DANILO DE FARIA REIS EVANGELISTA

DISSEMINAÇÃO SEGURA DE CONTEÚDO DIANTE DE ATAQUES SYBIL PARA A INTERNET DAS COISAS

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre. Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.

Orientador: Prof. Aldri Luiz dos Santos
Coorientadora: Profa. Michele Nogueira Lima

CURITIBA

2016

DANILO DE FARIA REIS EVANGELISTA

DISSEMINAÇÃO SEGURA DE CONTEÚDO DIANTE DE ATAQUES SYBIL PARA A INTERNET DAS COISAS

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

Orientador: Prof. Aldri Luiz dos Santos
Coorientadora: Profa. Michele Nogueira Lima

CURITIBA

2016

Dados Internacionais de Catalogação na Publicação (CIP)
Elaborado por: Sônia Magalhães
Bibliotecária CRB 9/1191

E92
2016

Evangelista, Danilo de Faria Reis
Disseminação segura de conteúdo diante de ataques sybil para a internet das coisas / Danilo de Faria Reis Evangelista ; orientador ; Aldri Luiz dos Santos ; coorientadora, Michele Nogueira Lima. – 2016.
70 f. ; 30 cm

Dissertação (mestrado) – Universidade Federal do Paraná, Curitiba, 2016
Bibliografia: f. 59-64

1. Internet das coisas. 2. Rede locais sem fio. 3. Informática. I. Santos, Aldri Luiz dos. II. Lima, Michele Nogueira. III. Universidade Federal do Paraná. Programa de Pós-Graduação de Informática. IV. Título.

CDD 20. ed. – 004

AGRADECIMENTOS

Gostaria de começar os agradecimentos pela minha família, meus pais Rachel e Alexis, que sempre foram e serão minha fortaleza nos momentos de turbulência. A minha irmã Júlia e namorada Ítala obrigado pela força e confiança. Tenho muito orgulho e admiração por vocês. Obrigado por todo apoio e amor dedicados a mim.

Quero agradecer ao meu mentor Aldri Luiz dos Santos pelas orientações que me auxiliaram no caminho árduo de me tornar um mestre. Muito obrigado pela confiança (e paciência) depositados em mim. Agradeço a Michele Nogueira Lima pelos ensinamentos, esclarecimentos e pelos esforços dedicados ao meu aprimoramento.

Aos colegas de laboratório deixo aqui meu muito obrigado. Muito obrigado mesmo, pela parceria, amizade, descontração, zoeiras, geladas, café, debates , concelhos, modelos, metodologias, livros, artigos, ideias, exemplos e pela força. Ao Alisson (Beavis), A mi hermano de otra madre (Christian), ao Bulbasauro (Ricardo), ao George da Floresta (Cláudio), Ao Filinho (Rodrigo), ao Robinho (Meu patrão), ao Benê (Benevid), ao Ganso (Jefferson), Ao Adi (Anonymous). Ao Luiz Baroni, ao Grande Arthur, a Andressa, ao Otto , ao Rafael, ao Ursinho (Metuzalem), ao Renato Melo, ao Tio San (Santiago), ao Ivan e ao Edgar. Brincadeiras a parte, vocês fizeram o meu caminhar mais leve nestes anos. Vou carregar um pedaço de vocês sempre.

Agradeço a todos que me influenciaram direta e indiretamente durante estes dois anos e meio. Muito obrigado pela paciência e compreensão nos momentos de dificuldade. Pela mão firme nas horas de insegurança. Pelos ouvidos nos momentos de desabafo, reclamação e cansaço extremo. Agradeço as palavras de sabedoria, os conselhos que perdi na confusão do caminho. Deixo aqui meu humilde muito obrigado, na certeza de que sem vocês não chegaria até aqui.

RESUMO

O avanço das tecnologias de comunicação e a redução dos dispositivos computacionais estão propiciando o desenvolvimento da Internet das Coisas (IoT). Esta rede integra desde lâmpadas, geladeiras, roupas, e até dispositivos computacionais, promovendo a geração de um grande volume de dados como também a interação entre os objetos e os seres humanos em ambientes residenciais, industriais, de saúde, entre outros. A integração entre estes objetos e dispositivos computacionais promove a geração de um grande volume de dados, os quais serão disseminados para o desenvolvimento de vários serviços em tempo real como o monitoramento das funções vitais, a localização de objetos, a mensuração da temperatura de um local. Contudo, uma rede IoT precisa lidar também com fatores como limitações de recursos, heterogeneidade dos dispositivos, perdas de enlace e a vulnerabilidade do meio sem fio. Tais fatores quando explorados por usuários maliciosos tornam a disseminação de conteúdo insegura. O serviço de disseminação de conteúdo nessas redes está sujeito a diversas ações maliciosas, entre as quais destaca-se a personificação de identidades realizada pelo ataque Sybil. Embora existam várias abordagens de detecção de ataque Sybil, como o Lightweight Sybil Detection (LSD), elas são custosas, desconsideram dispositivos heterogêneos, e não levam em conta atacantes Sybil com identidades roubadas. Assim, esta dissertação apresenta um mecanismo de controle de associações, denominado SA^2CI (**S**ybil **A**ttack **A**ssociation **C**ontrol for **I**oT), que busca prevenir associações de atacantes Sybil à disseminação de conteúdo da IoT. O desenvolvimento deste mecanismo é baseado em criptografia de curvas elípticas (ECC), funções não clonáveis (PUF) e recibos de identidades. A ECC auxilia na criação de um canal seguro com baixo custo computacional por onde a comprovação da identidade, representada pela PUF dos dispositivos será transportada para o cálculo e distribuição dos recibos de identidade, garantindo a sua legitimidade. O SA^2CI foi avaliado através de simulações, e comparado com o LSD através de métricas de eficácia e eficiência. Os resultados mostraram que o SA^2CI foi capaz de detectar ataque Sybil de forma eficaz, eficiente e constante, independente do tipo e quantidade de identidades.

