultados de falsos-positivos/negativos e principalmente a sobrecarga na rede.

3.2.1 Gerenciamento da confiança na Social Internet of Things

A introdução da *Social Internet of Things* (SIoT) por Atzori (Atzori et al., 2011), trouxe uma nova perspectiva para a modelagem da confiança na IoT. Com isso, novos trabalhos propuseram um gerenciamento da confiança influenciado pelo novo paradigma. Seguindo essa linha, um esquema para o gerenciamento da confiança na SIoT baseado no comportamento dos objetos foi proposto, com o objetivo de estabelecer uma comunicação confiável entre objetos (Kowshalya e Valarmathi, 2017). No esquema, os objetos estimam a confiança em outros objetos baseados nas próprias experiências (confiança direta) e experiências compartilhadas de outros objetos (confiança indireta). As propriedades aplicadas na construção da confiança incluem a centralidade, a energia, o interesse comunitário, a cooperatividade, e a pontuação pelo serviço.

Para computar a confiança, calcula-se cada propriedade individualmente junto com a confiança direta e indireta. Na composição final, todos os valores são normalizados e ponderados de acordo com sua importância. A influência social no esquema encontra-se na cooperatividade e no interesse comunitário. A cooperatividade pode ser calculada através da Equação 3.2.

$$Cooperatividade_{ij} = \frac{frinds(i) \cap friends(j)}{friends(i) \cup friends(j)} \tag{3.2}$$

Partindo do princípio que objetos com amigos em comum tendem a ser cooperativos, o trabalho utilizou para prever a cooperatividade entre objetos os laços sociais, no qual cada objeto processa uma lista de amigos prováveis para cooperação. Seguindo a mesma lógica, o interesse comunitário tende a ser maior em objetos com laço, podendo ser calculada pela Equação 3.3.

$$Interesse_{ij} = \frac{comunidade(i) \cap comunidade(j)}{comunidade(i) \cup comunidade(j)} \tag{3.3}$$

Para os autores, objetos com interesse em comum supostamente tendem a ter uma maior interação entre si, aumentando a performance da aplicação. As listas com os interesses em comum dos objetos caracterizam um início de formação de comunidades. Contudo, esse conceito não foi desenvolvido no trabalho, ficando em um estágio inicial e contribuindo apenas como propriedade da confiança. O trabalho ainda avaliou a confiabilidade do gerenciamento em meio a um ataque *Selective Forwards On Off*. O ataque baseia-se em alterar o estado do dispositivo de ligado (*On*) para desligado (*Off*) e vice-versa. Com esse comportamento, o atacante provoca uma contínua interrupção na rede (Perrone e Nelson, 2006). Os resultados obtidos pelos autores demonstram que o esquema mantém confiabilidade em meio ao ataque, assim como melhores desempenhos para a aplicação. Porém, o método baseia-se em servidores centralizados, não sendo escalável conforme a rede de dispositivos cresce, além de gerar pontos únicos de falha na rede.

Um trabalho recente apresenta um forte contexto social para o gerenciamento da confiança. O sistema CTMOS-SIOT (do inglês, *Context-based Trust Managment System for the Social Internet of Things*), consiste em um modelo centralizado para gerenciamento da confiança, no qual todas as informações são repassadas para uma autoridade central (Abderrahim et al., 2017). Ele contém três componentes: objeto, servidor de serviço e o servidor do gerenciamento da confiança. Os objetos formam a rede e apresentam diferentes capacidades. O servidor de serviço possui a responsabilidade de descobrir serviços na rede e disponibilizar a outros objetos. O servidor do gerenciamento da confiança recebe informações das entidades na rede e com base nisso calcula a confiança contextual e a reputação. Define-se os valores iniciais da confiança com

base nos tipos de relacionamentos estabelecidos, sendo esses relacionamentos aqueles definidos na SIoT (Atzori et al., 2012).

Para atualização da confiança o modelo segue três passos. No primeiro passo os autores tentam prever o comportamento dos objetos por meio de uma árvore de decisão. A árvore de decisão ajuda o modelo a encontrar a relação entre os atributos e similaridade. No segundo passo, calcula-se a similaridade social, utilizando o coeficiente de Jaccard e conjuntos de amizades, interesses em comum e perfil do objeto. Depois de calculada, envia-se a similaridade social para o servidor de gerenciamento da confiança. Como último passo, o servidor de gerenciamento atribui uma credibilidade para cada nó, utilizando a similaridade entre as duas partes envolvidas. Um mecanismo no qual os objetos avaliam suas transações também foi implementado para detectar comportamentos maliciosos. Os resultados mostram que o sistema é capaz de retornar objetos confiáveis para cada contexto e serviço, sem a necessidade de histórico do comportamento. No entanto, por se basear em um modelo centralizado, inevitavelmente compromete-se a escalabilidade do sistema, além do sistema apresentar problema com um ponto único de falha, afetando a segurança e o desempenho.

3.3 DISCUSSÃO

Como visto nas seções anteriores, a literatura oferece uma vasta gama de trabalhos focando o serviço de controle de acesso para rede IoT. Isso mostra que o problema existe e ainda segue sem uma resposta definitiva, enfrentando grandes desafios para aplicar os protocolos de segurança em todas os domínios de aplicação da IoT. Principalmente os ambientes restritos da IoT impossibilitam o emprego de técnicas como criptografias complexas. Ao buscar modos para contornar o problema, as pesquisas trazem conceitos subjetivos como a confiança e o risco. Os resultados demonstram serem promissores ao analisar o tráfego e o comportamento dos dispositivos requisitantes. Em especial, o CapBAC agrega vários conceitos da subjetividade dos objetos como a formação de comunidade e confiança entre entidades. Contudo, a complexidade da autoridade certificadora na solução demanda um dispositivo com grande poder de processamento na rede para analisar as requisições e tomar decisão.

Em contrapartida, o gerenciamento da confiança vem sendo considerado fundamental para atingir maiores níveis segurança. Ele proporciona maior flexibilidade que mecanismos de segurança tradicionais, facilitando a tomada de decisão. Porém, existem dois principais desafios ao integrar a confiança na IoT: interoperabilidade e dinamicidade. A interoperabilidade está diretamente ligada com a heterogeneidade dos dispositivos na IoT, onde diferentes dispositivos possuirão diferentes gerenciadores da confiança coexistindo. A dinamicidade vem dos diferentes contextos e mudanças em um ambientes IoT, em que os gerenciadores precisam atender a estas mudanças e adaptar as novas características do meio.

Além disso, a Tabela 3.1 sumariza os requisitos importantes ao escopo do controle de acesso na IoT. Observa-se que as abordagem não atendem a todos os requisitos destacados ou as implementam parcialmente. Como o caso da COCapBAC e TACIoT, onde o aspecto social não representa uma rede que possui a formação de relações sociais autonomamente como a SIoT; ou sua abordagem não é totalmente distribuída. Logo, existe a necessidade de novas abordagens que venham preencher todas as lacunas deixadas pelos trabalhos anteriores. Neste contexto, **um controle de acesso distribuído, flexível e dinâmico que possa unir o gerenciamento da confiança com os relacionamentos sociais dos objetos e uma percepção de comunidade** surge como uma alternativa, detalhada nos próximos capítulos e avaliada neste estudo.

Tabela 3.1: Requisitos para o controle de acesso na IoT vs. técnicas aplicadas

Técnicas	**Trabalhos**	**Distribuído**	**Escalável**	**Flexível**	**Dinâmico**	**Contexto**	**Social**
Criptografia	SA²CI	✓	✓	✓	✓		
Chave de capacidade	DCapBAC	✓	✓	✓			
	COCapBAC	✓	✓	✓	✓		✓*
Quantificação do Risco	AdRBAC	✓	✓	✓	✓	✓	
Confiança	FTBAC		✓	✓			
	TACIoT			✓	✓	✓	✓
	CTMOS-SIOT			✓	✓	✓	✓

3.4 RESUMO

Este capítulo apresentou uma discussão sobre os trabalhos encontrados na literatura sobre o controle de acesso na IoT. Primeiramente introduziu-se os trabalhos que abordam o serviço com as principais técnicas: CapBAC, RiskBAC e o TBAC. Criptografias flexíveis e funções não clonáveis (PUF) também foram apresentadas como ferramentas para garantir a privacidade. Dentre os trabalhos descritos, ressaltou-se a consideração do aspecto social para o modelagem das técnicas anteriormente ilustradas. Em seguida, apresentou-se como o gerenciamento da confiança é abordado dentro do contexto de redes *ad hoc*, heterogêneas e com restrição de recurso, assim como modela-se o gerenciamento da confiança para redes SIoT.

4 ELECTRON - UM CONTROLE DE ACESSO CONTRA ATAQUE SYBIL

Este capítulo detalha o mecanismo ELECTRON (*acc***E***ss contro***L** *driv***E***n on* **C***ommunity and social* **TR***ust* **O***f thi***N***gs*) baseado na confiança social e em contexto de comunidades para um controle de acesso resiliente a ataques Sybil (AS) na IoT. A Seção 4.1 apresenta uma visão geral do mecanismo proposto, ao abordar suas características e onde ele atua. A Subseção 4.1.1 descreve o modelo da rede IoT, e os serviços presentes. A Subseção 4.1.2 discorre sobre o comportamento do ataque Sybil dentro da rede anteriormente descrita. A Seção 4.2 exibe a arquitetura do mecanismo, ao detalhar como seus componentes atuam para extrair informações da rede e qual o fluxo dessa informação dentro da arquitetura. Em seguida, explicam-se, dentro de seus respectivos módulos, a definição das comunidades dentro do mecanismo, a construção da confiança social, a identificação dos ataques e a tomada de decisão do acesso.

4.1 VISÃO GERAL

O mecanismo atua como um *middleware* na rede IoT de modo auxiliar na segurança na disseminação e no compartilhamento de dados na IoT contra a presença de ataques de personificação. O mecanismo, chamado ELECTRON, fornece um serviço de controle de acesso a fim de impedir que nós atacantes acessem a rede. Ao aliar um modelo de gerenciamento da confiança às relações definidas segundo o paradigma SIoT construídas autonomamente pelos dispositivos e ao definir a noção de comunidades considerando seu contexto e os vínculos sociais, aprimora-se o serviço de controle de acesso impedindo que atacantes Sybil tenham acesso ao dados e lancem outros ataques que podem prejudicar a privacidade e disponibilidade dos mesmos. As comunidades criadas dentro da rede julgam fatores como interesses em comum e amizade, visto que dispositivos com os mesmos interesses e laços de amizade tendem a ser mais confiáveis e assim, enfraquecem a confiança em dispositivos desconhecidos. Isto acontece pois estes dispositivos possuem maior dificuldade para se relacionar na rede, auxiliando na identificação de possíveis atacantes.

O tipo de arquitetura para o mecanismo é um detalhe importante, e que traz vários tipos de discussões. Escolher entre uma abordagem centralizada ou distribuída, envolve diversos fatores, tais como escalabilidade e recurso computacional. Pensando nisso, deve-se analisar as vantagens e desvantagens para o modelo melhor se adequar às características da IoT. De um lado, centralizar toda a lógica em apenas um único dispositivo na rede (nó) pode não refletir a realidade, pois não existe a garantia de que um nó com recursos suficientes estará na rede. Contrariamente, em um modelo descentralizado cada nó deve armazenar e processar informações, resultando em uma redução na vida útil dos nós. Logo, pensando em uma melhor adaptação do modelo na IoT, este trabalho adota uma estratégia híbrida, onde a composição da confiança e a análise social distribuem-se pelos nós com mais recursos computacionais, enquanto os nós com restrição coletam dados dos vizinhos e repassam para o nó mais potente, reunindo os benefícios dos dois modelos.

4.1.1 Modelo da rede

O modelo da rede considera características, dentre elas a topologia composta por partes estruturadas e não estruturadas, onde os dispositivos (nós) cooperam no encaminhamento dos dados. A rede possui nós heterogêneos e cuja mobilidade pode ser diversa, isto é, estática ou

móvel. O conjunto N representa todos os nós que compõem a rede, sendo $N = \{n_1, n_2, ..., n_n\}$. A Figura 4.1 ilustra a representação deste modelo, onde os nós que compõem a rede IoT dividem-se em duas categorias: N_{man} (destacados na figura) e N_{sub}, no qual $N_{man} \subseteq N$, $N_{sub} \subseteq N$ e $N_{man} \cup N_{sub} = N$. Os nós dentro do conjunto N_{man} formam uma rede lógica distribuída, a fim de trocarem informações da confiança e relações sociais. Dessa forma, o mecanismo garante a escalabilidade da rede dividindo o gerenciamento da confiança social entre os nós no conjunto N_{man}, além de poder aumentar a capacidade de gestão apenas adicionando novos dispositivos para o conjunto de gerenciamento.

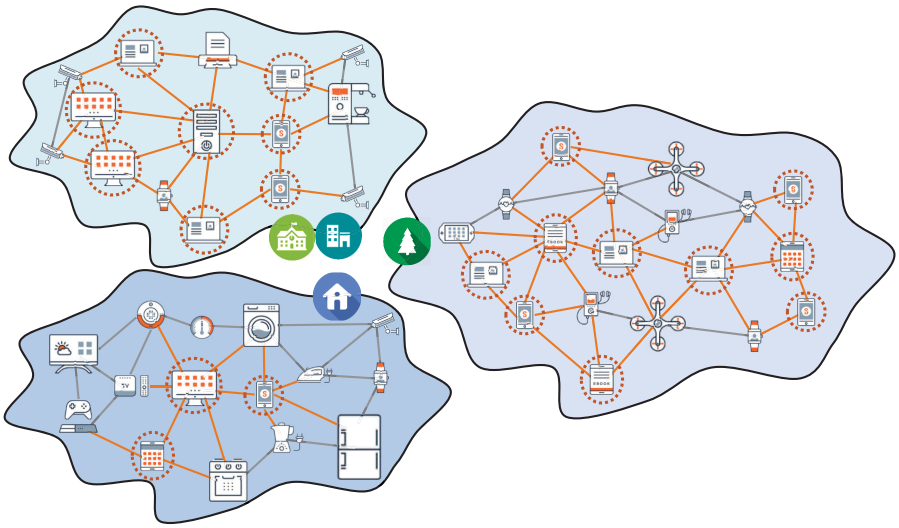


Figura 4.1: Modelo da rede IoT

A outra categoria de nós compreende os dispositivos no conjunto N_{sub}. Como característica esse grupo contém dispositivos com restrição de recursos, tanto de energia como de armazenamento e processamento. Por esses fatores, o conjunto N_{sub} está subordinado ao conjunto N_{man}, tendo apenas como função coletar os dados a sua volta e transmitir para o nó N_{man} mais próximo. Esta abordagem visa à adequação do mecanismo a heterogeneidade da IoT, onde nem todos dispositivos têm recursos para lidar com a complexidade do mecanismo. Dessa forma, os nós dentro do conjunto N_{man} formam um serviço lógico, provendo o controle de acesso para rede, com informações coletadas de todos os nós.

4.1.2 Modelo do ataque

A disseminação de conteúdo está sujeita a diferentes tipos de ameaças. Entre essas se encontra o AS, no qual o atacante personifica identidades, roubando identidades reais ou fabricando identidades falsas, para se passar por um nó legítimo. Ao alcançar acesso a rede, o atacante passa a ter acesso aos dados disseminados e pode lançar outros tipos de ataque, prejudicando requisitos de segurança como privacidade, confidencialidade e integridade dos dados, assim como também afetar a desempenho e o consumo de recurso em redes como a IoT. Com isso, este trabalho busca criar um mecanismo resiliente a AS. Neste trabalho, considera-se que o ataque tem como suas principais características: mobilidade diversa, rede *ad hoc* e que os dispositivos *Sybils* atuam de maneira individual, sem cooperação para formação de regiões Sybil, como explica a subseção 2.3.

O atacante pode lançar um ataque Sybil com identidades roubadas (Id_r) ou fabricadas (Id_f). O conjunto Id_r compreende identidades roubadas de nós legítimos pelo atacante, se tornando um maior desafio para o mecanismo identificar o seu comportamento Sybil, dado

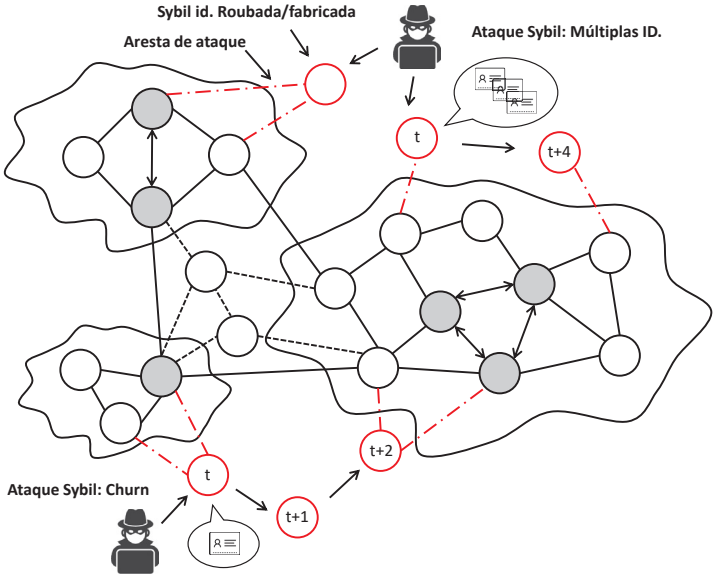


Figura 4.2: Ataque Sybil

que essas identidades possuem associações com outros dispositivos. Enquanto o conjunto Id_f possui identidades fabricadas as quais podem ser baseadas nas identidades roubadas, contudo sem possuir prévias autenticações na rede. O uso de identidades fabricadas pode não representar grande desafio, porém se o atacante fabricar muitas identidades e tentar por força bruta o acesso, ele impõem aos dispositivos da rede um grande desgaste na comunicação e uma possível falha na autenticação ao conquistar o acesso. O comportamento dos atacantes pode variar entre *churn* e múltiplas identidades (MI), como mostra a Figura 4.2. No comportamento *churn* o atacante possui apenas uma identidade, porém tenta várias associações com diferentes nós em um curto espaço de tempo. Entretanto, o comportamento MI possui várias identidades e uma movimentação menor ao utilizar suas muitas identidades para forçar a associação.

4.2 ARQUITETURA

O mecanismo ELECTRON opera de modo restrito ou não restrito, variando conforme o perfil do dispositivo (N_{man}, N_{sub}). A arquitetura exposta na Figura 4.3 representa os componentes do mecanismo compondo os nós N_{man}, pois este concentra a maior parte da lógica do mecanismo. Devido aos recursos limitados, os nós N_{sub} apenas coletam informações a sua volta e encaminham ao nó N_{man} mais próximo. Este, por sua vez, processa todas informações recebidas e decide quanto ao acesso à rede, de maneira a economizar recursos dos nós N_{sub}.

4.2.1 Módulo social

O módulo social compreende todas as funções referentes aos relacionamentos dos objetos até a noção de comunidade dentro do mecanismo. O módulo armazena informações sobre amizades e interesses em comum entre os dispositivos na rede, tanto do nó N_{man}, que o módulo faz parte, como dos nós N_{sub} subordinados. A amizade pode ser definida a partir de um número de interações entre dois dispositivos ou pela relação de amizade entre seus donos, assim como os interesses definidos pelo usuário ou extraído de seu comportamento. Essas informações são utilizadas no cálculo da confiança e para gerar a similaridade dos componentes da comunidade.

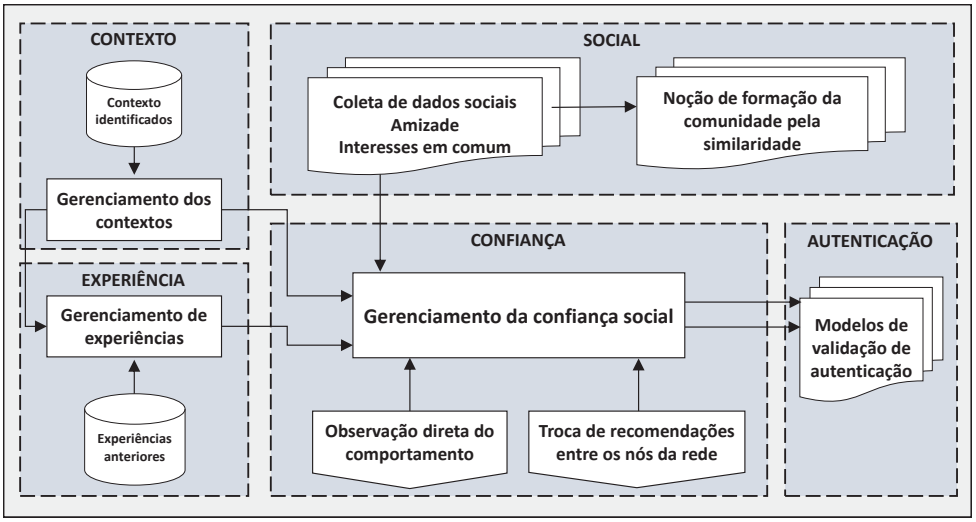


Figura 4.3: Arquitetura do ELECTRON

Ao longo da pesquisa bibliográfica, foi identificada uma especialização dentro da Internet das Coisas, onde os objetos começam a ser discernidos pelo comportamento social. Por meio do paradigma *Social Internet of Things*, os objetos passam a imitar o comportamento social de humanos e criar autonomamente relacionamentos entre si. Por se basearem no comportamento humano, espera-se que os objetos formem comunidades dentro da rede SIoT. Os objetos dentro dessa comunidade devem desfrutar de vantagens como fácil descoberta/fornecimento de serviços e conteúdo. Além de contribuir para segurança no controle de acesso à rede, pois amparado nos relacionamentos sociais espera-se que a confiança seja amplificada entre os objetos participantes.

As comunidades "especiais" (denominadas comunidades inteligentes) têm um papel importante no comportamento social dos objetos. Nesta seção apresentam-se suas especificações e formação. Devido a suas características, as comunidades são representadas através de grafos no qual considera-se a similaridade entre os nós da rede, formando um grafo de similaridade. Sendo G o grafo que representa toda a rede, V(G) o conjunto de vértices do grafo equivalente aos nós da rede e A(G) o conjunto de arestas representando a similaridade entre dois vértices, tal que $ij \in A(G) \Leftrightarrow S(i,j) > Similarity_{threshold}$. Dessa forma, denota-se a comunidade da seguinte forma:

$$C = \forall i, j \in V(G) \mid S(i,j) > Similarity_{threshold} \tag{4.1}$$

Onde $S(i,j)$ compreende uma função para calcular a similaridade no conjunto de vértices que pertencem a comunidade C, tal que sua similaridade seja maior que o limite $Similarity_{threshold}$. Este valor acima do limite indica que há uma forte similaridade entre tais vértices e, portanto, uma comunidade. Toda a arquitetura da rede se mantém dentro de uma comunidade, com a diferença que dentro da comunidade existe uma maior relação dos dispositivos. Esse comportamento reflete o maior nível de confiança entre os objetos dentro da comunidade, movidos principalmente pelas relações sociais - amizades e interesses em comum. A Figura 4.4 retrata uma rede SIoT composta por nós N_{man} e N_{sub}, nas cores cinza e branco, respectivamente, onde há três comunidades diferentes a partir da similaridade dos objetos. Na figura, alguns nós já possuem conexões estabelecidas - retratados por links contínuos e links direcionados para demonstrar a comunicação entre nós N_{man}, em outras inicia-se a comunicação para avaliação de acesso a rede - links tracejados.

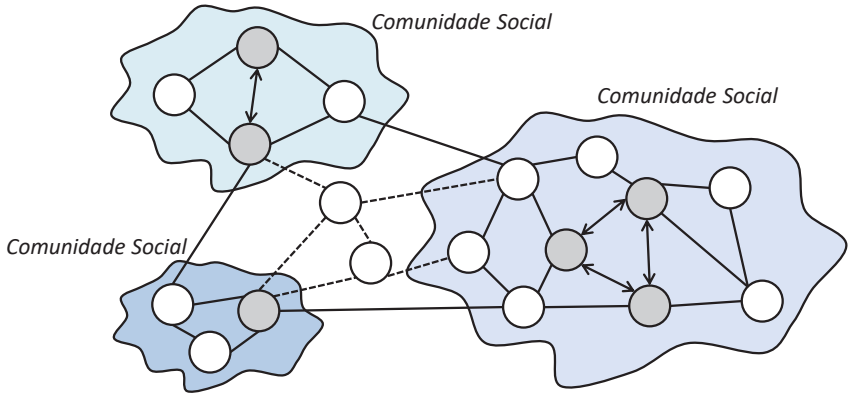


Figura 4.4: Comunidades em uma rede SIoT

Na Equação 4.1, $S(i, j)$ significa a similaridade social obtida reunindo informações sociais e comportamento dos usuários e objetos. Neste trabalho, essas informações sociais representam *a amizade e os interesses em comum* como métricas para o cálculo da similaridade social, de acordo com sua importância. Dada pela seguinte equação:

$$S(i, j) = Sim^{A}(i, j) * \varphi_A + Sim^{CI}(i, j) * \varphi_{CI} \tag{4.2}$$

Denota-se o peso da importância de cada métrica através da variável φ, sendo que $\varphi_A + \varphi_{CI} = 1$. A tupla $<A, CI>$ representa as informações sociais dos dispositivos, correspondendo respectivamente ao conjunto de amizades (A) e ao conjunto de interesses em comum (CI). As métricas são obtidas a partir do coeficiente de similaridade de Jaccard (Abderrahim et al., 2017), descritas a seguir:

Conjunto de Amizades (A): a amizade denota uma poderosa relação social, capaz de afetar recomendações, e está ligada intimidade entre as entidades. Computa-se a similaridade entre os conjuntos de amizade ($Sim^{A}(i, j)$) pela Equação 4.3, onde A_i e A_j representam as listas de amigos de i e j.

$$Sim^{A}(i, j) = \frac{|A_i \cap A_j|}{|A_i \cup A_j|} \tag{4.3}$$

Conjunto de Interesse em Comum (CI): usuários em uma mesma comunidade compartilham interesses similares. Logo, eles são mais prováveis a ter conhecimentos e padrões comuns para um serviço provido pelo mesmo dispositivo. Da mesma forma, computa-se a similaridade entre dois conjuntos de intesses em comum ($Sim^{CI}(i, j)$) pela Equação 4.4, onde CI_i e CI_j consistem nas listas de interesse em comum dos dispositivos i ej.

$$Sim^{CI}(i, j) = \frac{|CI_i \cap CI_j|}{|CI_i \cup CI_j|} \tag{4.4}$$

4.2.2 Módulo confiança

Um controle de acesso necessita de parâmetros para tomar decisões de modo a identificar quando negar ou conceder acesso a um determinado dispositivo. O ELECTRON baseia-se em um modelo de confiança, que coleta informações a sua volta e toma decisões com base nessas informações. Embora o uso de confiança no contexto da IoT não seja algo novo, neste trabalho,

alia-se a confiança com um forte contexto social dos objetos. A finalidade é que a sociabilidade apoie na obtenção de valores mais precisos sobre os comportamentos dos dispositivos. Adaptou-se, assim, a lógica subjetiva (LS) (Jøsang, 1997) como mostra a Equação 4.5, onde os parâmetros da confiança são influenciados por fatores sociais como amizade e tipo de relacionamento.

$$T_{ij}^{C} = \alpha D_{ij} + \beta S_{ij}^{C} + \gamma R_{ij} \tag{4.5}$$

Confiança direta (D_{ij}) está vinculada as próprias experiências do dispositivo com os seus vizinhos e reflete a confiança direta do nó i vista durante contato direto com o nó j. Ela representa o valor mais importante dentro da confiança, porque demonstra os resultados das escolhas do dispositivo. A Equação 4.6 denota o cálculo da confiança direta.

$$D_{ij} = b + d + u \tag{4.6}$$

Similaridade com a comunidade (S_{ij}^{C}) indica a intensidade em que o dispositivo j assemelha-se aos dispositivos pertencentes a comunidade C. Ao empregar o cálculo da similaridade, apresentada na Equação 4.2, essa propriedade influencia a confiança com fatores como interesses em comum e amizades. Com isso espera-se que esses fatores sociais ajudem a melhorar a acurácia na construção da confiança.

Recomendação (R_{ij}) trata da confiança de outros nós em relação ao nó j. Essa opinião é compartilhada entre os nós da comunidade, para então contribuir na construção da confiança geral de cada nó. A recomendação, denotada na Equação 4.7, não sofre nenhuma alteração social para sua computação.

$$R_{ij} = b + d + u \tag{4.7}$$

Todavia, as recomendações precisam ser medidas de acordo com a relação social estabelecida entre o recomendante e o requerente. Logo, estabeleceram-se valores para pesar as recomendações na Equação 4.5. Esse peso (γ) representa um *fator de relacionamento*, dentro da composição da confiança geral. Esse fator de relacionamento pondera as recomendações de acordo com as relações sociais, com o propósito de filtrar as recomendações mais importantes para a confiança. Então a confiança geral (T_{ij}^{C}) é obtida ao somar a confiança direta (D_{ij}) e as recomendações (R_{ij}) dos vizinhos de i em relação ao nó j. O valor da confiança geral encontra-se em um intervalo de [0...1], no qual α, β e γ ponderam a importância de cada propriedade de acordo com a situação. A Tabela 4.1 mostra os pesos estabelecidos para as recomendações de acordo com a relação social. Nota-se que o peso para as recomendações possui uma menor importância, deixando que a confiança direta e a similaridade com a comunidade influenciem mais a confiança. Assim, divide-se o valor restante entre α e β segundo o fator de relacionamento.

4.2.3 Lógica subjetiva

A lógica subjetiva (LS) tem sido aplicada em recentes trabalhos no contexto de IoT (Khan e Herrmann, 2017; Son et al., 2017). Seu principal conceito baseia-se em denotar a confiança através de opiniões. Em geral, a notação ω_x^A representa uma opinião dentro da LS. No qual x representa a variável alvo ou a proposição para qual a opinião se aplica e A indica o agente que detém a opinião. O princípio de que um agente A possui uma opinião sobre uma variável

Tabela 4.1: Fator de relacionamento

Relação dos objetos	**valor de γ**
Relação de propriedade (ROPR)	0.3
Relação de localização (ROL)	0.2
Relação de trabalho (ROT)	0.2
Relação social (RSO)	0.1
Relação Parental (ROP)	0.1

x significa que existe uma relação de crença dirigida. Crer e confiar são conceitos similares, a sutil diferença está em que a confiança assume dependência e riscos, enquanto a crença não necessariamente. As opiniões de confiança são abstraídas e representadas como um triângulo de opinião, Figura 4.5.

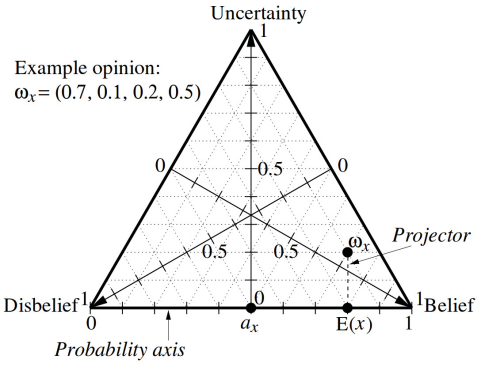


Figura 4.5: Triângulo de opinião (LS) (Jøsang, 1997)

Os conceitos crença (*belief*), descrença (*desbelief*) e incerteza (*uncertainty*) formam as pontas do triângulo e uma opinião denotada como $\omega_x^A = (b, d, u, a)$. Os parâmetros b, d e u representam crença, descrença e incerteza respectivamente, onde $\{b, d, u\} \in [0, 1]^3$ e $b+d+u = 1$. Os valores de b, d e u podem ser obtidos pela Equação 4.8. O parâmetro $a \in [0, 1]$ representa uma taxa base usada para computar o valor da expectativa probabilística, determinado como $E(\omega_x^A) = b + au$. Na ausência de uma evidência específica sobre uma determinada parte, a taxa base determina uma confiança *a priori* que pode ser aplicada a qualquer membro da comunidade (Jøsang et al., 2006).

$$b = \frac{pos}{(pos + neg + 2.0)} \quad d = \frac{neg}{(pos + neg + 2.0)} \quad u = \frac{2.0}{(pos + neg + 2.0)} \tag{4.8}$$

Constrói-se o valor da opinião com experiências positivas e negativas em relação a uma variável alvo x. Nas equações acima, as experiências positivas são expressas por *pos*, enquanto *neg* expressa as experiências negativas. Dessa forma experiências passadas podem ser convertidas em opiniões. Ademais, essas opiniões (os termos confiança e opinião são usados, nesse contexto, de forma intercambiável) possuem uma propriedade chamada transitividade. A transitividade se baseia na confiabilidade de uma opinião e que esta pode ser utilizada por outro agente. A partir disso, algumas operações podem ser obtidas, entre elas duas utilizadas neste trabalho: desconto e consenso.

Desconto é usado para avaliar correntes de transitividade. Em geral, utiliza-se desconto para expressar um grau de confiança em uma fonte de informação e, em seguida, descontar informações fornecidas por essa fonte como uma função da confiança na fonte. Expressa pela Equação 4.9.

$$\omega_C^{A:B} = \omega_B^A \otimes \omega_C^B \tag{4.9}$$

Consenso é usado para medir duas opiniões juntas. Também chamado de *fusão de confiança*, o consenso se baseia na ideia de coletar informação de diferentes fontes com a finalidade de se manter melhor informado e é expresso pela Equação 4.10.

$$\omega_C^{A \Diamond B} = \omega_B^A \oplus \omega_C^B \tag{4.10}$$

Entretanto, a confiança não é sempre transitiva. Por exemplo, ao assumir que Alice confie em Bob para cuidar de sua criança e Bob confia em Charlie para consertar seu carro, não implica que Alice confia em Charlie para cuidar de sua criança. Certos requerimentos semânticos precisam ser satisfeitos para que a confiança possa ser transitiva e que um sistema de confiança possa ser usado para derivar a confiança.

4.2.4 Módulo contexto e experiências

O gerenciador de contexto identifica e retorna o contexto atual do dispositivo. Sua base está na troca de informação entre os dispositivos. Informações como posição atual e tipos de dispositivos próximos podem ser adquiridas por um nó da rede. Tais informações formam o que denominamos de "contexto". A importância de conhecer o contexto inserido e se adaptar tem sido destacada em recentes pesquisas (Fernandez-Gago et al., 2017). Entretanto, devido à dinamicidade implícita da IoT, onde os objetos possuem uma grande mobilidade, lidar com apenas um contexto não representa a realidade. Logo, um gerenciador que receba informações e identifique o contexto atual se faz necessário para uma maior acurácia na avaliação.

Este módulo reflete uma lista detalhada sobre os ambientes em que o dispositivo foi inserido, isto é, lugares e tipos de dispositivos envolvidos. Deste modo, idealizou-se fazer com que o gerenciador de contexto contribuísse para o cálculo da confiança social. Impondo uma influência do contexto sobre a confiança social, de forma a conceder maior relevância para os ambientes em que os dispositivos estão operando. Com esse intuito, o gerenciador de contexto fornece o valor para a base do cálculo da confiança (a), apresentada na Seção 4.2.3, ao analisar o contexto atual dos dispositivos na comunidade. O resultado desta intervenção propicia uma melhor ou pior convergência da confiança conforme seu valor.

O gerenciador de experiências tem o objetivo de armazenar experiências ruins, em relação a serviços prestados por vizinhos. O propósito de armazenar experiências ruins baseia-se em uma abordagem psicológica, no qual pessoas tendem a guardar as configurações do ambiente que causaram interações negativas (McKnight et al., 1998). Portanto, o gerenciador de experiência mantém uma relação muito forte com o contexto, pois as más experiências serão relacionadas ao contexto atual. Neste módulo, são feitas associações entre experiências ruins e o contexto nas quais estas ocorreram, para que em futuras interações semelhantes o valor da confiança seja menor.

4.2.5 Módulo controle de acesso

O módulo controle de acesso toma a decisão de acesso ou não do dispositivo dentro do mecanismo ELECTRON. Para isso, recebe as informações do gerenciador de confiança e as emprega para tomar a decisão de acesso. A inteligência definida neste trabalho para a tomada de

decisão baseia-se, inicialmente, no valor calculado para confiança. Sendo ele acima de um *limite* (definido neste trabalho como 0, 6) o acesso é concedido aos serviços e aplicações disponíveis na rede. Porém, a inteligência para tomada de decisão pode ser ainda melhorada, abordando outras técnicas com maior fundamentação para a tomada decisão, como por exemplo a lógica Fuzzy.

4.3 FUNCIONAMENTO

Esta seção ilustra o funcionamento do mecanismo ELECTRON numa rede IoT de modo a auxiliar no controle da associação de nós mitigando a participação de nós em comportamento Sybil. A Figura 4.6 retrata uma rede IoT composta de cinco nós, chamados de nó N_a, N_b, N_c, N_d e N_e, dentro de uma comunidade de interesse, neste caso a Escola, onde o valor da taxa base (a) corresponde a 0,5. Inicialmente, os nós requisitantes enviam as listas de amizades e interesses em comum, correspondendo a lista de outros dispositivos que pertencem a amigos e interesses que o usuário possui, que no exemplo corresponde a disciplinas, professores ou alunos. Em seguida, o módulo gerenciador da confiança social do mecanismo, no caso junto ao nó N_b, determina uma opinião em cada nó da rede sobre o nó candidato, como visto no tempo t_1. A opinião inicia com valor zerado, mas é influenciada pelos gerenciadores de contexto e experiências. Onde o contexto define o valor a conforme a comunidade em que o nó candidato requisita acesso e o gerenciador de experiência pesquisa no histórico interações prévias do candidato. Se existir um histórico de contatos anteriores, computa-se as experiências positivas e negativas na formação da nova confiança social com o dispositivo.

Estabelecida a configuração da confiança, os nós da rede interagem com os nós candidatos. No tempo t_2, ainda na Figura 4.6, os nós da rede iniciam a avaliação da confiança direta com os candidatos e a medida que as interações ocorrem, as experiências positivas e negativas são computadas. A partir das primeiras experiências avaliadas, aplicando a Equação 4.8, calcula-se o valor da confiança direta de cada nó da rede para os candidatos. Em seguida, os nós N_a, N_b e N_c transmitem suas recomendações com base na confiança direta observada para seus vizinhos. Após o recebimento das recomendações, calcula-se o primeiro valor da confiança social dos candidatos. Filtrando as recomendações pela relação social estabelecida com o vizinho que enviou a recomendação e tendo seu valor persuadido pela similaridade do candidato com a comunidade, como denotado na Equação 4.5.

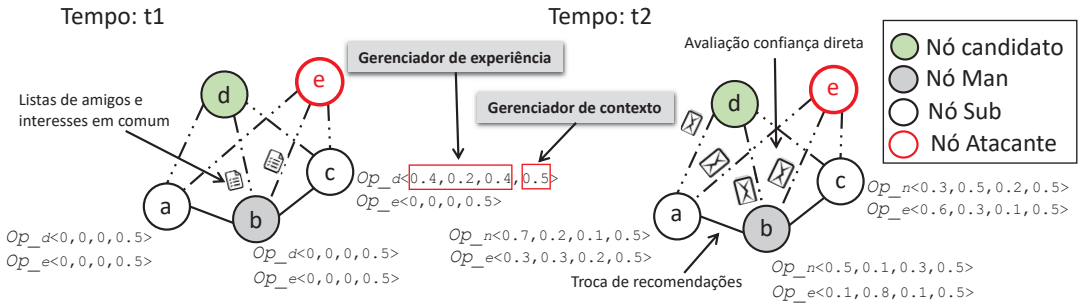


Figura 4.6: Criação dos opiniões sobre os candidatos

O nó N_e, atuando como atacante Sybil, entra em modo promiscuo e busca identidades para serem roubadas, ilustrado na Figura 4.7 no tempo t_3. As identidades roubadas pelos atacantes são armazenadas e novas identidades são fabricadas a partir da identidade adquirida. No tempo t_4, o nó N_e solicita o acesso à rede, executando o ataque Sybil na tentativa de autenticar-se com a identidade roubada. Entretanto, o módulo de autenticação ao verificar a confiança social do nó N_e constata que confiança dele não alcançou o valor mínimo de 0,6. Logo, com base no

comportamento, relações sociais e similaridade com a comunidade, o ELECTRON bloqueia o acesso pelo atacante no tempo t_5, e assim consegue preservar a privacidade da rede.

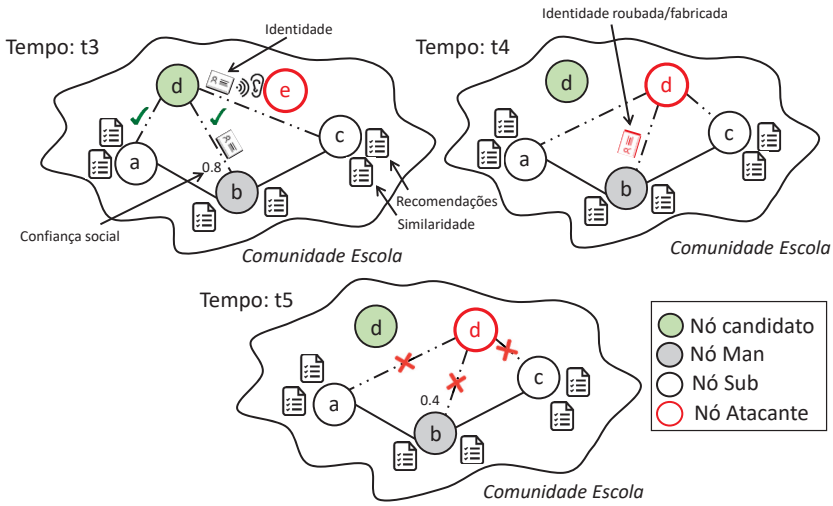


Figura 4.7: Detecção do ataque Sybil com id. roubada/fabricada

4.4 RESUMO

Este capítulo apresentou o mecanismo ELECTRON para o controle de acesso baseado em confiança e no contexto de comunidades. Inicialmente, foi descrito o modelo de rede onde o ELECTRON deve atuar, bem como os seus componentes. Em seguida, o AS foi modelado dentro do modelo de rede proposto e seu comportamento descrito. Então, como medida contra o ataque denotou-se o mecanismo ELECTRON para um controle de acesso resiliente a AS. O mecanismo apresenta um forte contexto social, onde considera-se a formação de comunidade baseadas em amizades e interesses em comum. As comunidades influenciam os valores da confiança entre os dispositivos, sendo esta utilizada para estimar o comportamento dos nós e na identificação de atacantes Sybil.

5 AVALIAÇÃO

Este capítulo apresenta a avaliação do mecanismo ELECTRON para o controle de acesso. A avaliação tem o objetivo de analisar a eficiência do mecanismo em detectar e negar acesso aos atacantes Sybil e divide-se em dois aspectos: o primeiro com foco nos aspectos sociais do mecanismo como a evolução da confiança social (T_{ij}^{C}); o segundo com foco nos aspectos de segurança em relação aos ataques. A Seção 5.1 descreve a implementação do ELECTRON e do ataque Sybil no simulador NS-3. A Seção 5.2 ilustra o cenário utilizado na simulação, assim como descreve os parâmetros de configuração aplicados na simulação. Ela também demonstra os conjuntos de dados (*dataset*) empregados para proporcionar maior realidade ao cenário. A Seção 5.3 detalha as métricas empregadas para aferir o desempenho e a segurança do mecanismo. Por fim, a Seção 5.4 apresenta uma discussão sobre os resultados obtidos na avaliação dos mecanismos ELECTRON e SA²CI, onde os pontos positivos e negativos dos mecanismos são analisados.

5.1 IMPLEMENTAÇÃO

Os mecanismos ELECTRON e SA²CI foram implementados e avaliados através do simulador discreto de eventos NS-3 (*Network Simulator 3*) (, 2011). Esta ferramenta foi escolhida pelo seu trabalho em pesquisas e artigos científico no estudo de novas soluções para redes. Seu código aberto e baseado nas linguagens C++ e Python corroboraram na escolha da ferramenta, no sentido de facilitar seu acesso. O código fonte do simulador encontra-se disponível para alterações, permitindo que protocolos e eventos possam ser modificados conforme a necessidade, além de possibilitar a implementação de funções de coleta de dados e métricas selecionadas para avaliação. A versão do simulador empregada foi a 3.27, tendo suporte aos principais protocolos de comunicação sem fio, o que possibilita sua utilização para avaliações no contexto da Internet das Coisas (IoT).

5.2 CENÁRIO DA SIMULAÇÃO

O cenário avalia a facticidade do mecanismo em um ambiente heterogêneo e com restrições de recursos, de forma a representar uma *smart neighborhood* (vizinhança inteligente), onde pessoas transitam de suas residências para escolas, academia, parques e até escritórios de trabalho - considerando casos em que o local de trabalho fica perto da residência. A simulação executada leva em conta dois *datasets* que trazem para a simulação informações reais de sociabilização e mobilidade. O primeiro *dataset* contém informações da rede social baseada em localização chamada de *Brightkite* e encontrada no repositório em (Cho et al., 2011a). Nela, os usuários compartilham com amigos suas localizações através de *checking-in*, em áreas como a cidade de São Francisco no Estados Unidos. Os dados consistem de ambientes como residência, trabalho e locais de lazer. A rede de amizade compõe-se de 58,228 nós e 214,078 arestas com informações coletadas entre abril de 2008 e outubro de 2010, sendo que cada aresta representa um laço de amizade. As informações de amizade foram implementadas nos dispositivos dentro da simulação a fim de criar um cenário social mais realístico. Também estabeleceram-se cinco comunidades representando ambientes como *residência, escola, escritório, academia e parque*. Para cada tupla (*b,d,u,a*) da confiança correspondente a opinião do vizinho (visto na Seção 4.2), definiu-se o valor de *a* de acordo com a comunidade em que o nó se encontra. Esse valor foi

determinado a partir de uma análise empírica sobre os níveis de segurança de cada comunidade. Iniciando com o valor 1 para os ambientes mais seguros, como o doméstico, e tendendo a 0 nos contextos menos seguros, tais como os ambiente abertos.

O segundo *dataset* consiste de informações de pessoas transitando à pé em ruas da cidade (Kouyoumdjieva et al., 2014). O cenário urbano ao ar livre foi modelado na área de Östermalm no centro de Estocolmo, Figura 5.1, e representa uma grade de ruas interconectadas com um tamanho variando entre $20m$ e $200m$. Em cada rua, considera-se uma largura de $2m$ para cada lado o qual representa as calçadas. A área de observação é conectada ao exterior por 12 passagens e assume-se que os nós entram no cenário através de cada uma dessas passagens com uma taxa de chegada denotada por $\lambda = 0,15\ s^{-1}$. Na chegada de um cruzamento, os nós continuam movimentando-se na mesmo direção com uma probabilidade de 0,5 ou mudando sua direção e virando em uma rua adjacente com a mesmo probabilidade. Os nós vagam pelas ruas desta maneira até que uma passagem de saída do cenário seja selecionada e o nó deixa a área. A área ativa do cenário ao ar livre é de $5872m^2$. O cenário caracterizado pela alta mobilidade, no qual os nós se movem constantemente em todo seu período de existência na área observada. Experimentos foram realizados mudando a probabilidade de seleção das ruas e substituindo as ruas centrais por quadrados. Os resultados demonstram que as medidas tomadas não afetam significativamente os dados e, consequentemente, a conclusão final obtida junto aos resultados.