Palavras-chave: IoT, disseminação segura, ataque Sybil, mecanismo de detecção.

ABSTRACT

The technological advance in communication and the reduction of computational devices are providing the development of the Internet of Things (IoT). This network integrates from lamps, fridges, clothes to computational devices, promoting promoting a huge volume of data, as well as an interaction between objects and humans in residential, industrial and health environments, allows the integration of communication between objects, computing devices, various services can be provided in real time, such as the monitoring of vital functions, the location of objects, the temperature measurement. However, an IoT network needs to deal with factors such as resource constraints, heterogeneity of devices, link losses and the vulnerability of the wireless medium. This factors, when exploited by malicious users, make the dissemination insecure. The content dissemination service in these networks is subject to various malicious actions, among which stands out the personification of identities held by Sybil attack. While there are several approaches to Sybil attack detection, such as Lightweight Sybil Detection (LSD), they are costly, disregard heterogeneous devices, and do not take into account Sybil attackers with stolen identities. This dissertation presents a mechanism of control of associations, denominated SA^2CI, that seeks to prevent associations of attackers Sybil to the dissemination of IoT content. The development of this mechanism is based on the usage of elliptic curve cryptography (ECC), non-clonable functions (PUF) and identity receipts. An ECC will assist in the creation of a secure channel with low computational cost through which a proof of identity, represented by the PUF of the devices will be transported to calculate the distribution of identity receipts, guaranteeing their legitimacy. The SA^2CI was evaluated through simulations and compared with LSD through metrics of effectiveness and efficiency. The results showed that the SA^2CI was able to detect Sybil attack effective, efficient and consistent manner, regardless of the type and amount of identities.

Keywords: IoT, security dissemination, Sybil attack, detection mecanism.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ECC	Elliptic Curve Cryptography
IoT	Internet of Things
IETF	Internet Engineering Task Force
LSD	Lightweight Sybil Defense
DAS	Defense Againist Sybil
LSDF	Lightweight Sybil Defense Framework
LSR	Local Sybil Resistance
MAC	Media Access Control
NFC	Near Field Communication
RFC	Request For Comment
RFID	Radio Frequency Identification
RPL	Routing Protocol for Low Power and Lossy Networks
RSSF	Redes de Sensores sem Fio
RSS	Received Signal Strength
RSSI	Received Signal Strength Indication
SA	Sybil Attack
SA^2CI	Sybil Attack Association Control for IoT
UL	Usuário Legítimo
UM	Usuário Malicioso
VANET	Veicular Ad Hoc Networks
MANET	Mobile Ad Hoc Networks
PUF	Função não Clonável Única

NOTAÇÃO

$\mathcal{N}$	Conjunto de nós da rede
$\mathcal{N}_L$	Nós com comportamento legítimo
N_S	Nós com comportamento Sybil
$\mathcal{N}_{kdc}$	Nós sem restrição de recursos
$\mathcal{N}_{mov}$	Nós com restrição de recursos
Id	Conjunto das identidades da rede
Id_ρ	Identidades roubadas
Id_φ	Identidades fabricadas
p, q	Dois números primos grandes
K_x	Chave privada do nó N_x
Q_x	Chave pública do nó N_x
GF_p	Corpo finito sobre p
S_x	Segredo do nó N_x compartilhado com o seu KDC
$E(GF)$	Grupo de pontos de uma curva E
z_n	Ponto da curva E usado para gera um recibo
V_{req}	Função de verificação de requisição
PUF_x	Código PUF do nó N_x
R_{N_x}	Recibo de identidade do nó N_x emitido por seu KDC
T_{det}	Taxa de Detecção
A_c	Acurácia
T_{fp}	Taxa de Falsos Positivos
CE	Consumo Energético
SS	Sobrecarga

CAPÍTULO 1

INTRODUÇÃO

Hoje em dia, a Internet está presente cada vez mais no cotidiano das pessoas, e o seu uso provê um maior conforto para todos. O avanço das tecnologias das redes sem fio, e a redução dos dispositivos computacionais estão propiciando o desenvolvimento da Internet das coisas (IoT, do Inglês Internet of Things). Estes dispositivos apresentaram um maior poder computacional, possibilitando a comunicação de forma inteligente entre eles. Assim, eles poderão oferecer serviços mais personalizados e eficientes de modo a facilitar o cotidiano das pessoas. Desta forma, a IoT está em desenvolvimento e ela é considerada um dos pilares da Internet do futuro [2, 3, 4].

A IoT consiste em uma rede híbrida, aberta e heterogênea que integra objetos desde lâmpadas, geladeiras, roupas até dispositivos computacionais [5, 6]. Esta rede proporciona a interação entre os objetos e os seres humanos em ambientes industriais, domiciliares, entre outros. Além disso, os objetos presentes na IoT possuem características como identidade, atributos físicos, e também usam interfaces inteligentes a fim de estabelecer uma comunicação [7]. Logo, através da IoT, serviços como a mensuração de temperatura, a localização de objetos, e até o monitoramento de funções vitais podem ser oferecidos aos seres humanos em tempo real.