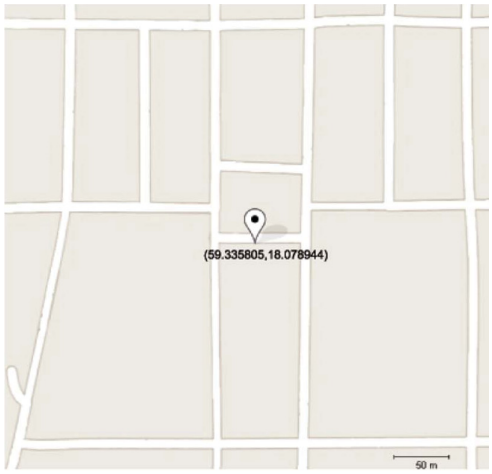


Figura 5.1: Cenário do *dataset* de mobilidade (Helgason et al., 2014)

O meio de transmissão baseia-se no padrão IEEE 802.15.4, utilizado pelo *framework* criado pelo IETF, chamado 6LoWPAN. O objetivo de utilizar o 6LoWPAN está no encapsulamento e mecanismos de compressão de cabeçalho que possibilitam o encaminhamento de pacotes IPv6 com mensagens de 127 $bytes$, melhor se adaptando a redes com dispositivos de baixo recurso computacional. Os dispositivos disseminam informações de uma origem para um destino com o propósito de simular uma aplicação em tempo real dentro de um ambiente IoT. Os atacantes requisitam acesso a rede através do uso de identidades roubadas ou fabricadas, com comportamento *churn* ou exibindo múltiplas identidades. Entre outros parâmetros de configuração estão a comunicação que utiliza o protocolo UDP (do inglês, *User Datagram Protocol*) e o total de nós nas simulações que variou entre 100, 150 e 200. Os valores da taxa base (a) foram definidos como 1, 0,7, 0,5, 0,4 e 0,2, respectivamente, para as comunidades *residência, escritório, escola, academia e parque*. Em cada simulação um total de 10% de atacantes busca acesso a rede, em um tempo total de $600s$ de simulação.

No início da simulação, uma fase de configuração inicializa os valores das variáveis de ambiente e os nós internos iniciam procedimentos para a primeira comunicação. Os

procedimentos consistem na abertura de um canal seguro para comunicação, utilizando uma criptografia assimétrica. Primeiro os nós mandam mensagens se anunciando, a fim de identificar os nós internos que integram a rede. Em seguida, chaves públicas são trocadas entre os dispositivos para iniciar uma comunicação segura. O objetivo de empregar a criptografia assimétrica nesse primeiro momento é criar um meio seguro para trocar uma senha única entre os dispositivos e a partir desse momento utilizar uma criptografia simétrica para a comunicação. A criptografia simétrica tem menor custo computacional para os dispositivos quando comparada com a criptografia assimétrica, tornando-a mais atrativa para um cenário com restrição de recurso. Durante a fase de configuração implementam-se as relações sociais presentes no *dataset Brightkite* (Cho et al., 2011a) e assume-se que não existe a presença de atacantes na rede. Ao final desta fase de configuração os nós iniciam a avaliação da confiança social, através da interação direta e por recomendações. O valor da confiança social inicia em 0 para todos os nós e permanece assim até que a configuração esteja completa. O tempo de duração da configuração dos nós fica um torno de $60s$, a partir daqui inicia-se a avaliação da confiança.

5.3 MÉTRICAS

As métricas aferidas na avaliação consideram a questão social de mobilidade dos usuários e a sua capacidade de proteger os ambientes de ataque Sybil que forjam uma identidade verdadeira ou falsa. Sendo empregada as métricas: ***Evolução da Confiança Social*** (T_{ij}^{C}), ***Taxa de Detecção*** (R_d), ***Acurácia*** (R_a), ***Falsos Positivos*** (R_{fp}) e ***Falsos Negativos*** (R_{fn}). A avaliação da T_{ij}^{C} aplica-se exclusivamente para o mecanismo ELECTRON, por considerar as relações sociais entre os dispositivos. As demais métricas avaliam ambos os mecanismos ELECTRON e SA²CI. Desta maneira, as métricas serão detalhadas a seguir.

A ***Evolução da Confiança Social*** (T_{ij}^{C}) indica como a confiança evolui ao longo do tempo através de uma função de distribuição cumulativa (CDF do inglês, *Cumulative Distribution Function*). O objetivo desta métrica é observar qual o comportamento da curva CDF em cada comunidade, pois os valores da taxa base de cada comunidade são únicos e estes influenciam como a confiança evolui ao longo do tempo. Os valores também foram separados conforme a relações social para se obter uma análise do comportamento da confiança em cada relação, lembrando que as recomendações são filtradas pelo tipo de relação social. Seu valor obtido pela Equação 4.5, previamente apresentada.

Taxa de detecção (R_d) contabiliza os ataques Sybil identificados corretamente pelo ELECTRON a partir da confiança social. O cálculo da R_d corresponde a razão entre o total de detecções, det_{ni}, e quantidade de ataques, T_{atq}, (Eq. 5.1). Esta métrica apresenta valores que variam entre 0% e 100%, onde quanto mais próximo dos 100% uma mensuração chegar maior será a eficácia do mecanismo.

$$R_d = \frac{\sum det_{ni}}{T_{atq}} \tag{5.1}$$

Acurácia (R_a) indica a precisão da detecção do ELECTRON. Esta métrica corresponde ao total de detecção do ataque Sybil, det_{ni}, a identificação correta dos nós legítimos da rede, det_{na}, dividido pelo total de requisições feitas à rede, T_{req}, (Eq. 5.2). A R_a também resulta em valores discretos entre 0 e 1, quando mais perto de 1 melhor a acurácia.

$$R_a = \frac{\sum det_{ni} + \sum det_{na}}{T_{req}} \tag{5.2}$$

Taxa de falsos positivos (T_{fp}) determina a quantidade de vezes que o ELECTRON identificou um ataque Sybil quando não existia o ataque. O seu cálculo acontece através da divisão entre o número de *Falsos Positivos* pela soma dos *Falsos Positivos* e *Verdadeiro Negativo* (nós legítimos classificados como legítimos). Seu valor é obtido pela Equação 5.3.

$$R_{fp} = \frac{FalsePos}{FalsePos + TrueNeg} \tag{5.3}$$

Taxa de falsos negativos (R_{fn}) determina a quantidade de vezes que o ELECTRON classificou um nó atacante como legítimo. O seu cálculo acontece através da divisão entre o número de *Falsos Negativos* pela soma dos *Falsos Negativos* e *Verdadeiros Positivos* (nós legítimos identificados corretamente). Seu valor obtido pela Equação 5.4.

$$R_{fn} = \frac{FalseNeg}{FalseNeg + TruePos} \tag{5.4}$$

5.4 RESULTADOS

Inicialmente avaliou-se o comportamento social dos dispositivos no ELECTRON dentro do cenário de *smart neighborhood* junto ao simulador NS-3. O mecanismo foi avaliado sob dois aspectos: destacando as relações sociais da SIoT na construção da confiança social; a eficácia do ELECTRON para garantir a segurança da rede, frente a um ataque Sybil. Os resultados foram divididos pelas quatro abordagens e comportamentos do ataque já mencionados. Os dados também foram separadas pelo total de nós na simulação. Primeiramente serão mostrados os resultados com 200 nós, em seguida com 150 nós, e por fim o resultado com 100 nós. Os resultados são descritos nas subseções a seguir.

5.4.1 ELECTRON - Análise da Percepção Social

Para analisar o comportamento social dos dispositivos, os valores da confiança social (obtidos da Equação 4.5) foram separados pelas 5 diferentes relações sociais da SIoT. A intenção de separar os valores pelas relações se deve pela influência de cada relação na confiança, tendo em vista que as recomendações são filtradas conforme a relação social construída com o nó vizinho. Os gráficos também foram diferenciados segundo a comunidade avaliada. Essa diferenciação acontece pois cada comunidade possui em contexto e o valor da taxa base (a), utilizada para se obter o *valor esperado*, definido exclusivamente para cada comunidade. Os gráficos a seguir contém o valor da confiança social em uma CDF. Encontram-se dois gráficos para cada comunidade, onde o primeiro mostra a evolução da confiança entre os nós internos à rede e o segundo dos nós externos que fazem a requisição de acesso.

Nesta seção, apenas alguns gráficos foram selecionados para contribuir para a discussão da evolução da confiança social. Selecionaram-se os gráficos do ataque Sybil com comportamento *churn* e identidades roubadas pois os resultados demonstram que este ataque representa o maior desafio para o mecanismo. Os gráficos também são referentes a simulação com 100 e 150 nós por apresentarem um comportamento distinto. A razão para essa seleção se deve ao grande número

que gráficos gerados pela simulação, além de mostrarem uma variação pouco representativa para construção da discussão. Porém, o restante dos gráficos referente aos outros ataques e a simulação com 200 nós encontram-se no Anexo A.

A Figura 5.2 demonstra a construção da confiança social entre os nós internos da rede e os nós externos com 100 nós. É possível ver que a relação parental (com menos importância na recomendações) tem o pior desempenho entre os nós internos, obtendo uma vantagem apenas na comunidade *Academia* sobre a relação do tipo social que foi perdida pouco depois dos 70% de simulação. No entanto seu comportamento vária quando avaliado entre os nós externos, alcançando valores mais altos na comunidade *Residência* e valores mais baixos na comunidade *Academia*. A evolução da confiança social entre os tipos de relação não segue um comportamento estável, como observado entre os nós internos. O maior valor para a confiança social entre os nós varia entre as relações, tendo uma evolução claramente menos estável que os nós internos. Essa instabilidade se deve ao comportamento dos atacantes entre os nós candidatos avaliado pelo mecanismo, causando constantes quedas no valor agregado da confiança social.

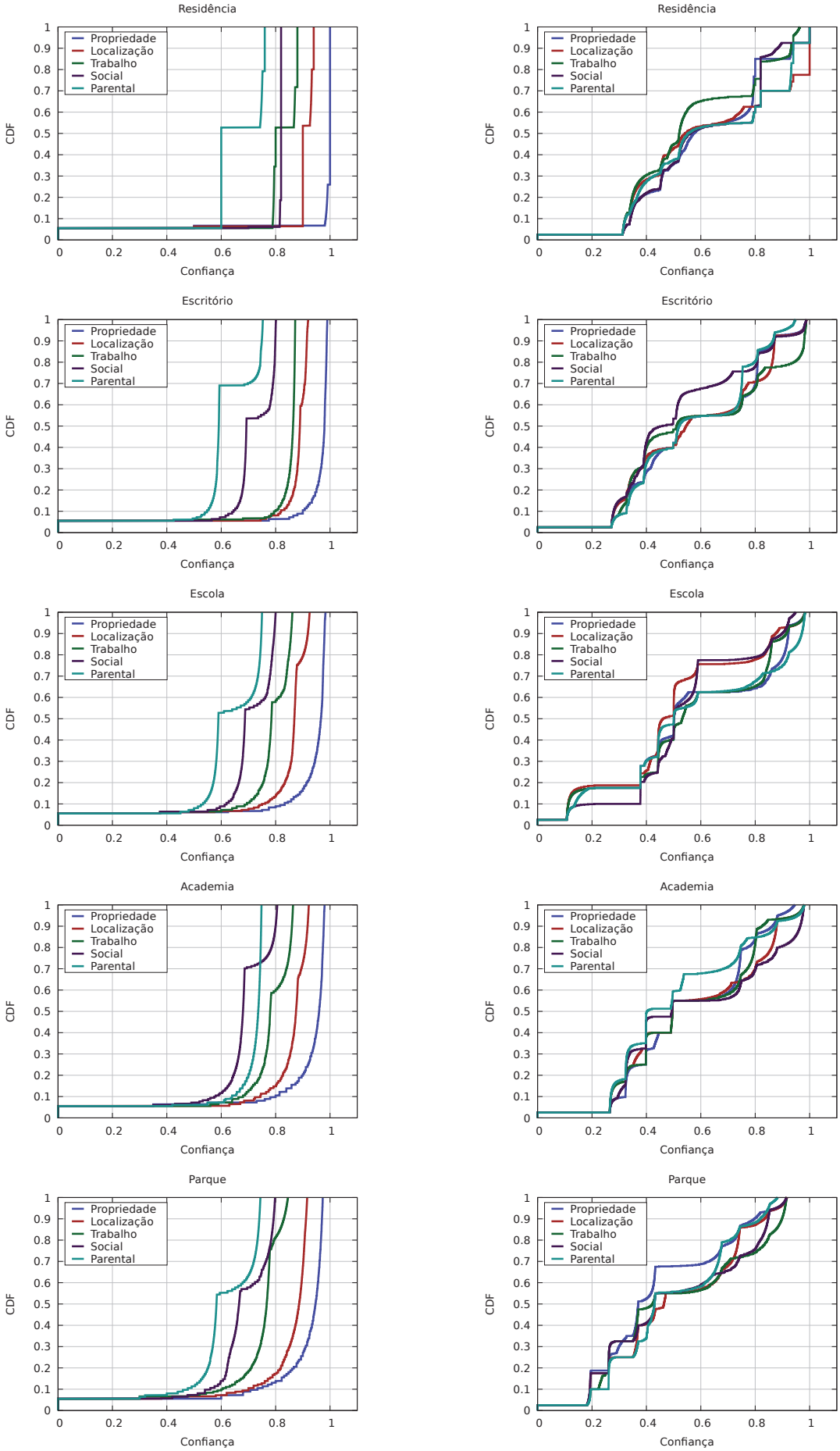


Figura 5.2: Evolução da confiança social em diferentes comunidades e relações (100 nós)

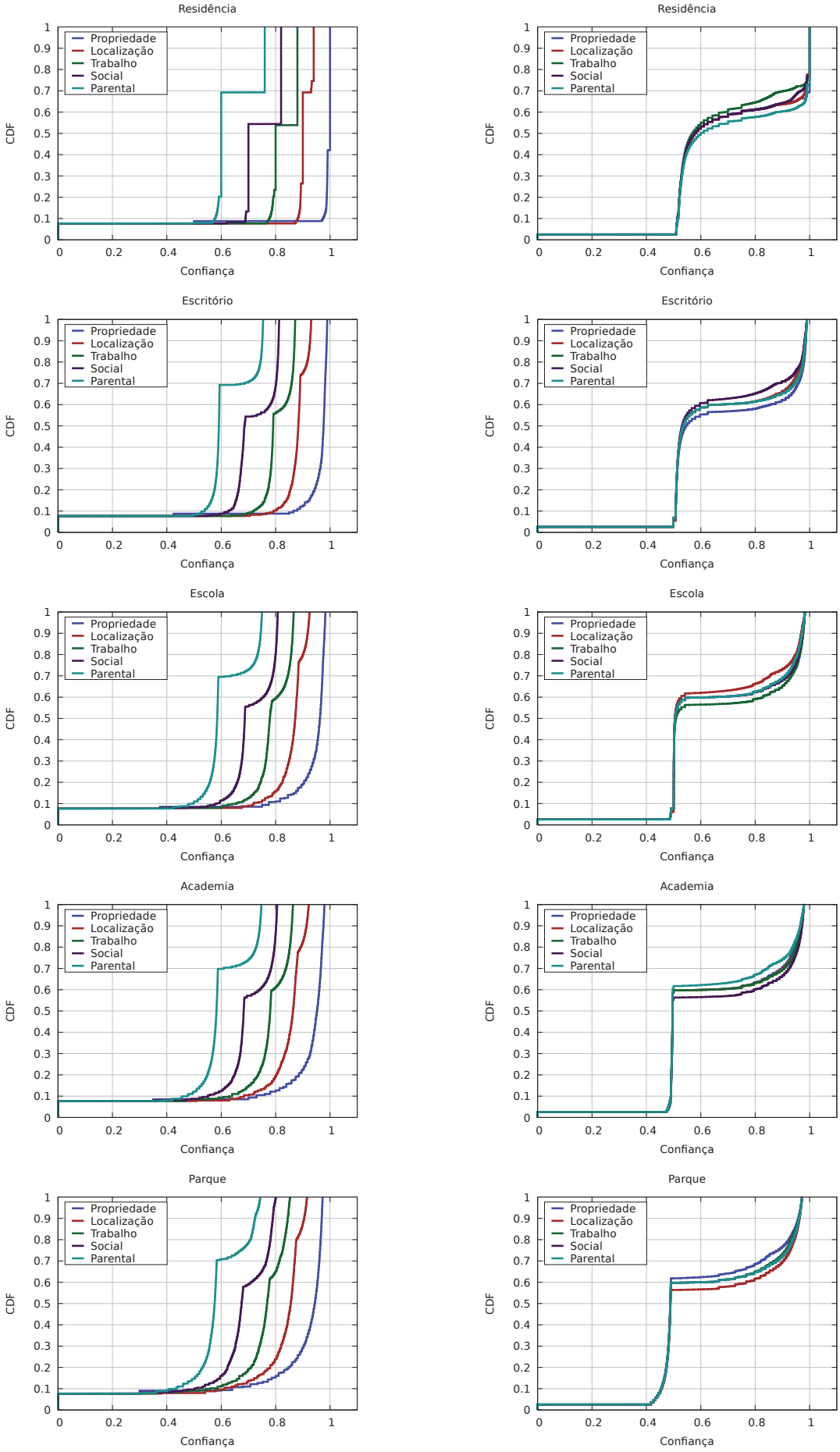


Figura 5.3: Evolução da confiança social em diferentes comunidades e relações (150 nós)

Porém, nos resultados da simulação com 150 nós apresentada na Figura 5.3, observa-se uma curva diferente na evolução da confiança social entre os externos (dispositivos que buscam acesso a rede). A simulação com 100 nós inicia com valores entre 0,1 e 0,3, enquanto a com 150 os valores da confiança iniciam entre 0,4 e 0,5. Isso acontece pela distribuição dos nós entre (i) internos da redes, (ii) candidatos legítimos ao acesso e (iii) atacantes, sendo o número de atacantes maior do que o de nós candidatos legítimos. Esse detalhe faz com que os valores da confiança sejam mais instáveis, variando para valores inferiores. Ao passo que na simulação com 150 nós existe um número maior de nós legítimos buscando acesso, fazendo com que os valores incrementem com uma maior constância.

A seguir, denotam-se as informações da confiança social no gráfico *boxplot*. Este tipo de gráfico consiste em uma ferramenta para visualização da distribuição de um conjunto de dados, formando um meio complementar para desenvolver uma perspectiva sobre o caráter dos dados. O gráfico com a CDF permite analisar como a confiança evoluiu em valores contínuos; agora a intenção é demonstrar como os valores finais da confiança estão dispostos. Tendo como objetivo neste trabalho detectar intrusos Sybil, o valor da confiança nos gráficos da Figura 5.4 referem-se apenas a avaliação dos nós internos sobre os nós externos que requisitam acesso à rede. A Figura 5.4 mostra os *boxplots* da confiança relativas a simulação com 100 nós. A primeira característica observada está na *posição* dos dados, indicada pela linha no centro da caixa. Esta linha representa o segundo quartil ou a mediana, denotando que pelo menos 50% da amostra está abaixo dela e os outros 50% acima. A mediana também está ligada a outra característica do gráfico: a *simetria*. Um conjunto de dados tem uma distribuição simétrica quando a linha da mediana se encontra no meio do retângulo. Caso contrário, os dados são assimétricos positivos, se a linha está próxima do primeiro quartil, ou negativos, se a linha está próxima do terceiro quartil.

Os valores na Figura 5.4 apontam que a mediana em todas as comunidades ficou abaixo de 0,6, variando entre 0,4 e 0,55. Esse dado indica que mais de 50% dos candidatos requisitando acesso na rede não obtiveram a confiança mínima para garantir o acesso (definida em 0,6). Entretanto, nota-se a discrepância onde candidatos conseguiram o valor máximo da confiança (1), como no caso da comunidade *Residência*. Outra característica trata da *dispersão* dos dados. A dispersão representa o intervalo *interquatilico*, sendo a diferença entre o primeiro e o terceiro quartil (tamanho da caixa). Nos gráficos, observam-se diferentes dispersões entre os dados, principalmente comparando as relações social e parental na comunidade *Escola*. Cerca de 75% dos valores na relação social não ultrapassou o valor de 0,6, enquanto na relação parental os valores chegaram a 0,9.

Este comportamento é inesperado, visto que o peso em recomendações para a relação parental é menor que a social. Porém ela mostra a capacidade do mecanismo de mesmo a relação possuindo valores maiores de recomendação, atribuir valores menores para relações com maior número de atacantes. Ainda na Figura 5.5, encontram-se os valores para a simulação com 150 nós. Nos gráficos os valores da confiança entre as comunidades não possuem expressivas diferenças, mostrando que o valor de a para cada comunidade não representa grande peso no valor final da confiança. Tendo um maior impacto na evolução da confiança, alterando o comportamento das curvas examinadas nas Figuras 5.2 e 5.3. A dispersão dos dados também chama a atenção na Figura 5.5, a qual possui uma amplitude bem maior que na simulação com 100 nós. Essa amplitude mostra a diferença entre os valores da confiança de candidatos legítimos e dos atacantes, expondo uma grande separação nos dados.

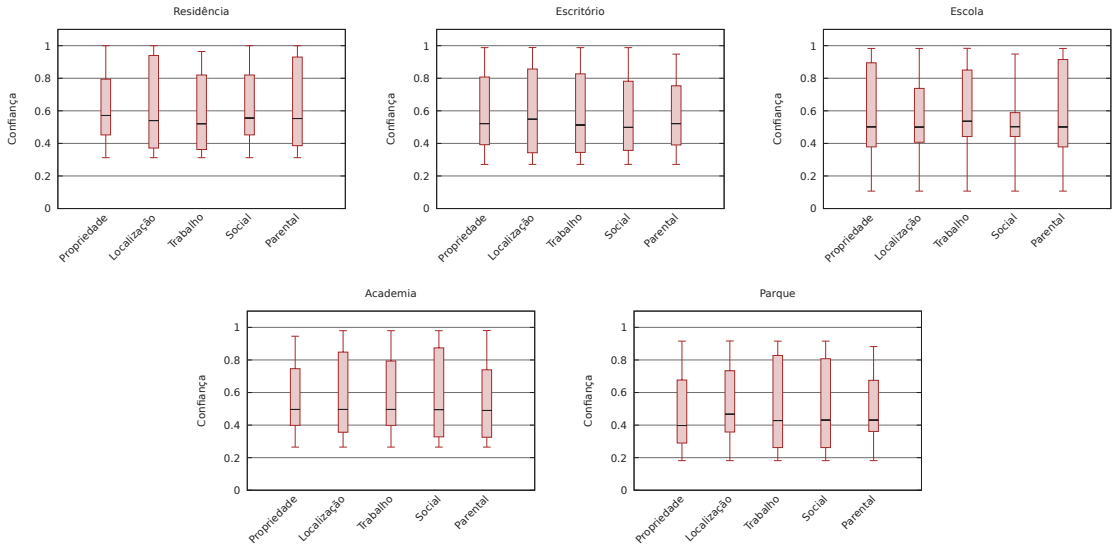


Figura 5.4: Variação da confiança social dos nós candidatos pelos nós da rede (100 nós)

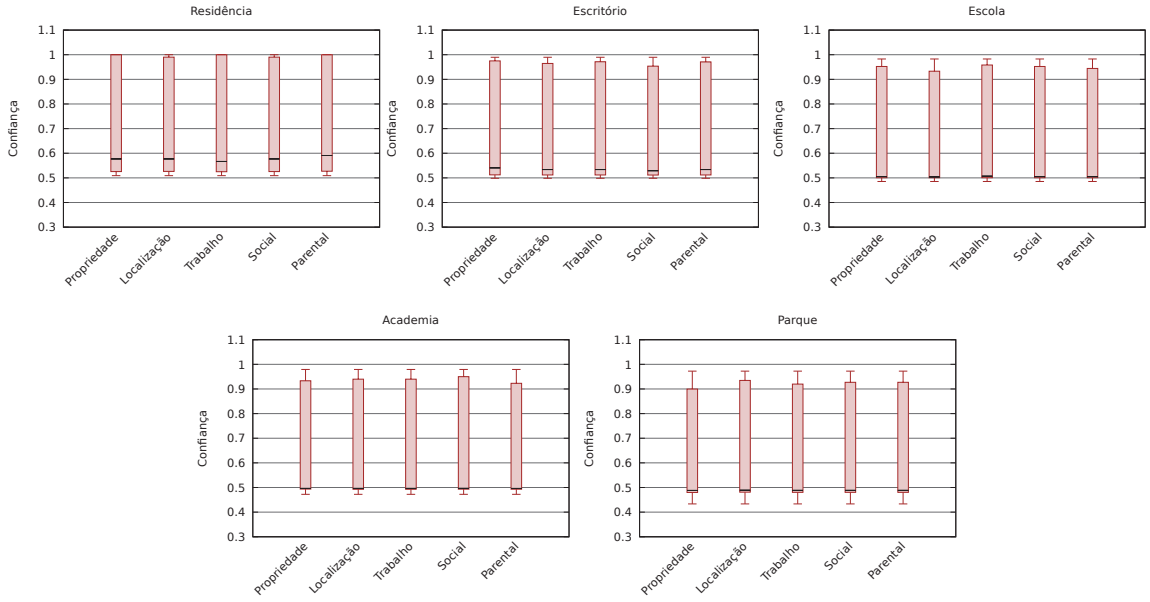
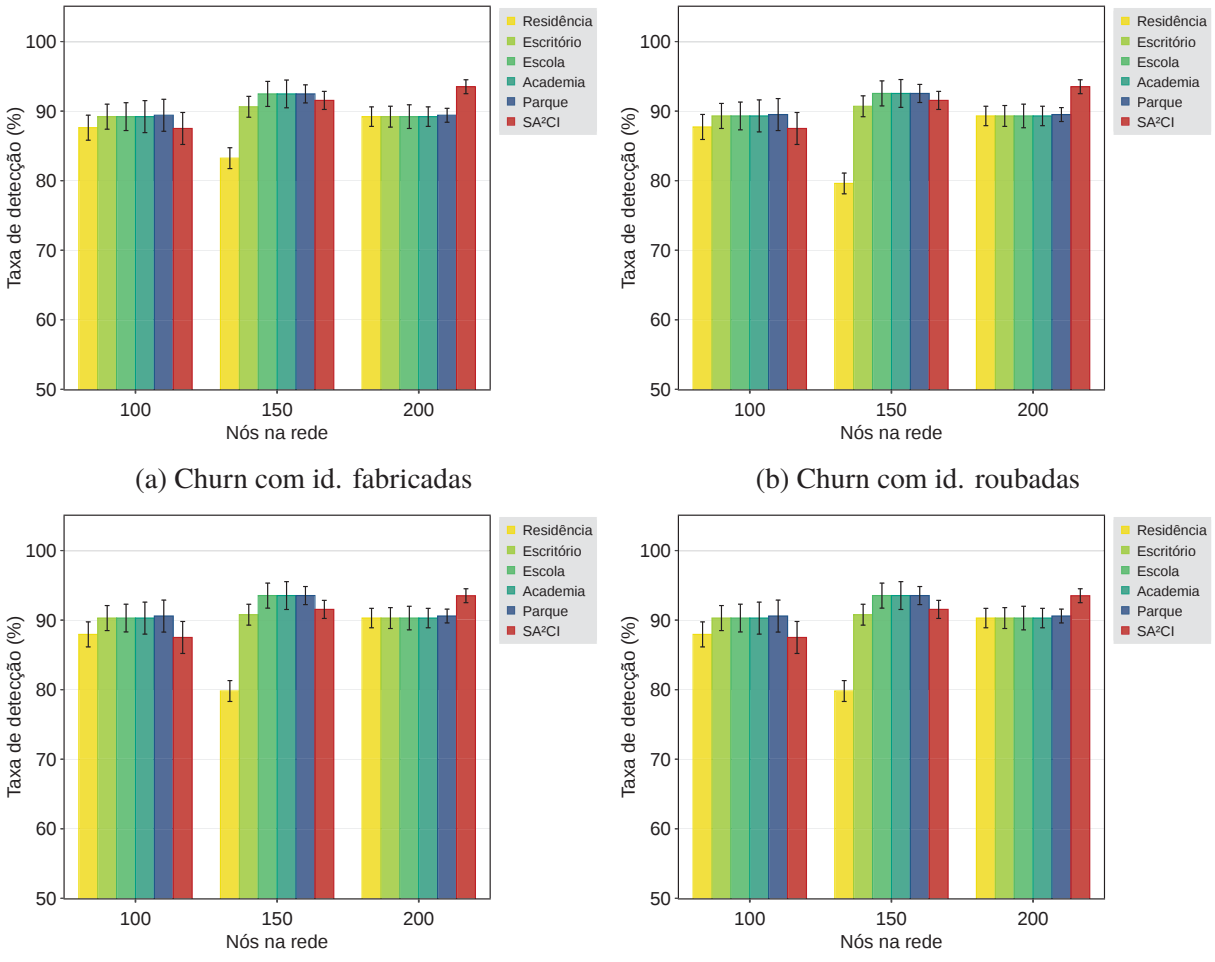


Figura 5.5: Variação da confiança social dos nós candidatos pelos nós da rede (150 nós)

5.4.2 ELECTRON - Análise da Eficácia da Segurança

Na análise da eficácia da detecção, avaliou-se os mecanismos ELECTRON e SA²CI na presença de atacantes Sybil, as seguintes métricas de segurança foram mensuradas: taxa de detecção (R_d), acurácia (R_a), taxa de falsos negativos (R_{fn}) e taxa de falsos positivos (R_{fp}). As taxas de detecções (R_d) foram agrupadas na Figura 5.6, contendo todos os comportamentos do atacante Sybil e todas as simulações com 100, 150 e 200 nós. Entretanto, devido ao grande volume de dados gerados e para manter a coesão na discussão dos resultados, as demais métricas se referem apenas ao atacante Sybil com comportamento *churn* aplicando identidades roubadas, executado nas simulações com 100 e 150 nós. O comportamento *churn* com identidades roubadas foi escolhido justamente por representar o maior desafio para o mecanismo e, assim, melhorar a discussão. Os demais resultados dos outros ataques e da simulação com 200 nós encontram-se nos Anexos A.1.

Na Figura 5.6, observam-se os gráficos com as taxas de detecção obtidos ao longo das simulações, com um total de 10% de atacantes. Ao analisar os dados da taxa de detecção do ELECTRON para o comportamento *churn* com identidades roubadas, em sua primeira medição ele não consegue identificar nenhum atacante, onde a taxa parte de 0% em todas a comunidades. Mostrando a complexidade de identificar o ataque considerando a alta mobilidade do atacante e o uso de identidades válidas na rede. No entanto, na Figura 5.6(b) observa-se que a taxa de detecção salta e alcança números entre 79.6% e 92.5%, se mantendo estável durante o resto da simulação. A razão para essa mudança brusca na taxa de detecção está no valor da confiança social construída entre os nós da rede. A taxa indica que o ELECTRON precisa de um tempo maior para ajustar na detecção de intrusos Sybil com alta mobilidade e identidades roubadas de nós da rede. Ao analisar mais profundamente o valor da confiança social como "princípio ativo" para identificar atacantes, espera-se que a taxa expresse um progresso gradativo na detecção das ameaças. Contudo, é nítido nos gráficos o alcance de eficiência por parte do ELECTRON, feito proporcionado pelas relações sociais filtrando as recomendações (confiança indireta) e as listas de amizades e interesses em comum influenciando na construção da confiança social.



(a) Churn com id. fabricadas

(b) Churn com id. roubadas

(c) Múltiplas id. roubadas

(d) Múltiplas id. fabricadas

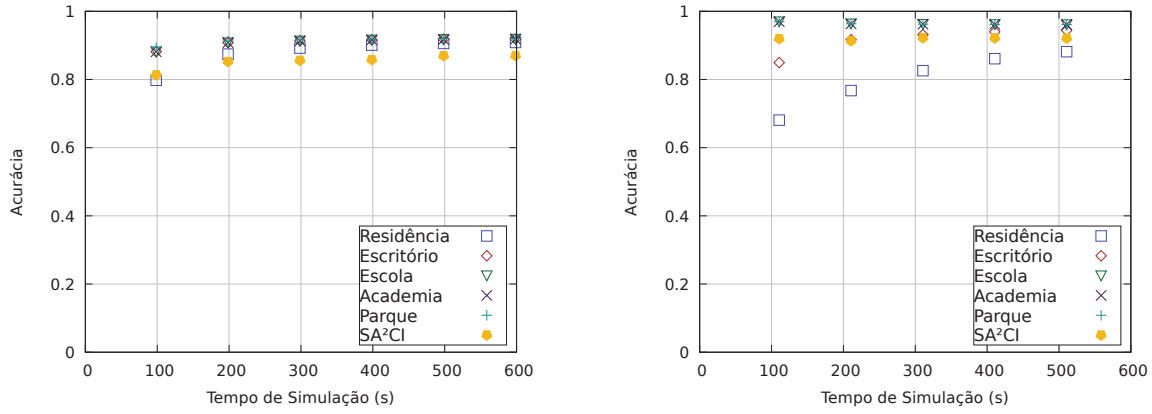
Figura 5.6: Taxa de detecção

As Figuras 5.6(a), 5.6(c) e 5.6(d) contêm os gráficos com a taxa de detecção para os ataques de múltiplas identidades fabricadas e roubadas e *churn* com identidades fabricadas. Observa-se nos gráficos que a taxa de detecção para a simulação com 200 nós obteve uma maior estabilidade em relação as outras simulações. As simulações com 200 nós começando

com uma taxa de detecção por volta de em 100% para os ataques com múltiplas identidades e caindo para uma taxa de 90.2%, como pode ser visto nas figuras acima. Esse comportamento acontece pelo valor da confiança aferido aos atacantes, principalmente na comunidade Residência e Escritório. Nestas comunidades os atacantes superaram o valor limite de 0.6 para garantir o acesso, conquistando maior sucesso ao burlar o mecanismo.

Na Figura 5.6, também percebe-se uma maior alteração nas comunidades *Escritório* e ainda mais brusca na *Residência*, justamente onde a taxa base (a) para cálculo da confiança é maior. Isto indica que uma taxa base superior não significa maior detecção, e que essas comunidades são mais sensíveis aos ataques, precisamente por convergir a confiança mais facilmente. Apesar de possuírem um sucesso menor na detecção, as comunidades *Residência* e *Escritório* terminam a simulação com taxas por volta de 79,6% e 90,6%, respectivamente, mostrando que apesar das desvantagens o ELECTRON ainda consegue boas taxas de detecção. Embora o mecanismo possua uma recuperação na taxa, ao ponderar que o motor de detecção é baseado em confiança e sociabilidade, uma desvantagem para o mecanismo é o atacante alterar seu comportamento.

Ao comparar as detecções entre ELECTRON e SA²CI percebe-se uma desvantagem do SA²CI na simulação com 100 e 150 nós. Entretanto, na simulação com 200 nós o mecanismo baseado em criptografias obtém uma taxa melhor de detecção, se comparada com as comunidades criadas pelo ELECTRON. Essa vantagem em uma maior quantidade de nós se deve ao grande números de nós formando opiniões para a construção da confiança no ELECTRON, o que torna mais difícil convergir para um consenso dentro da comunidade. Em compensação, em um ambiente com menor número de dispositivos, onde existem opiniões mais consistentes, o gerenciamento da confiança baseada nas relações sociais, mostrou-se mais eficiente ao detectar o ataque Sybil. Assim como apresentando uma estabilidade estabilidade entre as comunidades, mesmo em desvantagem para o SA²CI.



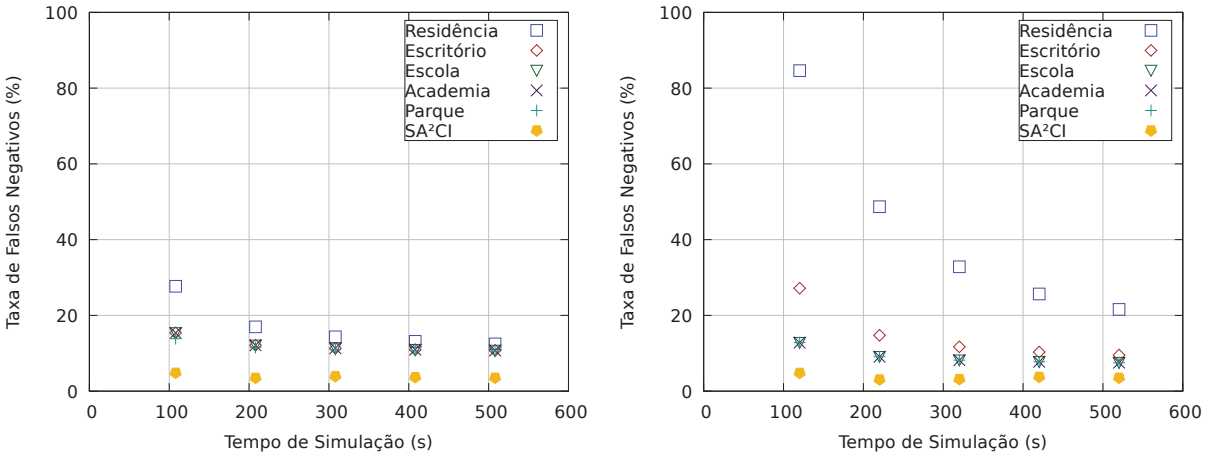
(a) 100 nós (b) 150 nós

Figura 5.7: Acurácia da detecção

Para complementar as informações da detecção dos atacantes pelo ELECTRON e SA²CI, mostra-se a seguir a acurácia da detecção (R_a) para o ataque *churn* com identidades roubadas nos gráficos da Figura 5.7. Percebe-se uma proporcionalidade entre a medição da R_a e a taxa de R_d. O gráfico na Figura 5.7(a) mostra a R_a na simulação com 100 nós, onde a comunidade *Residência* dispõe de valores menores. Reforçando o problema de uma convergência muito rápida da confiança social, melhor visto na Figura 5.7(b). Nota-se que a acurácia nas comunidades *Residência* e *Escritório* obtêm piores resultados comparada as outras comunidades para a simulação com 150 nós. Entretanto, as comunidades *Escola*, *Academia* e

Parque alcançam valores muito próximos de 1, sinalizando que uma maior quantidade de nós distribuindo recomendações contribui para uma melhor acurácia na detecção. Como resultado, atinge-se uma detecção acurada dos ataques conforme a confiança social estabiliza. Ao comparar o SA²CI percebe-se que a mesmo obteve uma acurácia melhor que as comunidades *residência* e *escritório* - comportamento observado na R_a, porém as outros comunidades se destacam por apresentarem uma leve vantagem; mostrando que o ELECTRON apresenta melhores medições para situações com maior exposição da segurança e para rede de pequeno e médio porte.

Em seguida, duas taxas importantes para se verificar a eficiência do mecanismo são dispostas: falsos negativos (R_{fn}) e falsos positivos (R_{fp}). A importância dessas taxas encontra-se na mensuração de possíveis erros na classificação de atacantes pelo mecanismo. Os falsos negativos representam o valor de atacantes classificados como nós legítimo da rede, e por isso, não taxados como ameaça. Em contrate os falsos positivos refletem os nós legítimos taxados como atacantes e impedidos de autenticar na rede.



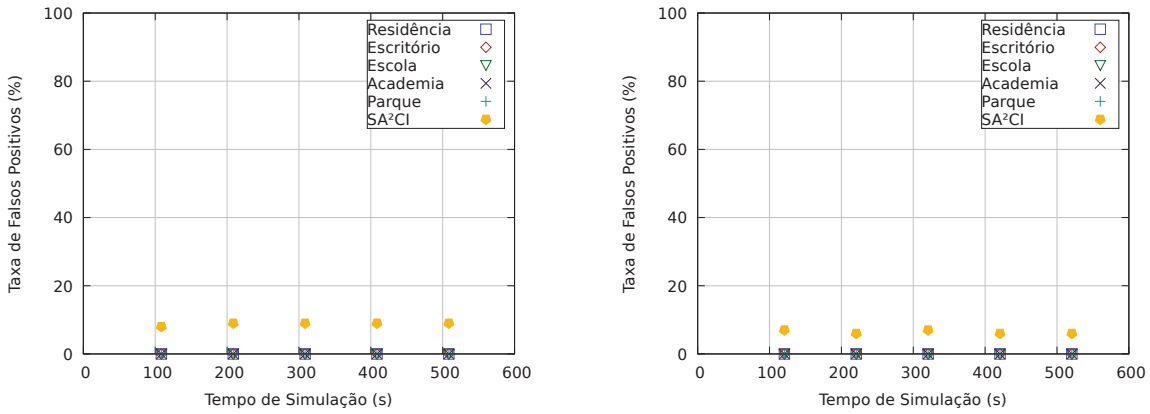
(a) 100 nós (b) 150 nós

Figura 5.8: Taxa de falsos negativos

Os gráficos na Figura 5.8 demonstram os valores da R_{fn} obtidos na detecção do mecanismos ELECTRON e SA²CI. Ao comparar a R_{fn} com os gráficos da R_d, percebe-se que elas são complementares para o mecanismo ELECTRON. Onde as atacantes não identificados pelo mecanismo foram classificados como nós legítimos. Alguns dos atacantes foram configurados para simularem o comportamento de nós legítimos, de forma a burlar o mecanismo e atingir confiança maiores. Como constatado na Figura 5.8(b), valores da R_{fn} chegaram perto de 90% na comunidade *Residência*, mostrando que houve problemas para identificar os atacantes no início da simulação. A medida que o valor da confiança social foi se ajustando aos dispositivos, conseguiu-se melhor identificar os atacantes obtendo ao final uma taxa de 22% para *Residência* e entre 10% para as demais comunidades. O mecanismo SA²CI obteve uma taxa menor na R_{fn} pois está menos suscetível a mudança de comportamento do atacante, comparada ao ELECTRON. Contudo, essa diferença se equilibra na R_{fp} como especificado na próximo gráfico.

A Figura 5.9 mostra os gráficos da R_{fp} aferidas aos mecanismos. Ao analisar os gráficos nota-se que não houve a ocorrência de falsos positivos na classificação do ELECTRON. Isso demonstra que o mecanismo consegue manter níveis estáveis de identificação de nós legítimos, sem classifica-los como atacantes. Porém, esse resultado acontece porque nenhum nó legítimo demonstrou comportamentos que podem levar o mecanismo a classifica-los como atacante. Logo, uma avaliação mais detalhada estudando outras tecnologias de transmissão e controle de canal precisa ser conduzida, a fim de obter-se valores definitivos dos falsos positivos do mecanismo. O

objetivo é mensurar os falsos positivos em ambientes com maiores taxas de colisão e perda de pacotes, para verificar como essas falhas impactam na precisão da R_{fp}. O SA²CI exibiu uma taxa de cerca de 11,4% de falsos positivos pois o atacante apresentando um comportamento *churn* oferece maior dificuldade ao mecanismo, devido a sua forma de associação e desassociação, o qual prejudica a distinção entre nós atacantes e nós legítimos. Em suma, ao analisar as R_{fn} e R_{fp} juntas, a razão de métrica sobre a outra acaba se igualando para a maioria das comunidades do ELECTRON e o SA²CI.



(a) 100 nós

(b) 150 nós

Figura 5.9: Taxa de positivos

6 CONCLUSÃO

A Internet das Coisas (IoT) está evoluindo em diferentes aplicações, abrangendo várias tecnologias, diferentes tipos de dispositivos e agregando conceitos subjetivos, mas quando modelados dentro de soluções para IoT trazem resultados tangíveis. Um exemplo consiste na formação do paradigma Internet das Coisas Social (SIoT), onde objetos imitam as relações sociais humanas e estabelecem cinco tipos de relações sociais entre si: relação de objeto parental (ROP), relação de objeto de propriedade (ROPR), relação de objeto por localização (ROL), relação de objeto para trabalho (ROT) e relação de objeto social (ROS). Entretanto, questões relacionadas a segurança da rede ainda permanecem sem respostas definitivas, sendo desafios para a implementação da IoT. Desafios principalmente na privacidade dos dados disseminados, comprometidos por um ataque Sybil. O atacante se aproveita de vulnerabilidades nas características da rede como heterogeneidade de objetos conectados, mobilidade e restrição de recurso para autenticar-se na rede e infligir a confidencialidade dos dados trafegados.

Os trabalhos encontrados na literatura buscam encontrar soluções que se adaptem as característica da rede. Uma classificação destas soluções pode ser feita através dos aspectos encontrados nas técnicas empregadas, as quais são: regras, características do objeto, histórico, contexto e sociabilidade. Dentro desses aspectos, destacam-se as técnicas baseadas em chave de capacidade, quantificação do risco e no gerenciamento da confiança. Essas abordagens mostram vantagens e desvantagens ao serem aplicadas. Entre as desvantagens encontram-se problemas como escalabilidade, falta de especificação, falta de flexibilidade em ambientes sociais altamente dinâmicos, entre outros. Logo, explorar a inteligência social incorporada nos objetos pode trazer vantagens como eficácia na detecção de ataques Sybil.

A fim de tratar essa questão, este trabalho propôs o mecanismo ELECTRON para o controle de acesso contra ataques Sybil à IoT. Ele leva em conta a sociabilização dos dispositivos como prevista no paradigma *Social* IoT. Essa sociabilização permite que objetos criem associações com maior peso com outros objetos específicos, produzindo uma percepção de comunidade dentro da rede IoT. A formação dessas comunidades entre os objetos baseia-se na similaridade em interesses, serviços partilhados ou contexto dos dispositivos. ELECTRON emprega o coeficiente de similaridade de Jaccard nas informações dos conjuntos de amizades e interesses em comum. Adaptou-se a Lógica Subjetiva para que o gerenciamento da confiança possa integrar os aspectos sociais dos dispositivos, constituindo uma confiança social. As relações sociais ponderam as recomendações dentro da rede, de forma a filtrar recomendações mais relevantes, e a similaridade com a comunidade influência no valor da confiança social. O gerenciador da confiança social analisa o comportamento de cada nó externo para avaliar a permissão de acesso, obtendo a permissão quando os dispositivos requisitante alcançam um valor mínimo da confiança social.

A avaliação comparou os mecanismos ELECTRON e SA²CI implementados no simulador NS-3. As informações sociais do ELECTRON foram incorporadas de dois *dataset* a fim de torna o cenário mais realístico. O primeiro *dataset* contém informações da rede social baseada em localização *Brightkite*, onde as informações de amizade foram incorporadas nos dispositivos da simulação. O segundo *dataset* disponibiliza informações para mobilidade dos dispositivos, considerando pessoas andando em ruas de uma cidade. Aplicaram-se métricas para analisar duas percepções sobre o mecanismo: percepção social e percepção de segurança. Na análise social demonstra-se a evolução da confiança social em cada comunidade e separada por relação social. Enquanto na análise de segurança, as métricas taxa de detecção, acurácia e taxa de falsos positivos/negativos mensuram a capacidade e eficiência em conter o ataque Sybil. Os

resultados demonstram que o mecanismo obteve dificuldade em encontrar os atacantes no início da simulação, entretanto conforme a confiança social se estabelecia, a taxa de detecção aumenta e os falses negativos diminuem. Além disso, o mecanismo não apresentou nenhuma ocorrência de falsos positivos, o que garante melhor fluidez para os nós legítimos. Isso mostra a contribuição das relações sociais e da confiança social para detectar diferentes comportamentos de ataques Sybil, bem como a eficácia da percepção do ELECTRON aos diversos ambientes. Ao comparar os resultados obtidos com o mecanismo baseado em criptografia SA²CI, notasse uma vantagem do ELECTRON na taxa de detecção em redes menores e médio porte, como também na taxa de falsos positivos. Contudo, em redes maiores e na taxa de falsos negativos o SA²CI obtém vantagem sobre o ELECTRON. Esse comportamento pode ser explicado pela crescente complexidade de convergir uma opinião em comum com um crescente número de dispositivos na rede, assim como os métodos de criptografia ajudam SA²CI a ter um melhor controle ao identificar o atacante, proporcionando uma menor taxa de falsos negativos.