A IoT pode estar contida em diversos ambientes num âmbito urbano como saúde, doméstico, transportes, entretenimento, indústria. Estes ambientes podem ser classificados pela densidade, área de abrangência, escalabilidade, heterogeneidade dos dispositivos e tecnologias. Dentro de cada ambientes diversos tipos de conteúdos podem ser disseminados dependendo do tipo de serviço oferecido por eles. Uma forma de distinção entre os tipos de dados trafegados nestes ambientes é classificá-los em conteúdos críticos e não críticos. Em um complexo hospitalar ou *eHealth*, por exemplo, os dados vitais coletados pelos sensores de um paciente possuem um nível de criticidade maior que as informações referentes a objetos dentro de uma geladeira uma residência. Diante disso, a IoT permite que a disseminação de dados nos seus ambientes possam melhorar a qualidade de vida das pessoas propiciando o desenvolvimento das cidades inteligentes.

Os objetos e dispositivos presentes nos ambientes IoT além de prover informação para as pessoas também passarão a interagir entre si e com os humanos [8, 9, 10]. Para que isto ocorra a IoT adota a tecnologia 6LoWPAN, na qual tem como base o protocolo IPv6 [11]. Este protocolo tem como objetivo a utilização de um numero maior de dispositivos e auxilia na auto configuração e gestão de uma rede IoT. O 6LoWPAN é essencial para permitir uma comunicação e serviços inteligentes por meio destes objetos, uma vez que ele possi-

bilita o transporte dos pacotes IPv6 em redes sem fio de baixo consumo de energia. Esta tecnologia então visa a comunicação entre os objetos, dispositivos e pessoas permitindo um melhor controle sob a grande quantidade de dispositivos e serviços prestados na IoT.

Contudo, a IoT possui desafios ligados a comunicação e a segurança como a interoperabilidade e a privacidade. Assim, ela está exposta a diversas vulnerabilidades de segurança que podem ser explorados por atacantes. Desta maneira, eles tem como objetivo interromper o funcionamento normal da rede comprometendo a confidencialidade das informações disseminadas. Além disso, a IoT herda as necessidades presentes nas redes sem fio e da Internet tradicional como a robustez, a confiabilidade, a confidencialidade, a integridade e a escalabilidade. Logo, a adoção de mecanismos que minimizem os efeitos destes atacantes é de suma importância para o desenvolvimento da IoT.

1.1 Motivação

O grande volume de dados gerado pelos dispositivos presente na Internet das Coisas (IoT) precisa ser encaminhado através do serviço de disseminação de conteúdo. Neste serviço, os participantes da rede encaminham as mensagens a partir de um dispositivo-origem até um dispositivo-destino. Diante disso, a disseminação de conteúdo precisa muitas vezes lidar com fatores como mobilidade, limitação de recursos e perdas de enlaces [12, 13], tido como caracterísitcas de dispositivos móveis. Além disso, a heterogeneidade dos dispositivos e das tecnologias da IoT dificulta a disseminação de conteúdo. Esses fatores quando explorados por usuários maliciosos tornam a disseminação de conteúdo vulnerável. Desta forma, esses fatores precisam ser considerados na disseminação de conteúdo para garantir que este serviço não seja afetado, manupulado, ou mesmo reduzido a sua qualidade.

Os objetos presentes numa rede IoT usam o serviço de disseminação de conteúdo de modo à encaminhar os dados coletados num ambiente até uma aplicação no âmbito da Internet. Neste serviço, a heterogeneidade dos dispositivos deve ser levada em conta uma vez que eles podem apresentar recursos limitados [14, 15]. Em uma disseminação de dados dentro de um ambiente IoT, esses objetos exploram os recursos dos dispositivos sem limite de recursos de modo à assegurar o maior tempo de vida daqueles com menores capacidades. Diante disso, a disseminação numa rede IoT é orientada pela capacidade do dispositivo/objeto, isto é, caso um objeto ou um dispositivo não possua recurso suficiente, o mais próximo com capacidade se encarrega de realizá-la, garantindo a continuidade dos serviços prestados. Assim, num ambiente da IoT o serviço de disseminação de conteúdo é base para que sejam disponibilizados aplicações para um usuário final.

A disseminação de conteúdo na IoT está sujeita a diversas ações maliciosas cometidas por um atacante, onde se destaca a personificação de identidades realizada pelo ataque Sybil (SA) [12, 16].O processo de personificação de identidades ocorre quando um atacante se passa por um usuário legítimo da rede. Para obter tais identidades este atacante

explora vulnerabilidades do meio sem fio, obtém essas identidades, e assim visa o acesso à disseminação dos dados [17, 18]. Um SA autenticado numa rede IoT visa alcançar vantagens como o uso de recursos não autorizados, o acesso à informações vitais, comprometendo a confidencialidade e a privacidade dos usuários da rede. Assim, o SA reduz a qualidade dos serviços suportados pela disseminação de conteúdo, resultando na falta de segurança dos dados trafegados na rede [19, 20].

As técnicas de detecção do SA encontradas na literatura identificam este ataque a partir das características em comum da rede [21, 22] da criptografia [23, 24], e do relacionamento entre os vizinhos [25, 26, 27]. Na técnica baseada em características comuns das redes aspectos como a força do sinal recebido, mobilidade e área de cobertura são considerados para identificar o ataque. Apesar de levar em conta a restrição de recursos dos dispositivos da IoT, esta técnica não é eficaz contra o ataque Sybil [28]. Já na criptografia a detecção de um SA considera chaves simétricas e assimétricas de modo a garantir a irretratabilidade das identidades legítimas de uma rede. No entanto, essa técnica requer constantes atualizações dos novos pares de chaves, demandando uma sobrecarga na rede. Enquanto que a técnica do relacionamento entre os vizinhos analisa as opiniões sobre um nó emitidas por seus vizinhos. Contudo, um nó malicioso que simule um comportamento legítimo pode ludibriar as opiniões dos vizinhos, se mantendo na rede. Logo, há a necessidade se tratar este ataque considerando as restrições de recursos dos nós da IoT.

Estas abordagens também não são eficientes quando aplicadas nas redes IoT. Em ambientes com interferências eletromagnéticas ou sonoras, a detecção baseada em características comuns das redes requer um tratamento especial contra estes efeitos adversos [29]. Visto que certas redes IoT requerem uma alta escalabilidade, a criptografia com chaves simétricas e hash não se aplica e a adoção da criptografia baseada em chaves publicas com o algoritmo de curvas elípticas torna-se uma alternativa [30]. A abordagem baseada no relacionamento entre os dispositivos detecta apenas o ataque com identidades fabricadas [31]. Dessa maneira, caso um atacante roube uma identidade legítima, ele terá acesso a rede por que esta abordagem desconsidera o não repúdio. Portanto, mesmo com a ausência de limitação de recursos o uso destas abordagens na IoT torna-se inviável.

1.2 Objetivos

Esta dissertação tem como objetivo garantir a disseminação segura de conteúdos diante de ataques Sybil (SA's) na Internet das coisas (IoT). Para garantir a confidencialidade no serviço de disseminação de conteúdo durante a associação de um dispositivo é proposto um mecanismo de segurança na disseminação de conteúdo denominado SA^2CI (**S**ybil **A**ttack **A**ssociation **C**ontrol for **I**oT). Este mecanismo emprega curvas elípticas a fim de criar um canal seguro para que as informações trafegadas na rede sejam confidenciais. A função não clonável (PUF) e a técnica de recibos são utilizadas para garantir a autenticidade

e a irretratabilidade de modo à assegurar a comprovação e a garantia da identidade um nó da rede. Além disso, este mecanismo monitora um SA através de assinaturas de comportamentos maliciosos durante uma solicitação de associação à rede. Como o SA viola os princípios da confidencialidade, autenticidade, e irretratabilidade, este mecanismo usa como base estes princípios e aplica técnicas para garantir a disseminação segura à SA's.

O mecanismo de controle de associações para IoT, SA^2CI, possui três fases, a inicialização, a configuração, e a gerência da disseminação. A primeira fase tem como objetivo gerar uma curva elíptica sob um acordo dos nós $\mathcal{N}_{kdc}$, sem restrição de energia, para que os nós $\mathcal{N}_{mov}$, com restrição, sejam configurados por meio de um canal seguro. Na segunda fase, os nós da rede são configurados de modo que todos recebam os seus pares de chaves e sua respectiva garantia da identidade, geradas através da PUF e do recibo de identidade. Logo após esta fase, o SA^2CI atua na rede monitorando as reassociações e as novas associações à rede por meio da verificação do recibo de identidades e também do comportamento de um nó, evitando que SA's tenha acesso a disseminação de conteúdo.

1.3 Contribuições

Este trabalho apresenta as seguintes contribuições:

- Um estudo sobre os mecanismos de detecção de ataques Sybil (SA) existentes na literatura. Estes mecanismos foram classificados em baseados nas características das redes, em criptografia, e no relacionamento entre vizinhos próximos. Através deste estudo foi possível levantar os requisitos necessários para a detecção deste ataque no serviço de disseminação de conteúdo.

- Uma quantificação do desempenho por meio de simulação de um dos trabalhos encontrados na literatura em um ambiente da IoT. Para realizar esta quantificação o critério adotado foi a adequabilidade com a IoT. Dessa maneira, o mecanismo LSD foi escolhido uma vez que ele é escalar, distribuído, leve e detecta SA's.

- Uma especificação do SA^2CI (**S**ybil **A**ttack **A**ssociation **C**ontrol for **I**oT), mecanismo de controle de associações para o serviço de disseminação de conteúdo da IoT. O SA^2CI possui três fases, a inicialização, a configuração da rede, e a gerência da disseminação. Estas três fases juntas possibilitam a identificação de associações de SA's ao serviço de disseminação de conteúdo da IoT.

- Uma avaliação do mecanismo SA^2CI diante de SA's. A avaliação considerou dois cenários, um doméstico e outro num ambiente *eHealth*. Além disso, o SA^2CI foi comparado com o mecanismo LSD em dois cenários, onde em ambos o SA^2CI obteve melhores resultados tanto na eficiência quanto no desempenho. A avaliação

mostrou que o mecanismo SA^2CI identifica SA's independente do tipo identidade e comportamento em uma requisição de associação.

1.4 Estrutura da dissertação

Esta dissertação está organizada em seis capítulos. O Capítulo 2 apresenta os fundamentos relacionados à disseminação na Internet das coisas (IoT), ao ataque Sybil (SA), os quais mostram os desafios desta rede para prover uma disseminação segura a SA's. Em seguida, o Capítulo 3 classifica e caracteriza as abordagens utilizadas para detectar SA's e as técnicas existentes para se estabelecer uma transmissão segura. Já o Capítulo 4, descreve o mecanismo de controle de associações para IoT (SA^2CI) que identifica ataques Sybil (SA's) com identidades roubadas e fabricadas com os comportamentos churn e com múltiplas identidades. O Capítulo 5 apresenta uma avaliação de desempenho composta por 2 cenários realísticos da IoT e a mensuração da eficácia e da eficiência dos mecanismos SA^2CI e LSD. Por fim, o Capítulo 6 conclui este trabalho apresentando também as suas direções futuras.