Desta forma, concluímos que a sociabilidade dos objetos pode contribuir para a segurança da rede, ao barrar o acesso de atacantes Sybil, que podem lançar outros ataques e comprometer a privacidade dos dados disseminados, ao contribuir para a sua detecção. O ELECTRON demonstrou que uma detecção efetiva pode ser alcançada com o uso das relações sociais construídas pelos objetos e pela similaridade dentro das comunidades; e portanto sendo possível detectar o ataque Sybil de forma distribuída, escalar e considerando a heterogeneidade dos dispositivos. Ao comparar ELECTRON com mecanismos da literatura como o SA²CI pode-se observar que ELECTRON teve uma maior efetividade em ambiente de até médio porte, o que entretanto, não inviabiliza o uso das relações sociais em ambientes maiores. O uso de técnicas de criptografia de baixa complexidade computacional pode ser uma alternativa para diminuir o número de falsos negativos e obter taxas de detecção maiores. Onde ELECTRON torna-se mais uma camada de segurança para ser empregada na IoT, apoiado por técnicas que garantam a segurança física dos dispositivos. Ao aplicar criptografias e funções anti clonagem, como a função PUF, interceptação de dados transmitidos pode ser evitado, junto a verificação de hardware do dispositivo. Desta forma, o ELECTRON ficaria apenas responsável em lidar com aspectos como o comportamento e inteligência nos dispositivos. Assim, este trabalho contribuiu com a adaptação dos conceitos de relações sociais, encontrados na SIoT, para um ambiente IoT sujeita a ataques Sybil, auxiliando a manter a privacidade na disseminação dos dados e detectando atacantes Sybil que buscam acesso a rede.

6.1 TRABALHOS FUTUROS

A demanda por um serviço eficiente no controle de acesso na IoT continua a crescer e permanece em aberto. Grande parte desta demanda está pautada pelo tipo de dados trafegados na rede, sendo em sua grande maioria dados pessoais dos usuários. Manter a privacidade das informações que circulam na rede é indispensável para o recebimento da IoT no dia-a-dia das pessoas em uma sociedade, seja ela em casa, no escritório, na escola, na academia ou no parque. Por isso, os sistemas, mecanismos ou protocolos devem ser robustos frente a dinamicidade da rede IoT e suas características de infraestrutura. Fornecendo meios de garantir a privacidade nas informações disseminadas na rede.

Por essa razão, todos os cenários e validações devem ser testados ao avaliar os mecanismos de segurança. Com esse intuito, empregar o ELECTRON em um cenário com maiores colisões e perda de pacotes se faz necessário. Implementar o mecanismo com tecnologias como *WiFi*, *ZigBee* e *Bluetooth* proporciona um ambiente com maiores chances de colisão e consequentemente um alto índice de retransmissões. Tanto os valores da confiança social (T_{ij}^{C}),

taxa de detecção (R_d), acurácia (R_a) e taxa de falsos negativos (R_{fn}) podem ser reavaliados de forma a verificar seu real impacto na identificação de atacantes. Entretanto, o principal objetivo consiste em avaliar a taxa de falsos positivos (R_{fp}) nesse cenário, ao analisar se as perdas e retransmissões podem afetar a avaliação do mecanismo sobre os nós legítimos, classificando-os como atacantes. Ao mesmo tempo incorporar técnicas de criptografia de baixa complexidade para melhor a identificação de atacantes que conseguiram alcançar confiança suficiente na rede para enganar o mecanismo, e assim, reduzir o número de falsos negativos.

Da mesma maneira, melhorar a inteligência na tomada de decisão do mecanismo contribui para que um número de atacantes detectados aumente. Isso pode ser obtido apenas fazendo alterações no módulo de Autenticação do mecanismo, e trazendo técnicas com maior base de pesquisa para encarregar-se da decisão do acesso. Uma boa técnica para ser incorporada no módulo é a lógica Fuzzy, por lidar com conceitos como a incerteza e a subjetividade. As funções Fuzzy geram valores nítidos com base em vários outros valores subjetivos e inconclusivos. Classificam-se então os valores nítidos em variáveis linguísticas, que são conjuntos que fornecem uma maneira sistemática de aproximação de fenômenos complexos ou mal definidos. A lógica Fuzzy tem sido aplicada em outros trabalhos para o controle de acesso na IoT, onde os conjuntos de variáveis linguísticas encontram-se definido para avaliar as requisições de acesso. Além disso, outro ponto a se considerar é a associar do ELECTRON com técnicas de *hardware*, de forma a criar variadas camadas de segurança.

REFERÊNCIAS

(2011), N.-. C. (2001). Ns-3 a discrete-event network simulator for internet system. `https://www.nsnam.org`. Accessed: 2018-01-20.

Abbas, S., Merabti, M., Llewellyn-Jones, D. e Kifayat, K. (2013). Lightweight sybil attack detection in manets. *IEEE Systems Journal*, 7(2):236–248.

Abderrahim, O. B., Elhedhili, M. H. e Saidane, L. (2017). Ctms-siot: A context-based trust management system for the social internet of things. Em *13th International Wireless Communications and Mobile Computing Conference (IWCMC 2017)*, páginas 1903–1908.

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 Tutorials*, 17(4):2347–2376.

Alaba, F. A., Othman, M., Hashem, I. A. T. e Alotaibi, F. (2017). Internet of things security: A survey. *Journal of Network and Computer Applications*, 88(Supplement C):10 – 28.

Alduais, N. A. M., Abdullah, J., Jamil, A. e Audah, L. (2016). An efficient data collection and dissemination for iot based wsn. Em *IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, páginas 1–6.

Alenezi, A., Wills, G., Atlam, H. F., Alenezi, A., Walters, R. J., Wills, G. B. e Daniel, J. (2017). Developing an adaptive risk-based access control model for the internet of things. (June).

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. (2011). Siot: Giving a social structure to the internet of things. *IEEE Communications Letters*, 15(11):1193–1195.

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.

Bachi, G., Coscia, M., Monreale, A. e Giannotti, F. (2012). Classifying trust/distrust relationships in online social networks. Em *International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, páginas 552–557.

Berardinelli, G., Manchon, C. N., Deneire, L., Sorensen, T. B., Mogensen, P. e Pajukoski, K. (2009). Turbo receivers for single user mimo lte-a uplink. Em *VTC Spring 2009 - IEEE 69th Vehicular Technology Conference*, páginas 1–5.

Bernal Bernabe, J., Hernandez Ramos, J. L. e Skarmeta Gomez, A. F. (2016). Taciot: Multidimensional trust-aware access control system for the internet of things. *Soft Comput.*, 20(5):1763–1779.

Breese, J. S., Heckerman, D. e Kadie, C. (1998). Empirical analysis of predictive algorithms for collaborative filtering. Em *Proceedings of the Fourteenth Conference on Uncertainty in Artificial Intelligence*, UAI'98, páginas 43–52, San Francisco, CA, USA. Morgan Kaufmann Publishers Inc.

Buyya, R. e Srirama, S. (2019). *Fog and Edge Computing: Principles and Paradigms*. Wiley.

Carrero, M. A., da Silva, R. I., dos Santos, A. L. e Hara, C. S. (2015). An autonomic in-network query processing for urban sensor networks. Em *2015 IEEE Symposium on Computers and Communication (ISCC)*, páginas 968–973. IEEE.

Chakraborty, T., Dalmia, A., Mukherjee, A. e Ganguly, N. (2017). Metrics for community analysis: A survey. *ACM Comput. Surv.*, 50(4):54:1–54:37.

Cheng, P. C., Rohatgi, P., Keser, C., Karger, P. A., Wagner, G. M. e Reninger, A. S. (2007). Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. Em *IEEE Symposium on Security and Privacy (SP '07)*, páginas 222–230.

Cho, E., Myers, S. A. e Leskovec, J. (2011a). Friendship and mobility: user movement in location-based social networks. Em *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining*, páginas 1082–1090. ACM.

Cho, J., Swami, A. e Chen, I. (2011b). A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys Tutorials*, 13(4):562–583.

Cho, J.-H., Chan, K. e Adali, S. (2015). A survey on trust modeling. *ACM Comput. Surv.*, 48(2):28:1–28:40.

Conti, M., Dehghantanha, A., Franke, K. e Watson, S. (2018). Internet of things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78:544 – 546.

ETSI (2017). The european telecommunications standards institute. `http://www.etsi.org/`. Accessed: 2017-12-10.

Evangelista, D., Mezghani, F., Nogueira, M. e Santos, A. (2016a). Evaluation of sybil attack detection approaches in the internet of things content dissemination. Em *Wireless Days (WD 2016)*, páginas 1–6.

Evangelista, D., Silva, E., Nogueira, M. e Santos, A. (2016b). Um controle de associações resistente a ataques sybil para a disseminação segura de conteúdo da iot. Em *13th International Wireless Communications and Mobile Computing Conference (IWCMC 2017)*, páginas 16–29.

Feng, Z., Xu, X., Yuruk, N. e Schweiger, T. A. J. (2007). A novel similarity-based modularity function for graph partitioning. Em *Proceedings of the 9th International Conference on Data Warehousing and Knowledge Discovery*, DaWaK'07, páginas 385–396, Berlin, Heidelberg. Springer-Verlag.

Fernandez-Gago, C., Moyano, F. e Lopez, J. (2017). Modelling trust dynamics in the internet of things. *Inf. Sci.*, 396(C):72–82.

Ferreira, J. L. M. (2014). Segurança em redes sem fio. Monografia de especialização (Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Rede.), UTFPR (Universidade Tecnológica Federal do Paraná), Curitiba, Brazil.

Figueiredo, C. M., dos Santos, A. L., Loureiro, A. A. e Nogueira, J. M. (2005). Policy-based adaptive routing in autonomous WSNs. Em *International Workshop on Distributed Systems: Operations and Management*, páginas 206–219. Springer.

Fleisch, E. (2007). What is the internet of things? an economic perspective. Auto-ID White Paper.

Fortunato, S. (2010). Community detection in graphs. *Physics Reports*, 486(3):75 – 174.

Furlaneto, S. S., Dos Santos, A. L. e Hara, C. S. (2012). An efficient data acquisition model for urban sensor networks. Em *2012 IEEE Network Operations and Management Symposium*, páginas 113–120. IEEE.

Gartner (2017). The gartner report. `https://www.gartner.com/doc/3803530?srcId=1-6595640685`. Accessed: 2017-11-08.

Gielow, F., Jakllari, G., Nogueira, M. e Santos, A. (2015). Data similarity aware dynamic node clustering in wireless sensor networks. *Ad Hoc Networks*, 24:29–45.

Girvan, M. e Newman, M. E. J. (2002). Community structure in social and biological networks. *Proceedings of the National Academy of Sciences of the United States of America*, páginas 7821–7826.

Gusmeroli, S., Piccione, S. e Rotondi, D. (2012). Iot access control issues: A capability based approach. Em *Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, páginas 787–792.

Gusmeroli, S., Piccione, S. e Rotondi, D. (2013). A capability-based security approach to manage access control in the internet of things. *Mathematical and Computer Modelling*, 58(5):1189 – 1205. The Measurement of Undesirable Outputs: Models Development and Empirical Analyses and Advances in mobile, ubiquitous and cognitive computing.

Hang, C.-W. e P Singh, M. (2012). Trust-based recommendation based on graph similarity.

Helgason, O., Kouyoumdjieva, S. T. e Karlsson, G. (2014). Opportunistic communication and human mobility. *IEEE Transactions on Mobile Computing*, 13(7):1597–1610.

Hernández-Ramos, J. L., Jara, A. J., Marín, L. e Skarmeta Gómez, A. F. (2016). Dcapbac: Embedding authorization logic into smart things through ecc optimizations. *Int. J. Comput. Math.*, 93(2):345–366.

Hussein, D., Bertin, E. e Frey, V. (2017). A community-driven access control approach in distributed iot environments. *IEEE Communications Magazine*, 55(3):146–153.

Jayasinghe, U., Truong, N. B., Lee, G. M. e Um, T. W. (2016). Rpr: A trust computation model for social internet of things. Em *2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, páginas 930–937.

Jøsang, A., Hayward, R. e Pope, S. (2006). Trust network analysis with subjective logic. Em *Proceedings of the 29th Australasian Computer Science Conference-Volume 48*, páginas 85–94. Australian Computer Society, Inc.

Jøsang, A. (1997). Artificial reasoning with subjective logic.

Khan, Z. A. e Herrmann, P. (2017). A trust based distributed intrusion detection mechanism for internet of things. Em *IEEE 31st International Conference on Advanced Information Networking and Applications (AINA 2017)*, páginas 1169–1176.

Kouyoumdjieva, S. T., Ólafur Ragnar Helgason e Karlsson, G. (2014). CRAWDAD dataset kth/walkers (v. 2014-05-05). Downloaded from `https://crawdad.org/kth/walkers/20140505`.

Kowshalya, A. M. e Valarmathi, M. L. (2017). Trust management in the social internet of things. *Wireless Personal Communications*, 96(2):2681–2691.

Krco, S., Pokric, B. e Carrez, F. (2014). Designing iot architecture(s): A european perspective. Em *2014 IEEE World Forum on Internet of Things (WF-IoT)*, páginas 79–84.

Le, V.-D., Scholten, H. e Havinga, P. (2012). Unified routing for data dissemination in smart city networks. Em *3rd IEEE International Conference on the Internet of Things*, páginas 175–182.

Li, S., Xu, L. D. e Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, 17(2):243–259.

Li, X., Lu, R., Liang, X., Shen, X., Chen, J. e Lin, X. (2011). Smart community: an internet of things application. *IEEE Communications Magazine*, 49(11):68–75.

Liben-Nowell, D. e Kleinberg, J. (2003). The link prediction problem for social networks. Em *Proceedings of the Twelfth International Conference on Information and Knowledge Management*, CIKM '03, páginas 556–559, New York, NY, USA. ACM.

Lima, M. N., dos Santos, A. L. e Pujolle, G. (2009). A survey of survivability in mobile ad hoc networks. *IEEE Communications Surveys and Tutorials*, 11(1):66–77.

Lin, X. (2013). Lsr: Mitigating zero-day sybil vulnerability in privacy-preserving vehicular peer-to-peer networks. 31:237–246.

Liu, J., Xiao, Y. e Chen, C. L. P. (2012). Authentication and access control in the internet of things. Em *32nd International Conference on Distributed Computing Systems Workshops*, páginas 588–592.

Mahalle, P. N., Thakre, P. A., Prasad, N. R. e Prasad, R. (2013). A fuzzy approach to trust based access control in internet of things. Em *Wireless VITAE 2013*, páginas 1–5.

Mannes, E., Nogueira, M. e Santos, A. (2012a). A bio-inspired scheme on quorum systems for reliable services data management in MANETs. Em *2012 IEEE Network Operations and Management Symposium*, páginas 278–285. IEEE.

Mannes, E., Nogueira, M. e Santos, A. (2012b). Reliable operational services in MANETs by misbehavior-tolerant quorum systems. Em *Proceedings of the 8th International Conference on Network and Service Management*, páginas 343–349. International Federation for Information Processing.

Marsh, S. P. (1994). Formalising trust as a computational concept. Relatório técnico, University of Stirling.

McKnight, D. H., Cummings, L. L. e Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management review*, 23(3):473–490.

Medjek, F., Tandjaoui, D., Romdhani, I. e Djedjig, N. (2017). Performance evaluation of rpl protocol under mobile sybil attacks. Em *IEEE Trustcom/BigDataSE/ICESS*, páginas 1049–1055.

Meissner, S. e Walewski, J. W. (2013). *Guidance to the ARM: Overview*, páginas 39–44. Springer Berlin Heidelberg, Berlin, Heidelberg.

Nath, S. V. (2017). *IoT ARCHITECTURE*, páginas 239–249. John Wiley and Sons, Inc.

Ouaddah, A., Mousannif, H., Elkalam, A. A. e Ouahman, A. A. (2017). Access control in the internet of things: Big challenges and new opportunities. *Computer Networks*, 112:237 – 262.

Parwekar, P. (2011). From internet of things towards cloud of things. Em *2nd International Conference on Computer and Communication Technology (ICCCT-2011)*, páginas 329–333.

Perrone, L. F. e Nelson, S. C. (2006). A study of on-off attack models for wireless ad hoc networks. Em *1st Workshop on Operator-Assisted (Wireless Mesh) Community Networks*, páginas 1–10.

Pongle, P. e Chavan, G. (2015). A survey: Attacks on rpl and 6lowpan in iot. Em *2015 International Conference on Pervasive Computing (ICPC)*, páginas 1–6.

Quercia, D. e Hailes, S. (2010). Sybil attacks against mobile users: Friends and foes to the rescue. Em *Proceedings IEEE INFOCOM*, páginas 1–5.

Rajan, A., Jithish, J. e Sankaran, S. (2017). Sybil attack in iot: Modelling and defenses. Em *International Conference on Advances in Computing, Communications and Informatics (ICACCI 2017)*, páginas 2323–2327.

Sethi, M., Kortoçi, P., Francesco, M. D. e Aura, T. (2015). Secure and low-power authentication for resource-constrained devices. Em *5th International Conference on the Internet of Things (IOT)*, páginas 30–36.

Shaikh, R. A., Adi, K. e Logrippo, L. (2012). Dynamic risk-based decision methods for access control systems. *Comput. Secur.*, 31(4):447–464.

Sicari, S., Rizzardi, A., Grieco, L. e Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, 76(Supplement C):146 – 164.

Solhaug, B., Elgesem, D. e Stolen, K. (2007). Why trust is not proportional to risk. Em *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, páginas 11–18.

Son, H., Kang, N., Gwak, B. e Lee, D. (2017). An adaptive iot trust estimation scheme combining interaction history and stereotypical reputation. Em *14th IEEE Annual Consumer Communications Networking Conference (CCNC 2017)*, páginas 349–352.

Truong, N., Lee, H., Askwith, B. e Lee, G. M. (2017). Toward a trust evaluation mechanism in the social internet of things. 17:1346.

Valarmathi, M. L., Meenakowshalya, A. e Bharathi, A. (2016). Robust sybil attack detection mechanism for social networks - a survey. Em *3rd International Conference on Advanced Computing and Communication Systems (ICACCS 2016)*, volume 01, páginas 1–5.

Vasseur, J. e Dunkels, A. (2010). *Interconnecting Smart Objects with IP: The Next Internet*. Elsevier Science.

Wallgren, L., Raza, S. e Voigt, T. (2013). Routing attacks and countermeasures in the rpl-based internet of things. 2013.

Weyrich, M. e Ebert, C. (2016). Reference architectures for the internet of things. *IEEE Software*, 33(1):112–116.

Wortmann, F. e Flüchter, K. (2015). Internet of things. *Business & Information Systems Engineering*, 57(3):221–224.

Yan, Z., Zhang, P. e Vasilakos, A. V. (2014). A survey on trust management for internet of things. *Journal of Network and Computer Applications*, 42:120 – 134.

Yang, Z., Fan, Y. e Zhang, B. (2010). A fusion model of overall trust relationship from multiple attributes in trusted networks based on dynamic entropy gain. Em *IEEE International Conference on Information Theory and Information Security*, páginas 323–326.

Zhang, K., Liang, X., Lu, R. e Shen, X. (2014). Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal*, 1(5):372–383.

APÊNDICE A – RESULTADOS COMPLEMENTARES DA AVALIAÇÃO

Neste apêndice encontram-se os resultados complementares da simulação dos mecanismos ELECTRON e SA²CI no NS-3. Em razão do grande volume de gráficos gerados na simulação e de modo a não criar uma discussão extensa no Capítulo 5, os gráficos da foram alocados para este capítulo. A primeira seção traz os resultados complementares do ELECTRON para a percepção social e, logo em seguida, os resultados complementares para a percepção de segurança dos mecanismos ELECTRON e SA²CI. Os gráficos presentes neste apêndice compreendem a simulação completa com 200 nós, onde todos os comportamentos do ataque Sybil estão presentes. Além da simulação com 200 nós, os resultados complementares da simulação com 100 e 150 nós encontram-se a seguir, isto é, com os resultados dos ataques de múltiplas identidades roubadas e fabricadas e o comportamento *churn* com identidades fabricadas. A forma de demonstração dos resultados segue a do Capítulo 5, onde os resultados encontram-se separados pela percepção social empregada no mecanismo e pela eficácia da segurança, no qual avalia-se a contribuição da confiança social para preservação da privacidade.

A.1 ELECTRON - ANÁLISE DA PERCEPÇÃO SOCIAL

Na análise da percepção social, os gráficos demonstrando a evolução da confiança social (T_{ij}^{C}) em uma CDF e no gráfico *boxplot*. As figuras iniciais referem-se a simulação com 200 nós, demonstrando a evolução da confiança social em uma CDF sob a seguinte sequência do comportamento do atacante: *(i)* múltiplas identidades roubadas, *(ii)* múltiplas identidades roubadas, *(iii) churn* com identidades roubadas e *(iv) churn* com identidades fabricadas. Entre as Figuras A.1-A.4 destaca-se o comportamento da confiança social entre os nós externos, onde a confiança social permanece menos instável, sofrendo grandes alterações como a observada no simulação com 100 nós. Em seguida as Figuras A.5-A.7 complementam os dados da simulação com 150 nós, assim como as Figuras A.8-A.10 completam os resultados da simulação com 100 nós. Os gráficos *boxplot* da simulação com 200 nós se encontram entre as Figuras A.11-A.14 representando a dispersão dos dados da confiança social na simulação. Em fim, as Figuras A.15-A.17 e A.18-A.20 demonstram os gráficos *boxplot* da confiança social das simulações 150 e 100 nós respectivamente.