CAPÍTULO 2

FUNDAMENTOS

Este capítulo apresenta os fundamentos necessários à compreensão do contexto da pesquisa, do problema e da proposta. A Seção 2.1 apresenta as características gerais da IoT, sua aplicação em determinados ambientes, suas arquiteturas e tecnologias existentes neste paradigma. A Seção 2.2 descreve a disseminação de conteúdo na IoT, mostra as técnicas e os mecanismos para o encaminhamento de mensagens. A Seção 2.4 detalha a os princípios e os requisitos de segurança para redes sem fios necessários para a alcançá-la, além de, descrever o ataque *Sybil*, apresentando o seu comportamento e as formas de detecção. A Seção 2.5 mostra as estratégias existentes contra o ataque *Sybil*.

2.1 Internet das Coisas

A Internet das Coisas (IoT, do inglês *Internet of Things*) tem propiciado uma mudança de paradigma na comunicação e nos tipos de serviços oferecidos para as pessoas [32]. Este novo paradigma compreende objetos como lâmpadas, geladeiras e até canetas, os quais coletam informações e comunicam-se entre si e com dispositivos computacionais. Tanto a coleta quanto a comunicação entre os objetos e esses dispositivos proporcionam serviços personalizados para os usuários, por exemplo, a mensuração de temperatura de um ambiente, localização geográfica e monitoramento de funções vitais. Em 2010, tal paradigma recebeu a denominação de visão do futuro [33].

Na IoT, os objetos são considerados inteligentes quando possuem a capacidade de coletar dados e disseminá-los. Cada objeto dispõe basicamente de um sensor e/ou atuador, um microprocessador, um dispositivo de comunicação sem fio e uma fonte de energia [34]. Além dessas capacidades, os objetos apresentam características especiais, como, identidade e interfaces inteligentes que facilitam a interação entre os mesmos [35]. Tais características viabilizam a comunicação e cooperação com o intuito de garantir a troca de dados entre dispositivos e objetos presentes na IoT.

Os objetos e os dispositivos inteligentes são capazes de realizar vários serviços personalizados na IoT. Estes serviços abrangem desde tarefas triviais como a mensuração de temperatura e a localização geografica até tarefas complexas, por exemplo, o monitoramento de funções vitais. Assim, os dados do ambiente são disseminados para aplicações que interagem com as pessoas.

A IoT pode ser aplicada no domínio urbano, contudo, existem outros domínios como o rural e o militar [36]. O domínio urbano concentra uma boa parte das atenções dos pesquisadores devido a grande quantidade de serviços disponibilizados e os desafios exis-

tentes para que os mesmos sejam entregues. Este domínio é composto pelos ambientes cotidianos tais como a saúde, o domicilar, o transporte, o entretenimento, a indústria, entre outros. Desta forma, estes ambientes passam a ser inteligentes quando diferentes tipos de objetos inteligentes e dispositivos computacionais trabalhem para fazer a vida das pessoas contidas nesse ambiente mais confortável [37].

Os ambientes inteligentes compreendem os objetos inteligentes, os dispositivos computacionais, os serviços e as pessoas. Nestes ambientes pode-se ter três visões de funcionamento: a computação virtual, os ambientes físicos, os ambientes humanos [38]. A computação virtual permite os objetos inteligentes e dispositivos computacionais a acessarem os serviços em qualquer lugar e a qualquer momento. Os ambientes físicos podem ser incorporados com uma variedade de objetos e dispositivos, seu tamanho oscila do nano ao macro. Nos ambientes humanos os objetos e dispositivos encontram-se incorporados nas pessoas ou fazem parte do uso delas, por exemplo, celulares, relógios inteligentes, marcapasso, entre outros. Com isso, estas três visões possibilitam observar a IoT de forma global, com a computação virtual, dividida em domínios a partir dos ambientes físicos e o relacionamento deste paradigma com as pessoas, no ambiente humano.

A comunicação na IoT provê a adoção de novas tecnologias como 6LoWPAN e outras existentes como o Identificador por rádio frequência (RFID, do inglês *Radio Frequency Identification*), a comunicação de campo próximo (NFC, do inglês *Near Field Communication*) e o padrão IEEE 802.15.4. Essas tecnologias são alicerce para a comunicação entre os dispositivos deste paradigma. O uso destas tecnologias na IoT promove o desenvolvimento de serviços nos seus demais domínios. Entretanto, essas tecnologias atuam em diferentes fases da comunicação e para que haja um maior controle sobre elas a literatura utiliza arquiteturas de três e cinco camadas. Desta forma, essas arquiteturas serão apresentadas na próxima subseção.

2.1.1 Arquiteturas

Ainda não existe um padrão, de fato, para a arquitetura da IoT [39]. Como mencionado anteriormente, existem várias entidades que estabelecem padrões para a IoT. Contudo, dois padrões de arquiteturas encontram-se bem difundidos na literatura, o modelo de cinco camadas e o modelo de três camadas. Estes modelos descrevem o funcionamento dos serviços presentes em cada uma das suas camadas onde o conjunto destes propiciam a comunicação entre os dispositivos.