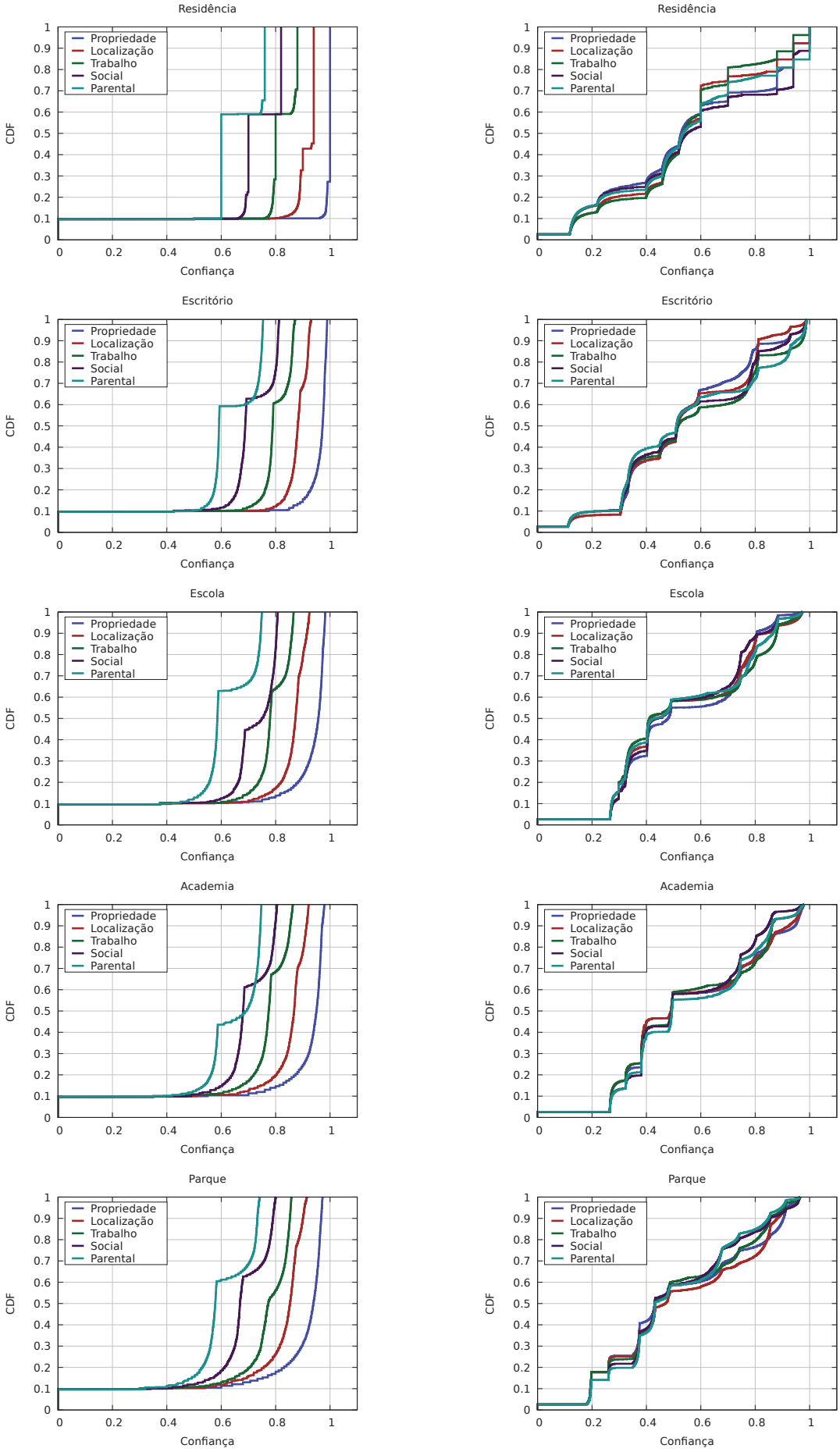


Figura A.1: Evolução da confiança social com 200 nós e ataque múltiplas id. roubadas

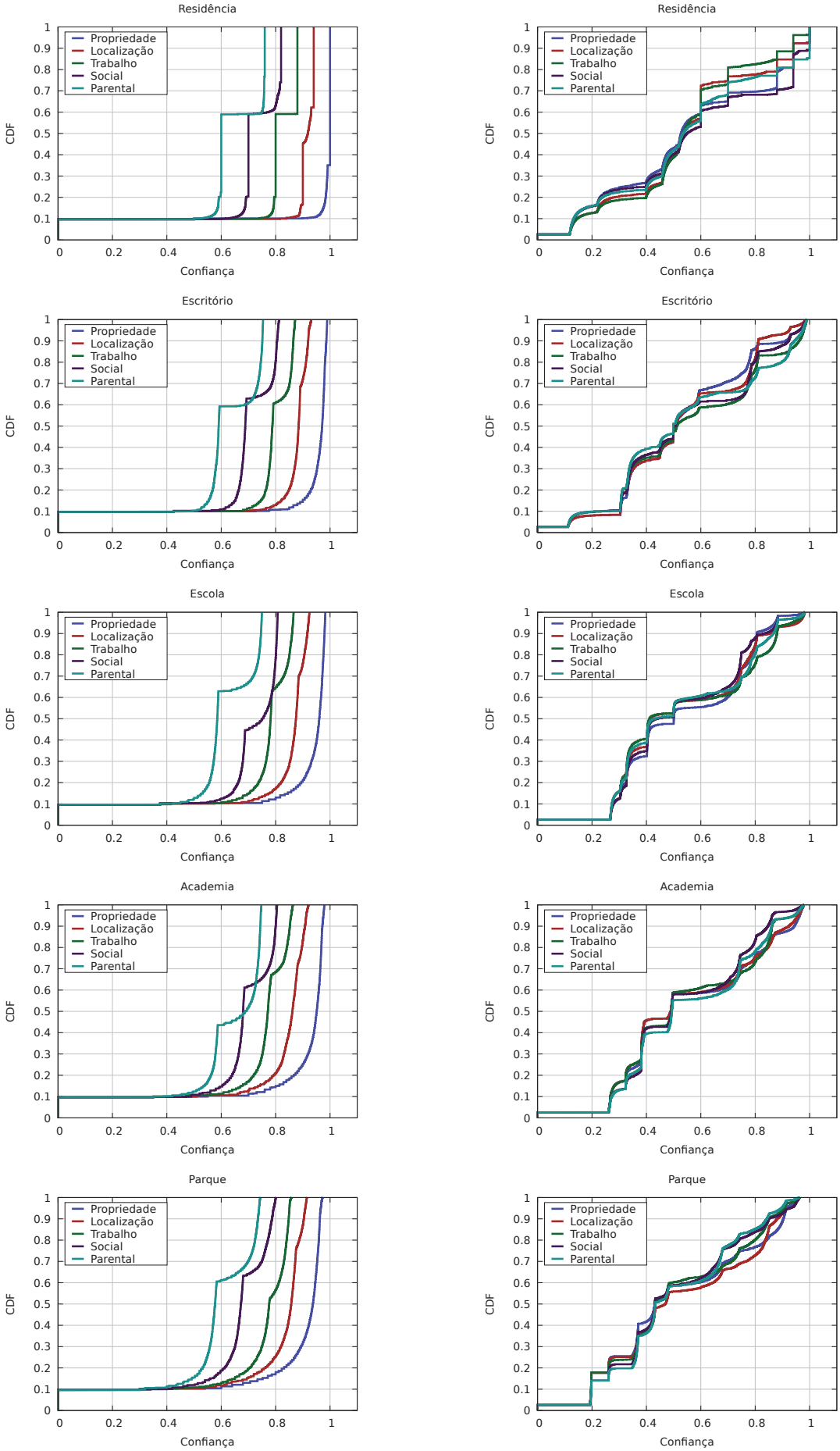


Figura A.2: Evolução da confiança social com 200 nós e ataque múltiplas id. fabricadas

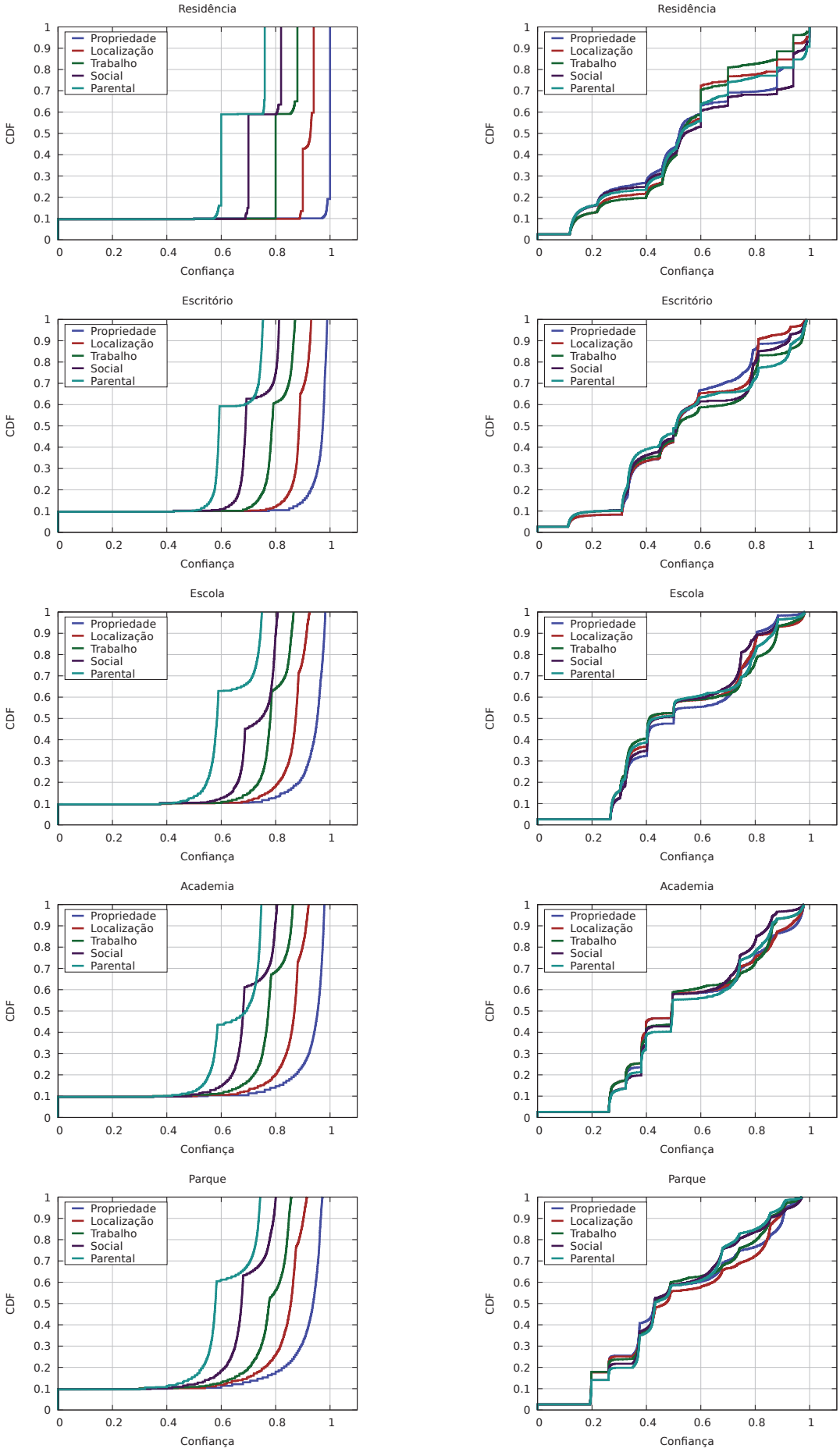


Figura A.3: Evolução da confiança social com 200 nós e ataque churn roubadas

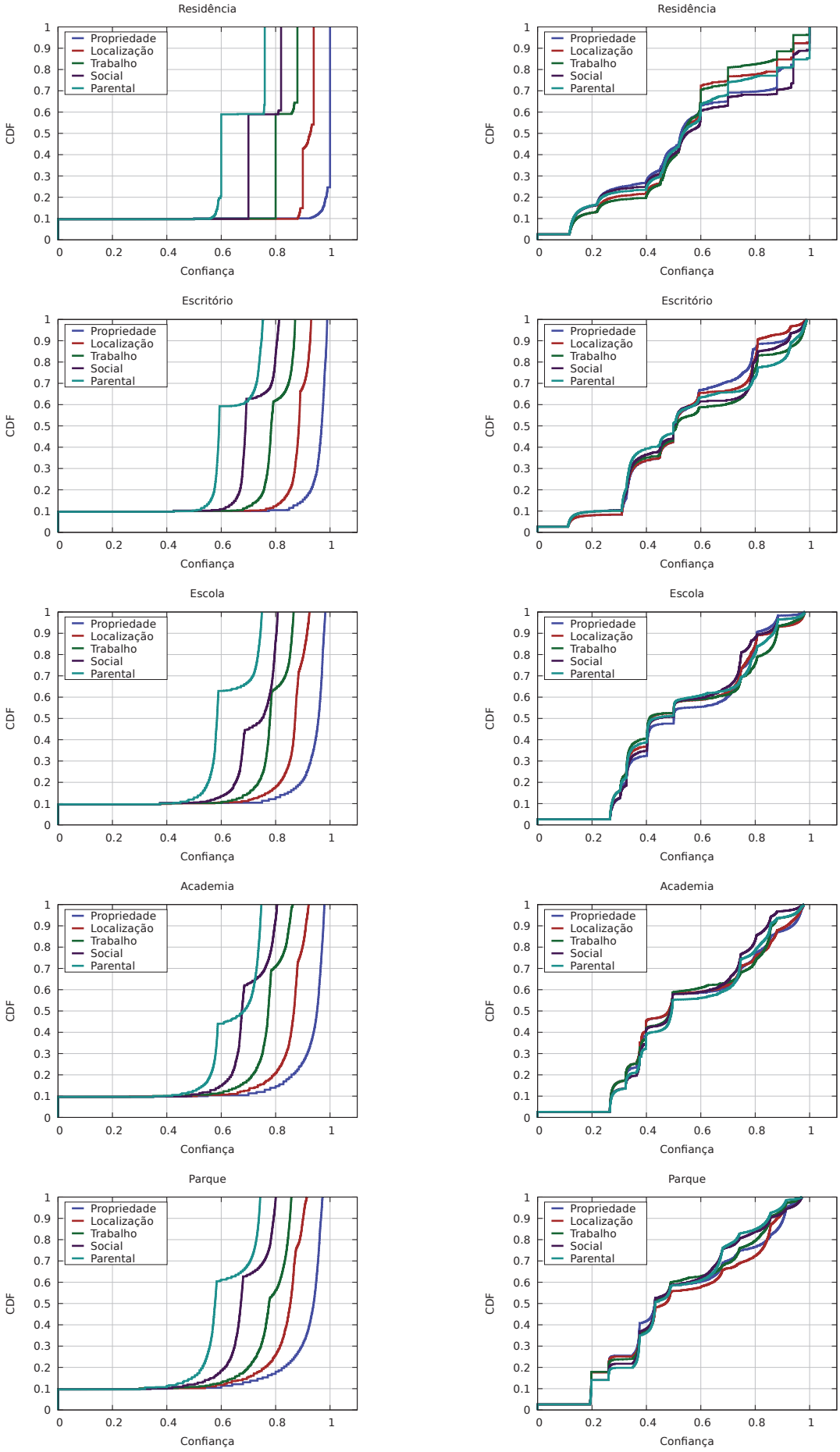


Figura A.4: Evolução da confiança social com 200 nós e ataque churn fabricadas

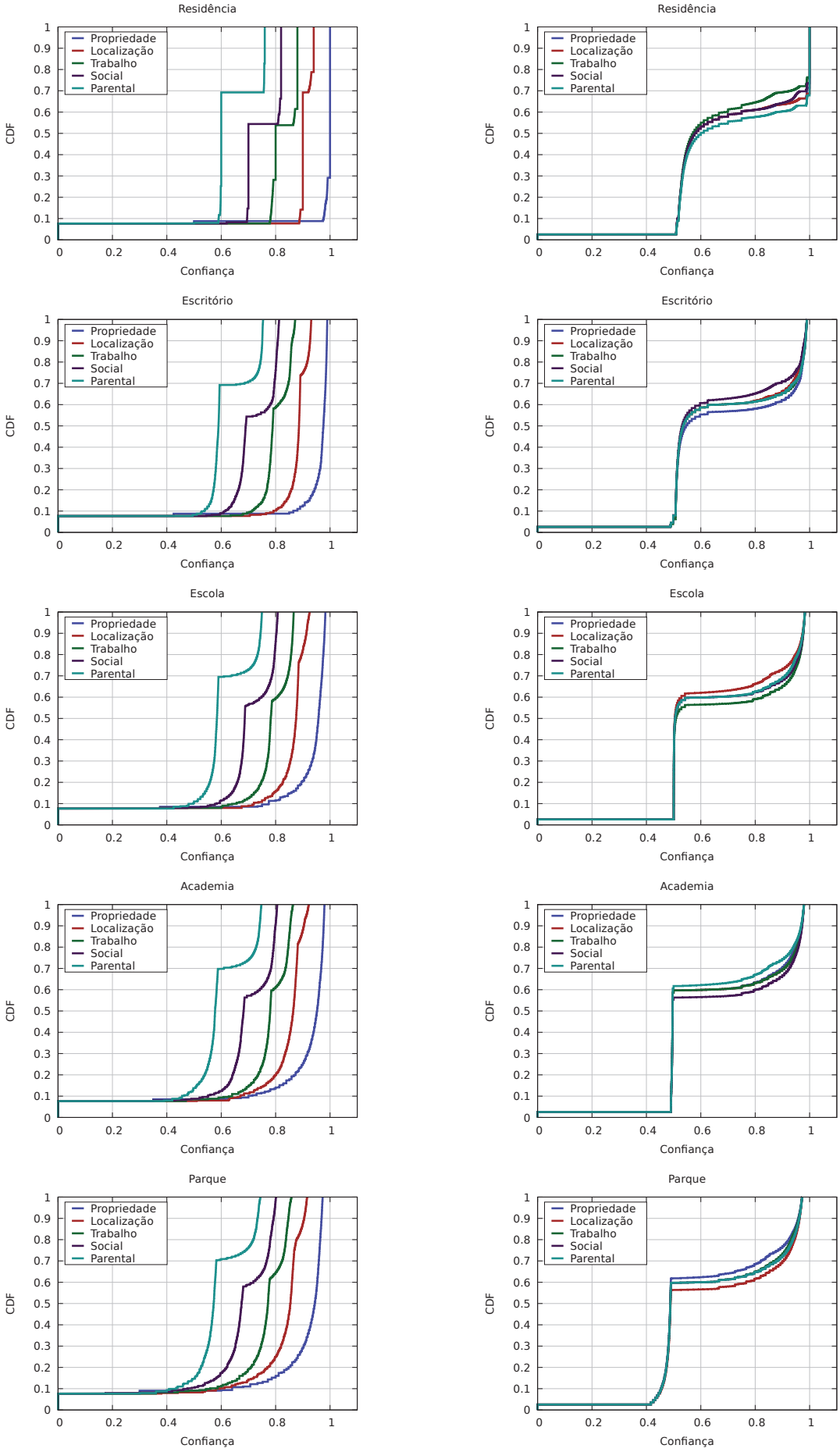


Figura A.5: Evolução da confiança social com 150 nós e ataque múltiplas id. roubadas

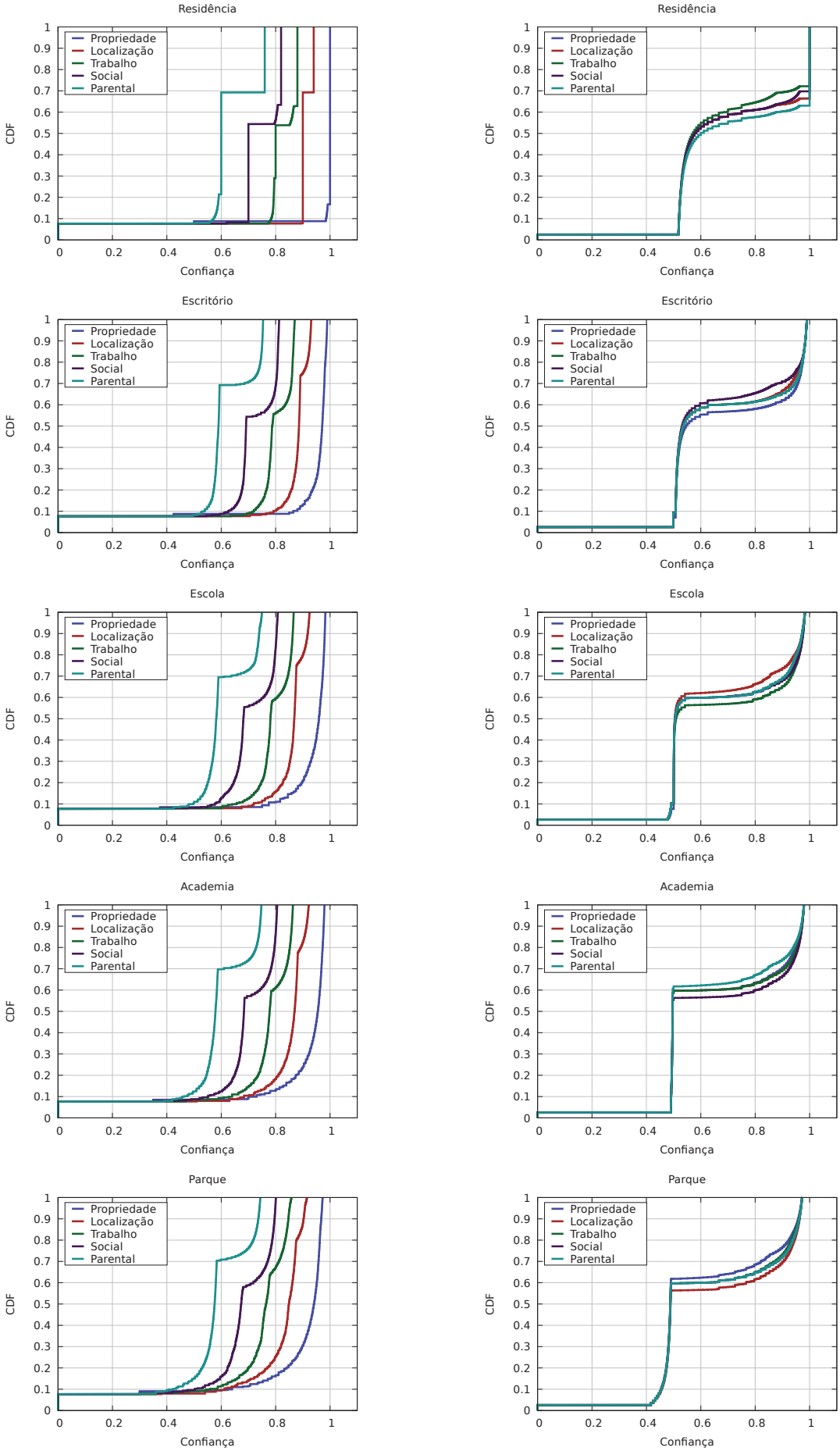


Figura A.6: Evolução da confiança social com 150 nós e ataque múltiplas id. fabricadas

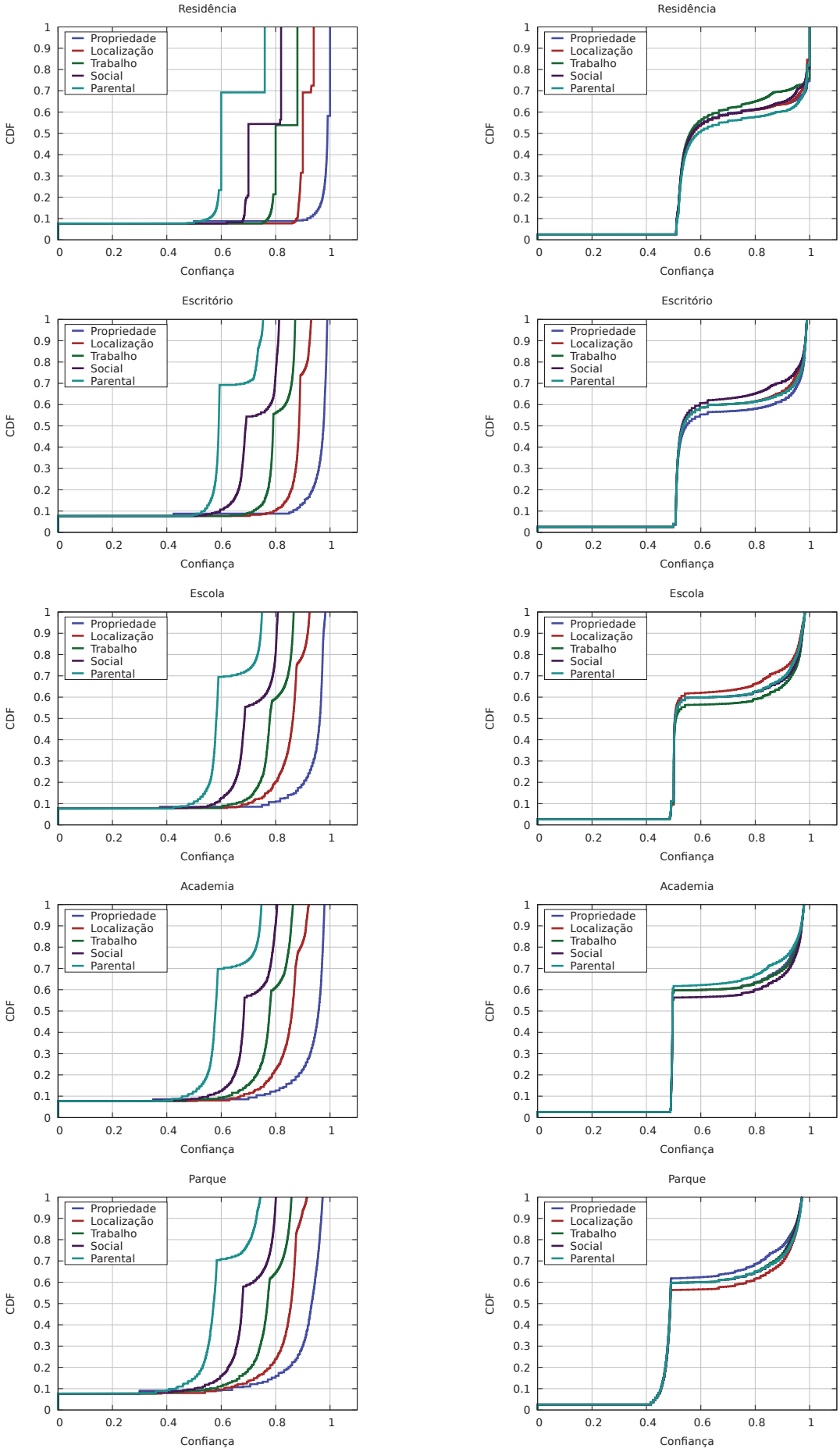


Figura A.7: Evolução da confiança social com 150 nós e ataque churn fabricadas

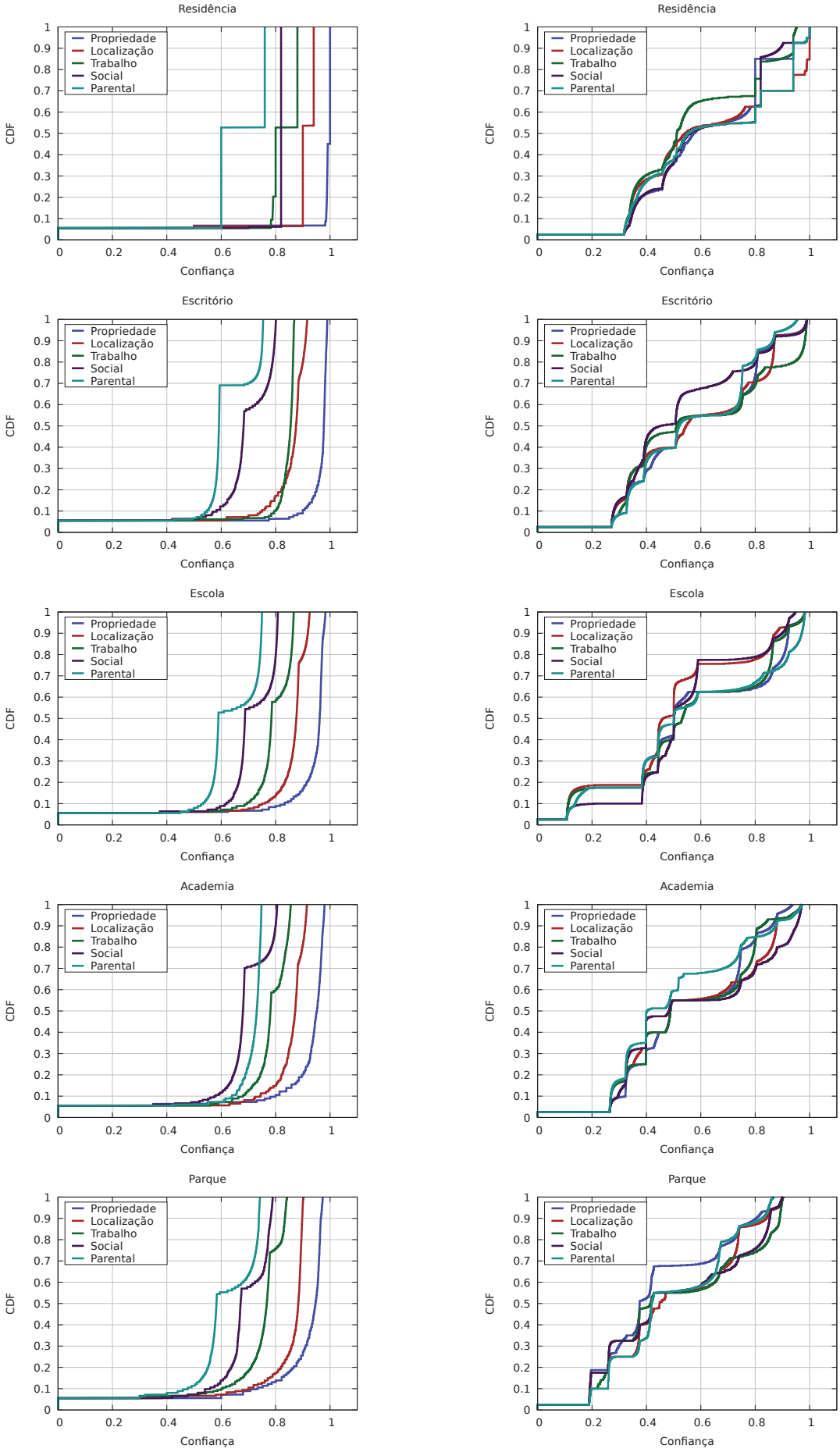


Figura A.8: Evolução da confiança social com 100 nós e ataque múltiplas id. roubadas

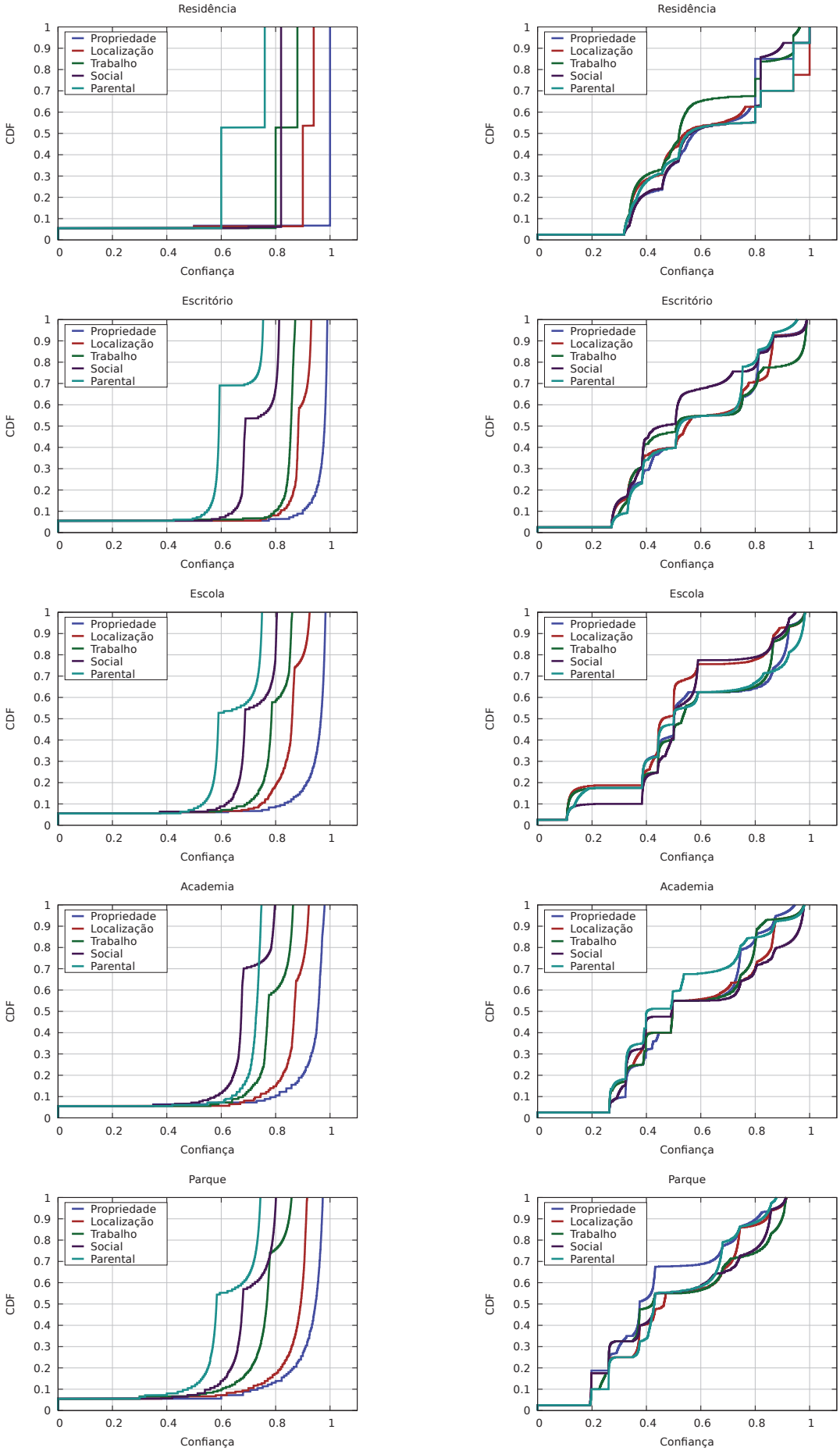


Figura A.9: Evolução da confiança social com 100 nós e ataque múltiplas id. fabricadas

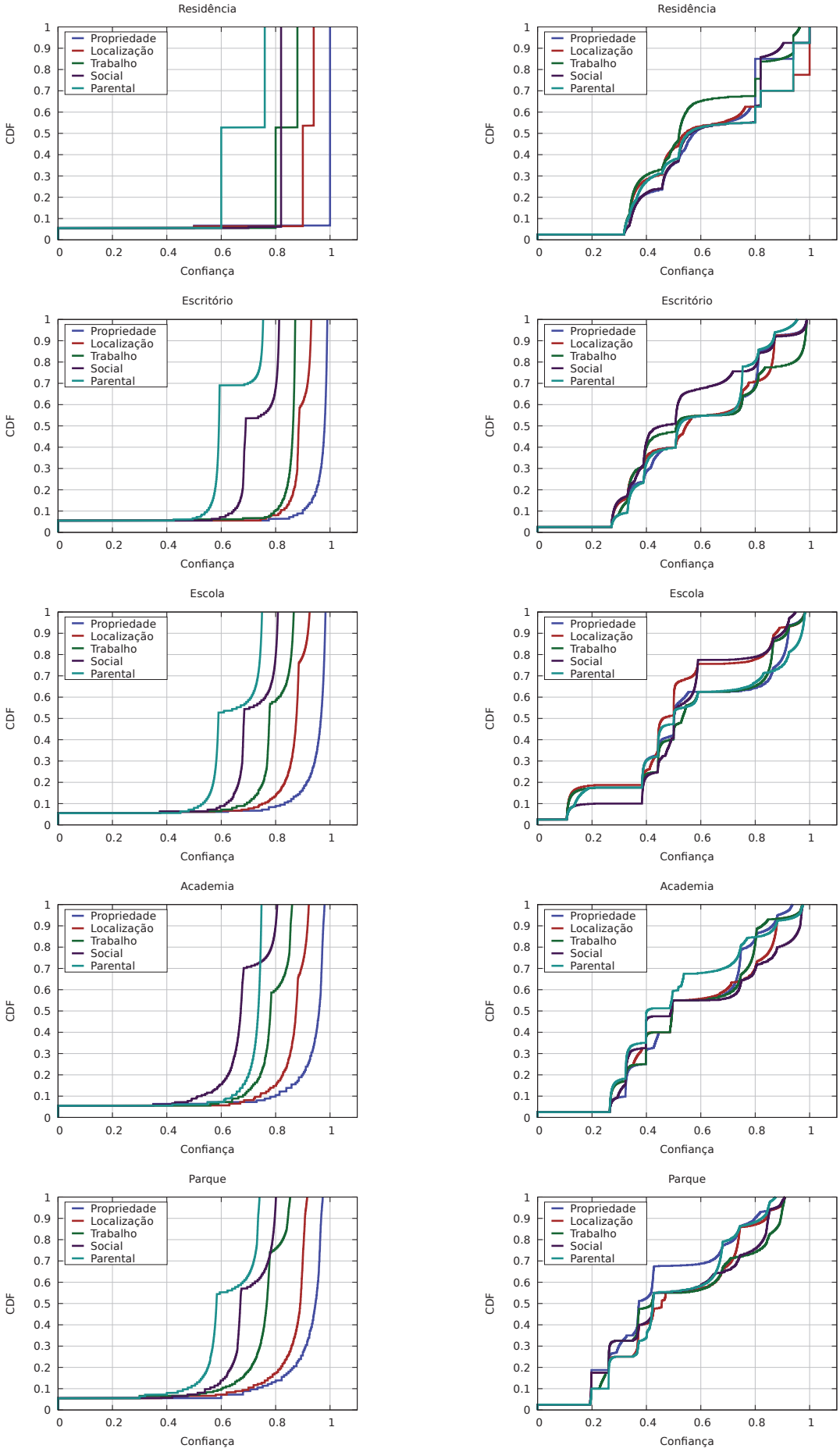


Figura A.10: Evolução da confiança social com 100 nós e ataque churn fabricadas

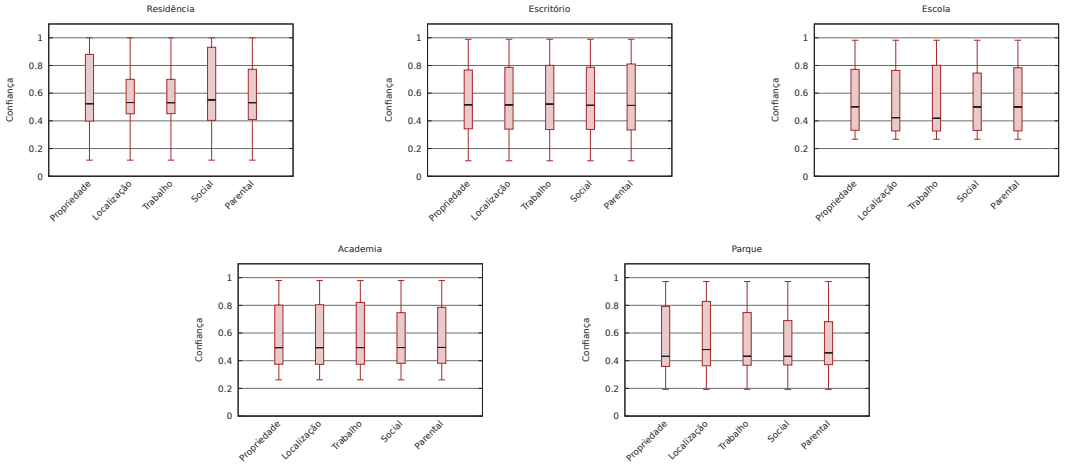


Figura A.11: Variação da confiança social com 200 nós e ataque de múltiplas id. roubadas

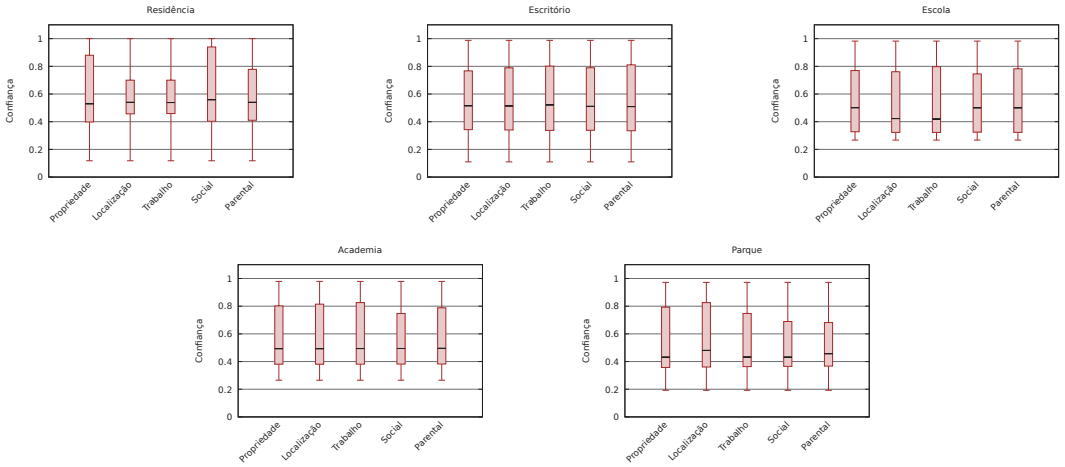


Figura A.12: Variação da confiança social com 200 nós e ataque de múltiplas id. fabricadas

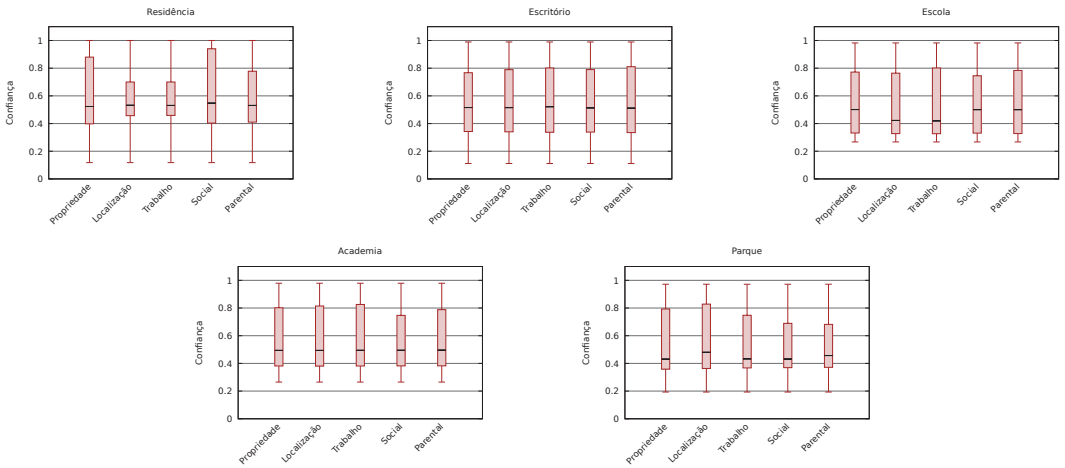


Figura A.13: Variação da confiança social com 200 nós e ataque de churn roubadas

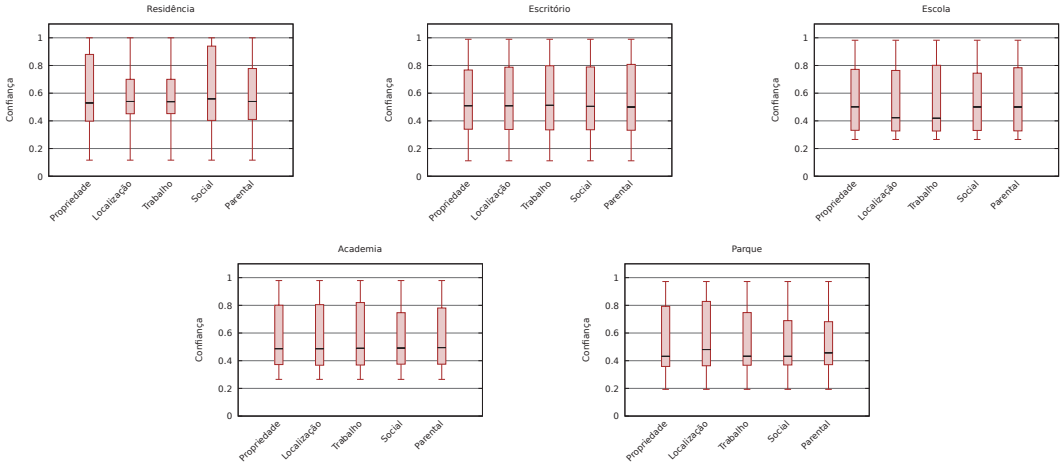


Figura A.14: Variação da confiança social com 200 nós e ataque de churn fabricadas

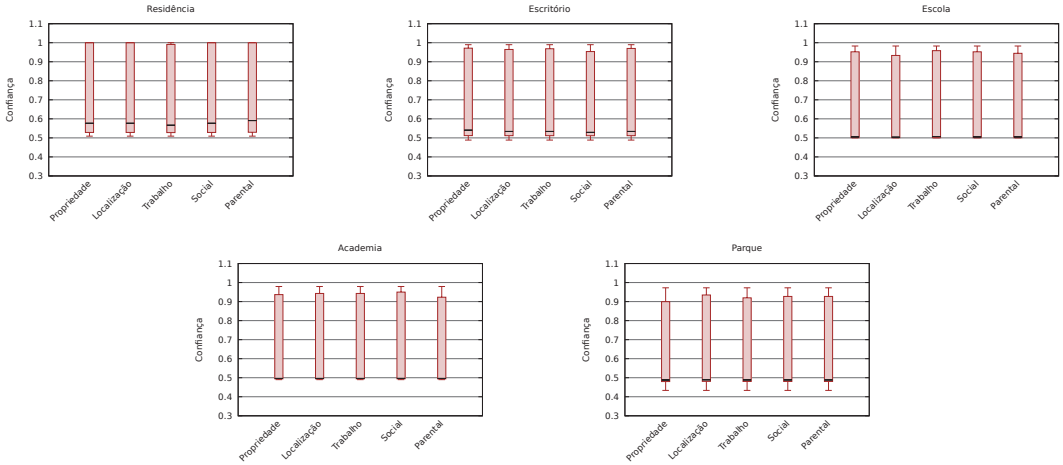


Figura A.15: Variação da confiança social com 150 nós e ataque de múltiplas id. roubadas

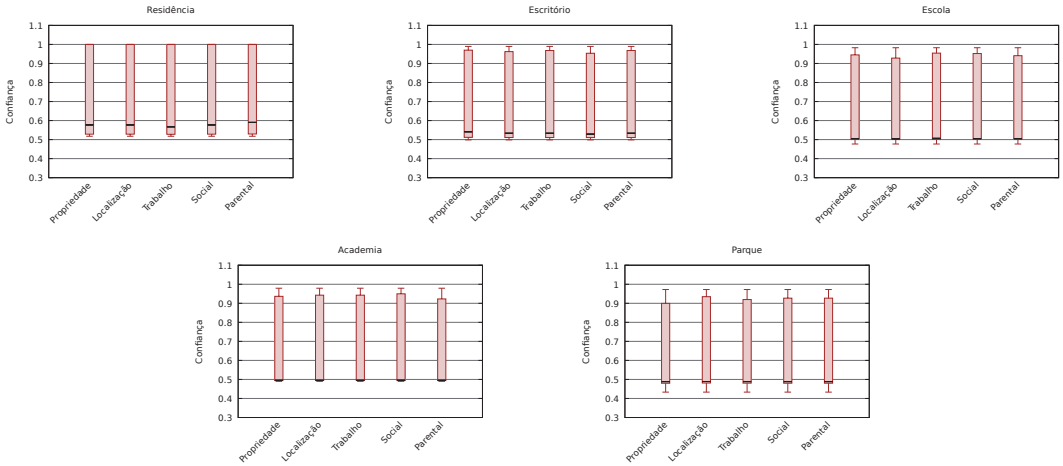


Figura A.16: Variação da confiança social com 150 nós e ataque de múltiplas id. fabricadas

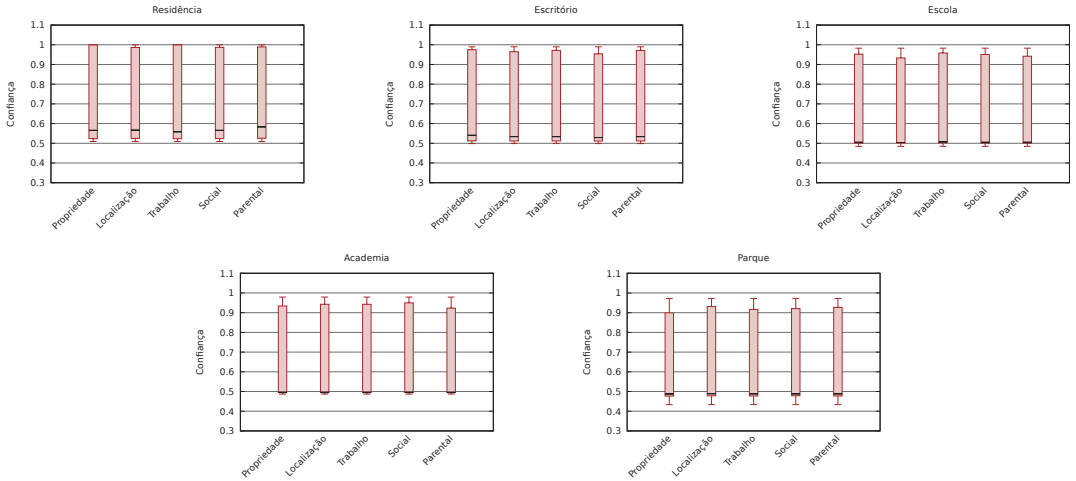


Figura A.17: Variação da confiança social com 150 nós e ataque de churn fabricadas

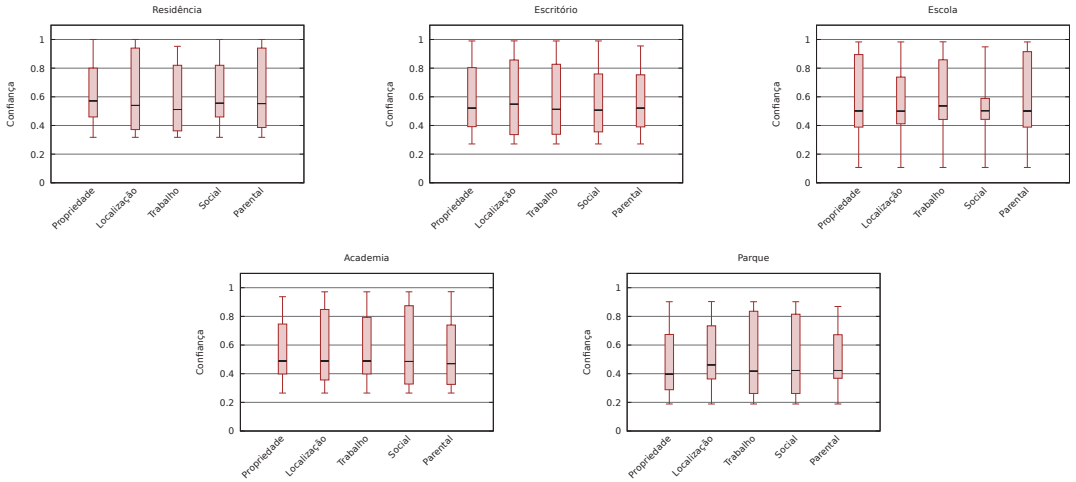


Figura A.18: Variação da confiança social com 100 nós e ataque de múltiplas id. roubadas