As duas arquiteturas possuem três camadas semelhantes nas quais são a camada perceptual ou sensitiva, a camada de rede e a camada de aplicação. A primeira camada da arquitetura é a camada perceptual ou sensitiva, ela tem como principal objetivo a coleta dos dados através do sensoriamento. Logo após a etapa de coleta, os dados disseminados vão para a camada de rede. Esta camada utiliza o endereçamento IPV6 [40] e o proto-

colo de roteamento (RPL) [41] com o intuito de realizar a transmissão origem/destino do determinado conteúdo. Por fim, a camada de aplicação disponibiliza o conteúdo para o destinatário (usuário final), onde este interage com o conteúdo através de aplicações.

Os dois modelos existentes na literatura divergem em algumas funções presentes nas duas camadas adicionais do modelo de cinco camadas. Eles estão representados na Figura 2.1, onde na parte da direita é possível observar duas camadas adicionais, a camada de gateway e a camada de middleware. A camada de gateway controla a comunicação no ambiente da IoT e transmite mensagens entre os objetos e os sistemas. A camada de middleware que tem como principal objetivo prover uma maior flexibilidade na associacão entre intefacaces de hardware e software.

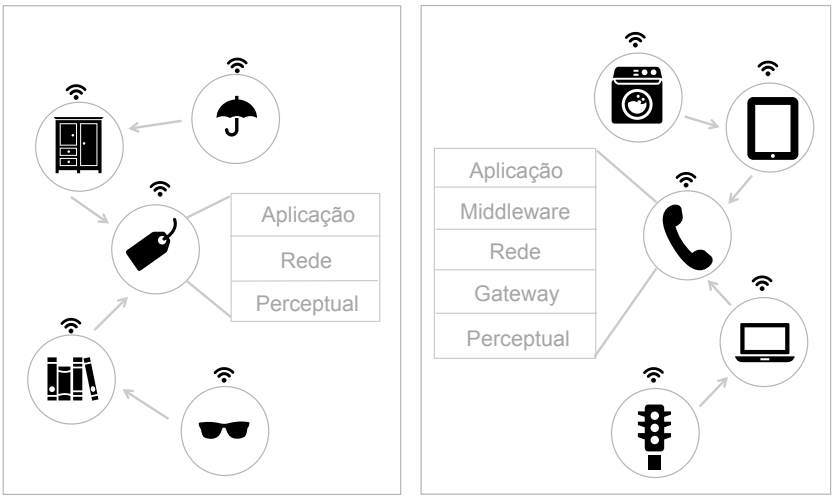


Figura 2.1: Arquitetura com 3 e 5 camadas

A arquitetura da IoT provê subsídios necessários a fim de realizar a comunicação entre os dispositivos. Para que esta comunicação ocorra, requesitos como escalabilidade e interoperabilidade devem ser satisfeitos [2]. A escalabilidade gerencia o crescente aumento de dispositivos na IoT. Por outro lado, a interoperabilidade trata da comunicação entre diversas tecnolgias de forma transparente. Tais requisitos quando atendidos permitem a comunicação entre os dispositivos, possibilitando assim o desenvolvimento de aplicações e serviços.

2.1.2 Tecnologias de comunicação

O surgimento da IoT proporciona mais praticidade e conforto para as pessoas. Contudo, os dispositivos presentes neste tipo de rede variam de acordo com a tecnologia utilizada em um ambiente. Desta forma, existem uma série de tecnologias as quais se aplicam na IoT. A adoção de RFID, do NFC e das redes de sensores sem fio (RSSFs, do inglês *Wireless Sensor Networks*) crescem continuamente nos ambientes de cobertura da IoT.

Dentre as tecnologias apresentadas anteriormente, apenas as RSSF está contida no

escopo deste trabalho. Este tipo de rede consiste em dispositivos sensores dispostos de forma distribuída em uma determinada área [42]. Os sensores que compõem as RSSF tem as seguintes características: cooperação, limitação de recurso e mobilidade [43]. Cada sensor compreende de uma bateria, um rádio e processador desempenhando a sua principal função na qual consiste da coleta de informações.

As RSSF despertaram a atenção no cenário acadêmico e industrial devido à vasta possibilidade de aplicações contidas nos ambientes. Desta forma, ambientes domésticos, hospitalares, comerciais e militares utilizam os dados coletados em prol do benefíco humano. Sendo assim, a coleta de dados, principalmente em ambientes de díficil acesso, colaborou com o aumento das RSSFs nestes ambientes. Portanto, estas redes inseridas no contexo da IoT contribuem com a evolução deste paradigma.

2.2 Disseminação de conteúdo

O desenvolvimento da computação pervasiva tem possibilitado os dispositivos computacionais realizarem a comunicação em qualquer lugar e a qualquer momento [5]. Isto beneficiou a IoT, visto que os objetos e dispositivos contidos neste paradigma necessitam deste tipo de comunicação, pois ambos precisam coletar e transmitir informações relacionadas aos ambientes e as pessoas. Contudo, estas informações armazenadas pelos objetos devem ser transmitidas para um dispositivo com maior poder computacional com o intuito de processar e/ou encaminhar estas informações. Este procedimento denomina-se disseminação de conteúdo.