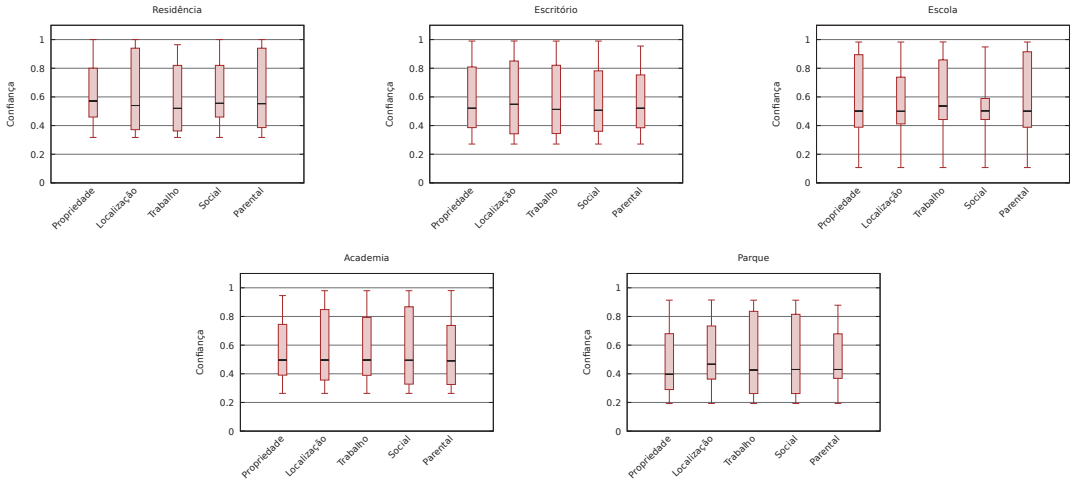


Figura A.19: Variação da confiança social com 100 nós e ataque de múltiplas id. fabricadas

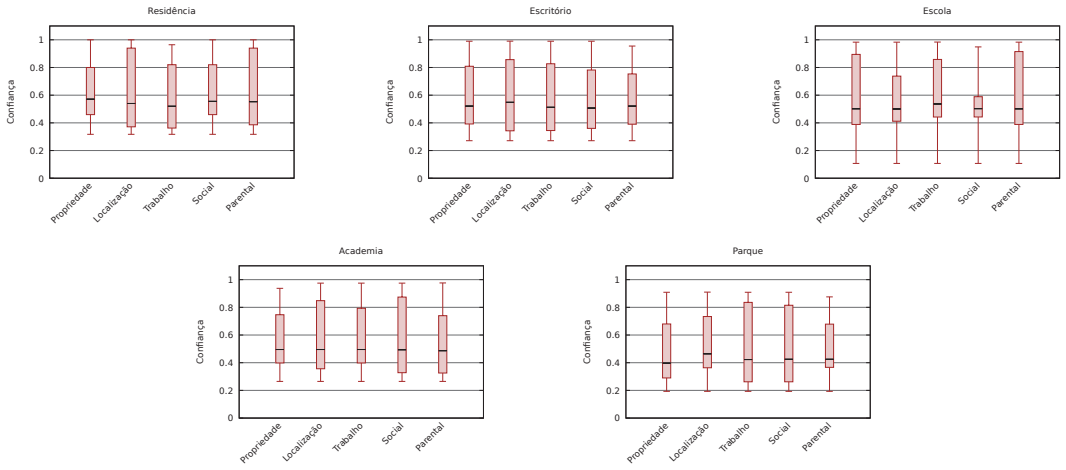
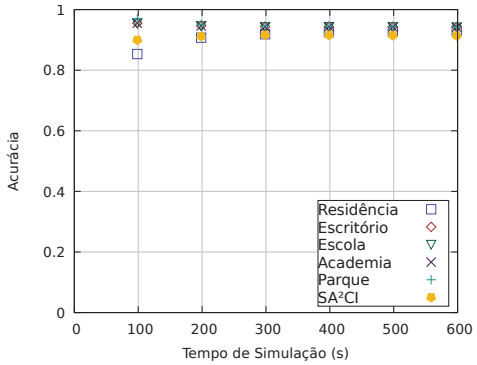


Figura A.20: Variação da confiança social com 100 nós e ataque de churn fabricadas

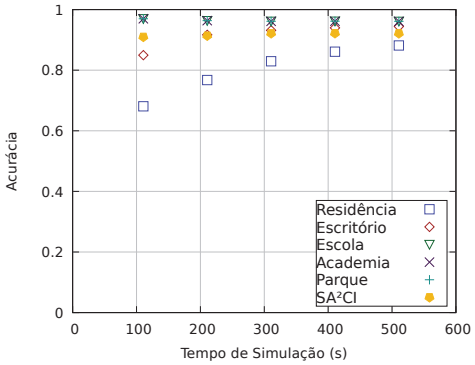
A.2 ELECTRON - ANÁLISE DA EFICÁCIA DA SEGURANÇA

Esta seção descreve os resultados referentes a eficácia da segurança dos mecanismos ELECTRON e SA²CI ao detectar o ataque Sybil. Primeiramente demonstra-se a acurácia (R_a), em seguida a taxa de falsos negativos (R_{fn}) e a taxa de falsos positivos (R_{fp}). Os dados das simulações de 100, 150 e 200 nós estão agrupados pelo tipo de ataque e o gráfico do ataque *churn* com identidades roubadas para a simulação de 200 nós ao fim, pois não foi exibido no Capítulo 5.

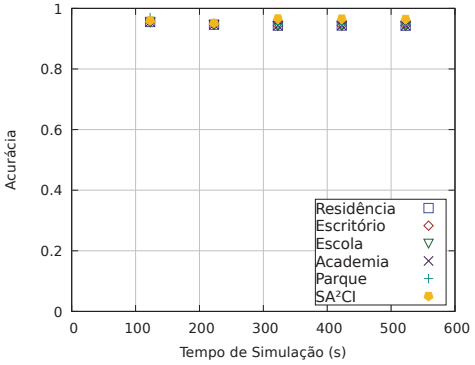
Para complementar as informações da taxa de detecção do ataque, denota-se os valores da acurácia da detecção nas Figuras A.21-A.23. Assim como verificado na detecção do ataque, a acurácia sofre uma maior queda na simulação de 100 e 150 nós, indicando que a combinação numérica de nós obteve maior dificuldade para avaliar precisamente a confiança, enquanto a simulação com 200 nós obteve maior estabilidade em todas as comunidades. A Figura A.24 para o ataque *churn* com identidades roubadas na simulação com 200 nós. Enfim, as duas últimas métricas correspondem a taxa de falsos negativos, entre as Figuras A.25-A.27 e a Figura A.28 para a simulação com 200 nós para o ataque *churn* com identidades roubadas, e os falsos positivos na Figura A.29. Ao analisar os falsos negativos da mecanismo ELECTRON, percebe-se que segue o mesmo comportamento da taxa de detecção e acurácia, alcançando valores de 80% no início da simulação e estabilizando em 22% ao final para a comunidade Residência. Ao focar na taxa com 200 nós observa-se uma constância de 10% nos falsos negativos. Por outro lado, a taxa de falsos positivos manteve-se em 0% para todos os comportamentos de ataque e para todas as simulações, mostrando que em nenhuma circunstância do cenário montado o mecanismo classificou nós legítimos como atacantes.



(a) 100 nós

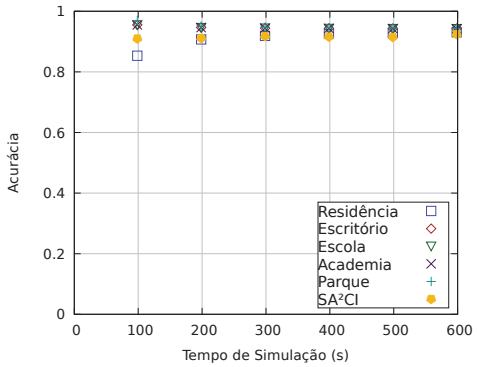


(b) 150 nós

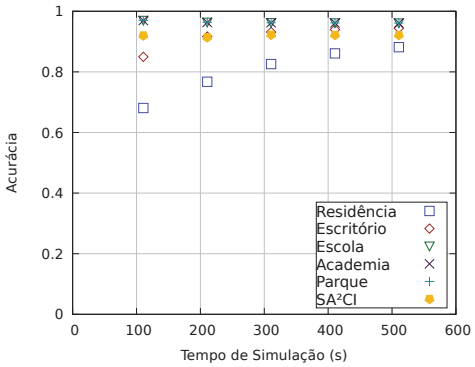


(c) 200 nós

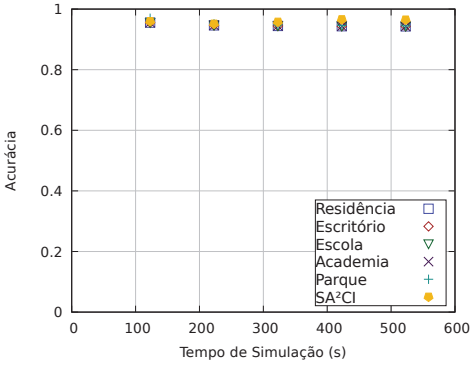
Figura A.21: Acurácia da detecção com ataque múltiplas id. roubadas



(a) 100 nós

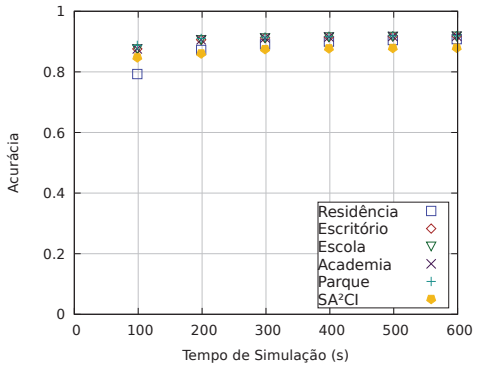


(b) 150 nós

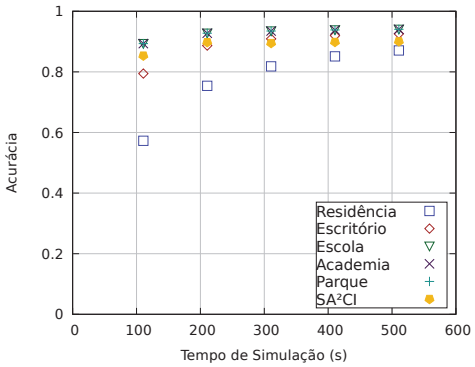


(c) 200 nós

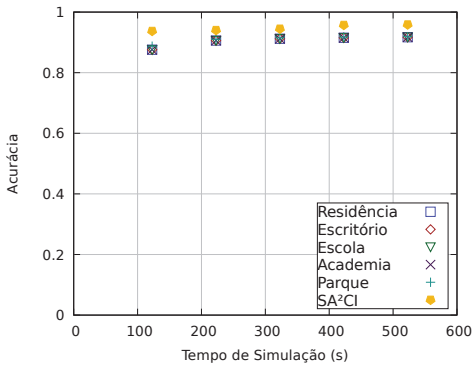
Figura A.22: Acurácia da detecção com ataque múltiplas id. fabricadas



(a) 100 nós



(b) 150 nós



(c) 200 nós

Figura A.23: Acurácia da detecção com ataque churn com id. fabricadas

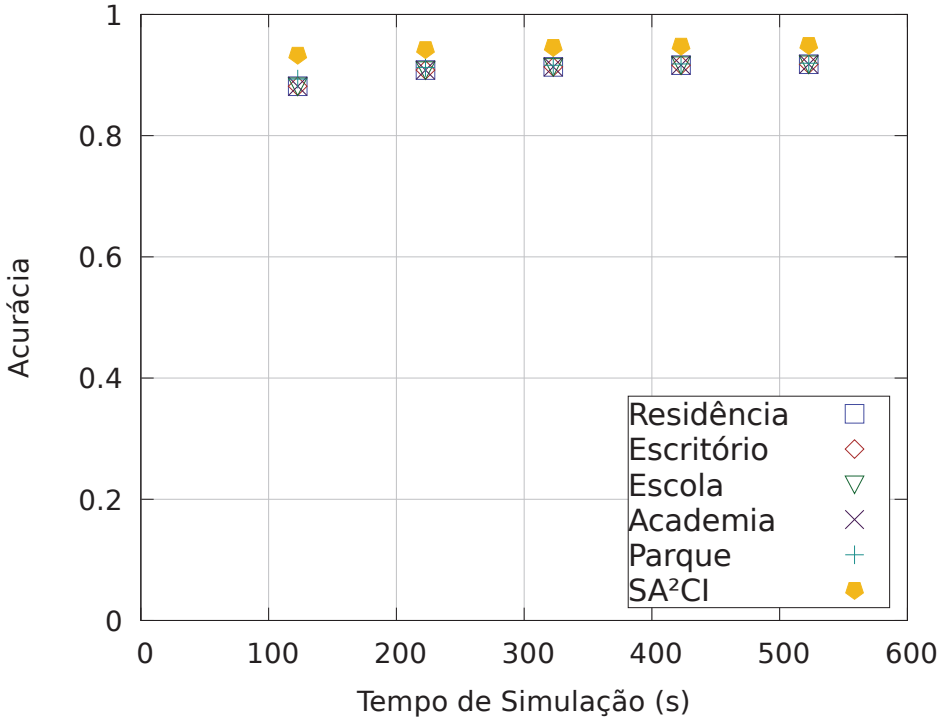
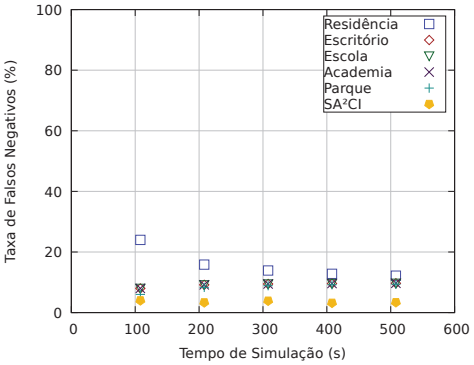
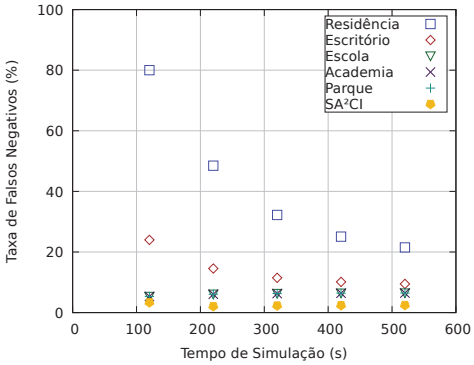


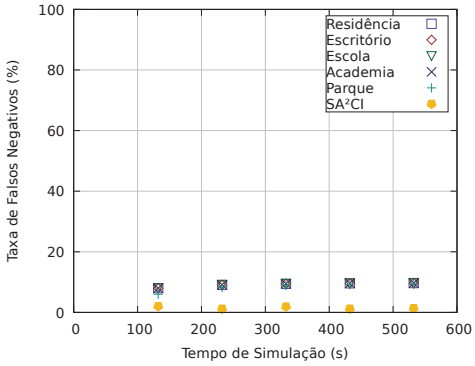
Figura A.24: Acurácia da detecção com ataque churn com id. roubadas 200 nós



(a) 100 nós

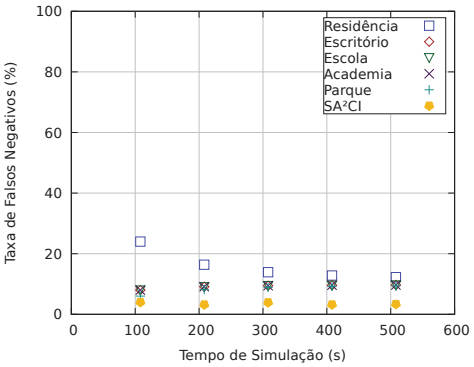


(b) 150 nós

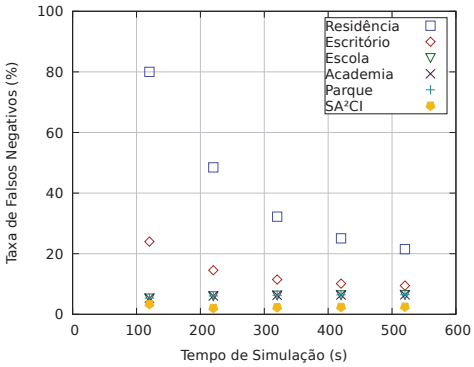


(c) 200 nós

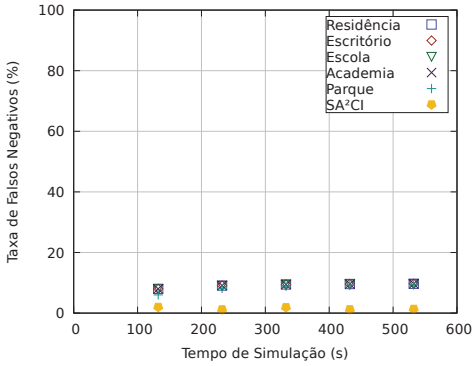
Figura A.25: Taxa de falsos negativos com ataque de múltiplas id. roubadas



(a) 100 nós

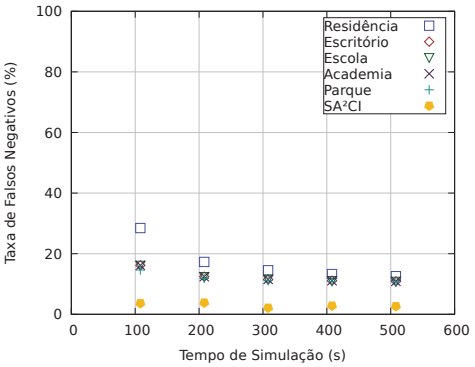


(b) 150 nós

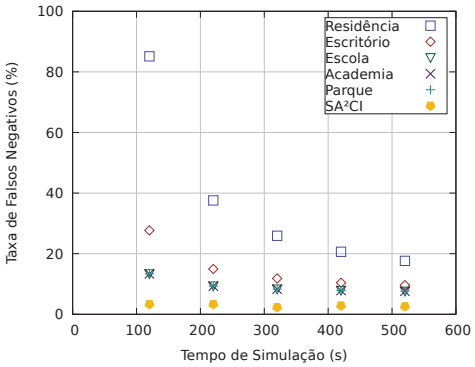


(c) 200 nós

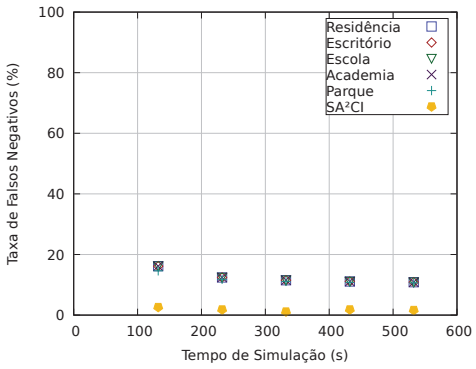
Figura A.26: Taxa de falsos negativos com ataque de múltiplas id. fabricadas



(a) 100 nós



(b) 150 nós



(c) 200 nós

Figura A.27: Taxa de falsos negativos com ataque churn id. fabricadas

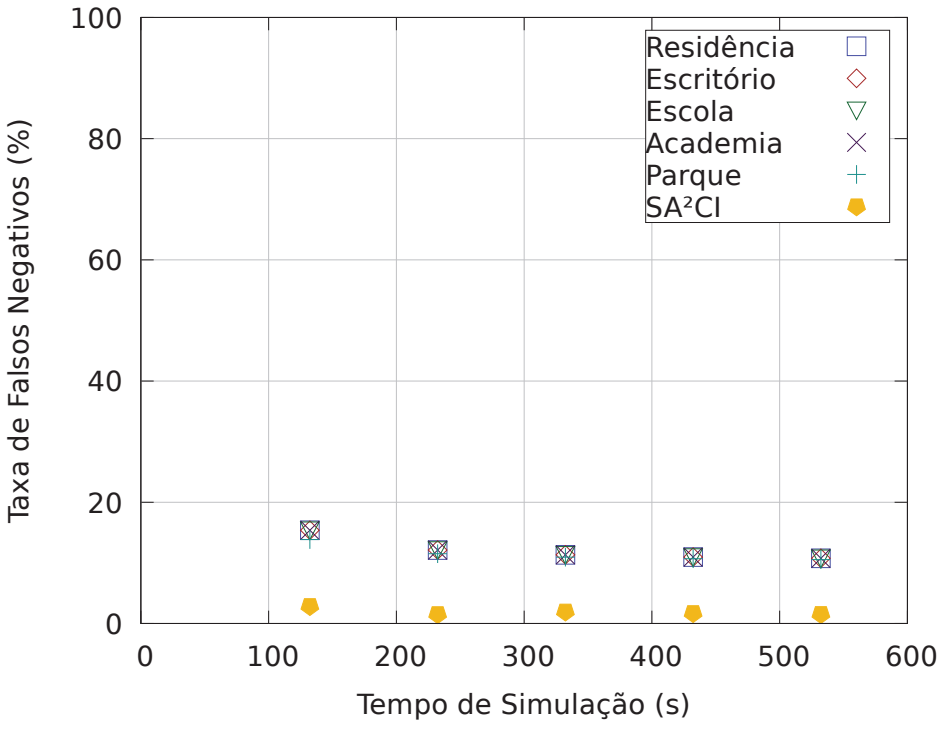
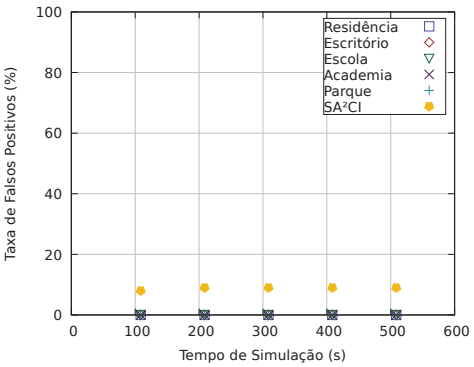
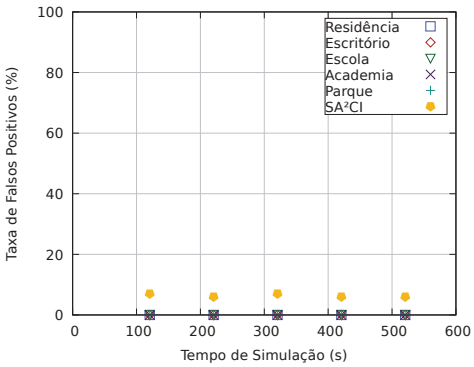


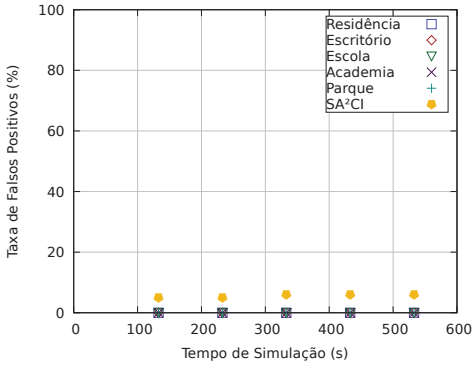
Figura A.28: Taxa de falsos negativos com ataque churn com id. roubadas 200 nós



(a) 100 nós



(b) 150 nós



(c) 200 nós

Figura A.29: Taxa de falsos positivos em todos os comportamentos do ataque