Os tipos de conteúdos disseminados na IoT variam de acordo com o ambiente. Estes conteúdos são: texto, áudio e vídeo. Assim, em ambientes como rodovias inteligentes, indústrias, por exemplo, o principal tipo de conteúdo disseminado é o textual. Visto que nestes ambientes o objetivo primordial dos objetos consiste em monitorar as velocidades, as informações de vagas de estacionamento, a temperatura do ambiente, as funções vitais entre outros. Em ambientes de entretenimento e comerciais o conteúdo mais disseminado varia entre áudio e vídeo. Tendo em vista que nesses ambientes, serviços como *streaming* de vídeos, compartilhamento de áudio e imagens são mais explorados. Portanto, o conteúdo transmitido em cada um desses ambientes muda de acordo com as características apresentadas, das necessidades dos usuários e da capacidade dos dispositivos presentes

Outra forma de identificar os conteúdos consiste em classificá-los de acordo com a criticidade, a emergência e a periodicidade da coleta. Na saúde, nas rodovias e nas indústrias, por exemplo, o conteúdo disseminado nos ambientes são críticos, emergenciais e necessitam de uma coleta constante. Esta classificação leva em conta o tipo de serviço disponível no ambiente. Estes possuem serviços os quais trabalham com informações pessoais ou sigilosas, como informações vitais, acidentes em rodovias e componentes de um processo químico. Em ambientes domésticos e de entretenimento o conteúdo não é

critico, nem emergencial e o tipo de coleta realizada ocorre de forma periódica. Visto que o conteúdo disseminado nestes ambientes não exige tanta privacidade quanto nos ambientes de saúde e rodoviário. Logo, este tipo de classificação facilita o desenvolvimento de serviços nos ambientes da IoT, adequando modo de funcionamento dos serviços em relação aos ambientes.

2.2.1 Encaminhamento de conteúdo na IoT

A disseminação do conteúdo na IoT ocorre através de múltiplos saltos. Isto acontece devido a baixa taxa de transmissão e ao curto raio de alcance dos dispositivos presentes nesta rede. Com essas restrições, os padrões de roteamento existentes nas demais redes não se adotam para a IoT. Assim, a Força Tarefa da Internet (IETF, do inglês *Internet Task Force*) desenvolveu uma série de especificações (RFC's) sobre a comunicação e o encaminhamento de mensagens para dispositivos com curto raio de alcance e limitações de bateria e processamento. Portanto, a camada física e a camada de enlace utilizam o padrão 802.15.4 e a camada de rede implementa o 6LoWPAN (do inglês, *IPV6 over Low Power Wireless Personal Area Network*) respectivamente.

O padrão IEEE 802.15.4 define a camada física e a subcamada de controle de acesso para dispositivos de baixa taxa de transmissão. Este padrão opera tipicamente em distâncias até 10 metros e utiliza endereços que variam entre 16 a 64 bits acomodando 2^{16} dispositivos por rede [44]. Os links que atuam sobre o 802.15.4 apresentam três tipos de frequências: 2.4 GHz alcançando 250 kbps, 915 MHz atingindo 40 kbps e 868 MHz com 20 kbps [45]. Além disso, esses links contam com 27 canais distribuidos nas três frequências, das quais 16 foram alocados para 2.4 GHz, 10 para 915 MHz e 1 para 868 MHz. Assim, este padrão é base para diversas tecnologias como Zigbee [46], ISA100 [47] e WirelessHart [48].

O 6LoWPAN atua na camada de rede e tem como objetivo realizar a comunicação pelo protocolo IPV6 em redes 802.15.4. Visto que o IPV6 possui uma grande quantidade de campos no seu cabeçalho, esse tipo de rede realiza um série de fragmentações, desfragmentações e compressões com o intuito de proporcionar a comunicação para dispositivos de baixa capacidade de transmissão. Este processo é importante devido o fato do IPV6 ter um MTU máximo de 1280 octetos e nas redes 802.15.4 este valor equivale 127 [49]. Desta forma, o 6LoWPAN cria uma camada de adaptação entre o 802.15.4 e o IPV6 mediante a necessidade da rede e dos dispositivos.

A arquitetura das redes 6LoWPAN descreve a forma como os dispositivos estão dispostos na rede e o seu modo de funcionamento. Esta rede pode assumir três formas: ad hoc, simples e estendida. No modo ad hoc as redes não estão conectadas à internet e funcionam sem qualquer tipo de infraestrutura. O modo simples consiste em redes interligadas a outras redes ou com a internet através de um gateway. O último modo, estendido,

conta com múltiplas redes de arquitetura simples interligadas por diversos coordenadores ligados a um backbone ou até mesmo à internet. Contudo, para que haja o encaminhamento de mensagens na IoT, é necessário adotar um protocolo com o intuito de coordenar a troca de mensagens entre os dispositivos.

O protocolo de roteamento para redes de baixa potência e com perdas (RPL, do inglês *Routing Protocol for Low-Power and Lossy*) foi recentemente padronizado para IoT [12]. Desta forma, o RPL trabalha de forma conjunta com o 6LoWPAN a fim de realizar o encaminhamento de mensagens dos dispositivos da IoT. Assim, este protocolo realiza adaptações de acordo com as características do ambiente, tais restrições oferecem desafios para o roteamento das mensagens como a limitação de bateria, processamento e padrões de tráfego ponto a ponto, multiponto para ponto e vice-versa.

O encaminhamento de informações em uma rede utiliza múltiplas instâncias do RPL [41], isto varia de acordo com as restrições e características da rede. Desta forma, o funcionamento básico deste protocolo consiste em separar o pacote, processá-lo e encaminhar para o roteamento. Além disso, o processo de encaminhamento de mensagens do RPL faz uso de pacotes RPL com o intuito de associá-los a instância do ambiente e a validação de dados. Portanto, este protocolo lida com a topologia dinâmica da IoT operando de forma autônoma.

O conjunto dessas tecnologias, 802.15.4, 6LoWPAN e RPL, permitem o encaminhamento de mensagens na IoT. Mesmo contendo uma série de limitações como restrição de energia e processamento as redes 6LoWPAN em conjunto com o padrão 802.15.4 desempenham o seu papel de forma correta em dispositivos de baixa capacidade. Contudo, os dispositivos e as próprias redes, nos dias de hoje, necessitam de estratégias que garantam a segurança tanto da identidade dos dispositivos quanto dos recursos das redes.

2.3 Princípios de segurança para rede sem fio

A troca de informações entre os dispositivos dos sistemas computacionais carece de segurança, visto que existem vulnerabilidades desde o meio de comunicação até no próprio dispositivo [50]. Assim, a segurança destas informações baseia-se em três atributos: a confidencialidade, a integridade e a disponibilidade. A confidencialidade garante o acesso a tal conteúdo apenas a usuários autorizados. O segundo atributo, a integridade, consiste da ausência de alterações impróprias no conteúdo da informação. A prontidão da informação a qualquer momento diz respeito a disponibilidade. Logo, estes atributos quando aplicados na comunicação entre sistemas computacionais salvaguardam a informação.

Apesar de muitos esforços científicos na área da comunicação e infraestrutura, a segurança vem se tornando o principal foco de pesquisa na IoT. Visto que as aplicações presente neste tipo de rede manipulam dados confidenciais de seus usuário nos demais ambientes deste paradigma. Com estas informações expostas, usuários maliciosos podem

interceptar dados pessoais, criar identidades falsas, entre outras ações [51]. Logo, atributos como privacidade e confidencialidade ganham destaque na IoT. As subseções a seguir descrevem do ataque Sybil e as vulnerabilidades exploradas por atacantes, dentre eles o Sybil, na disseminação de conteúdo da IoT.

2.3.1 O ataque Sybil

A presença do ataque Sybil nas redes de computadores compromete a efetividade das aplicações presentes neste contexto. Este ataque caracteriza-se pela manipulação de identidades falsas ou roubadas. Os *usuários maliciosos* (UM) realizam estes ataques explorando as vulnerabilidades das redes, como a interceptação de pacotes. Sendo assim, a ocorrência de ataques Sybil nos sistemas presentes na IoT afeta em relatórios equivocados, sistemas de votação, acesso indevido a um conteúdo entre outros males [52, 53, 24]. Como a maioria dos atacantes Sybil se comportam de forma semelhante dos utilizadores normais, a detecção desse ataque é difícil e de suma importância para a confidencialidade do conteúdo disseminado nestas redes.

As ações maliciosas causadas pelos atacantes Sybil foram classificadas em três formas de ataques Sybil(SA, do inglês Sybil Attack) SA-1, SA-2 e SA-3, representados na Figura 2.3 [54]. Um atacante SA-1 constrói conexões, a partir de pseudo identidades, com nós honestos. O objetivo deste ataque consiste em manipular a opinião geral ou ganhar popularidade. Além de criar conexões com nós honestos, o ataque SA-2 personifica o comportamento normal de um *usuário legítimo* (UL). Desta forma, o SA-2 tem intuito de roubar e violar a privacidade de usuários e manipular de forma maliciosa sistemas de reputação.

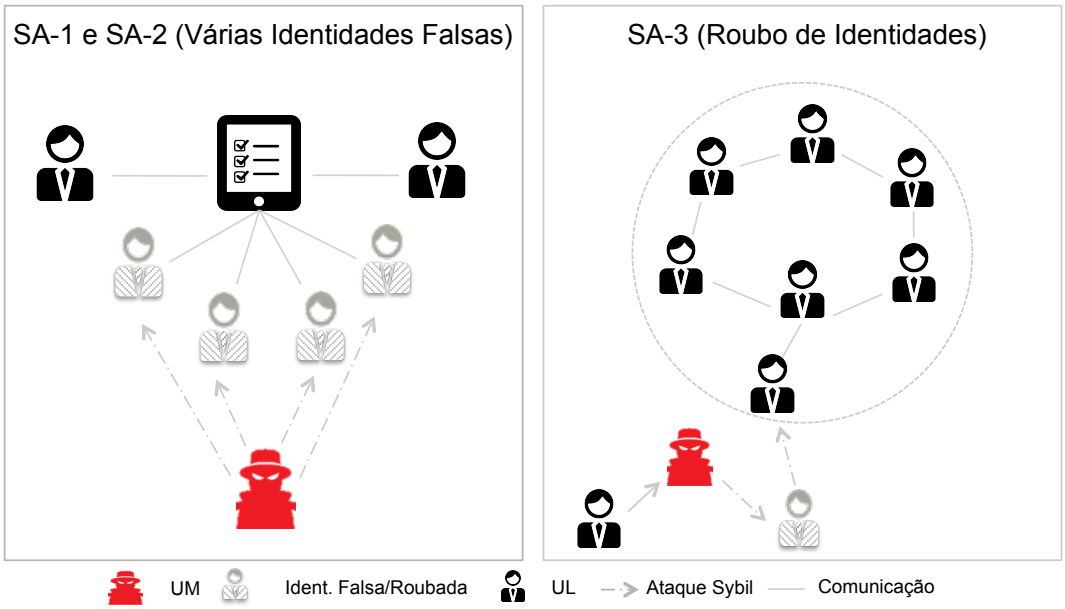


Figura 2.2: Ataque Sybil com identidades falsas e roubadas

Os ataques SA-1 e SA-2 estão presentes em redes sociais, em contra partida, o SA-3 ocorre em outro contexto, em redes móveis. Um ataque SA-3 é similar ao SA-2, entretanto, devido o SA-3 estar presente em ambientes móveis as suas conexões são intermitentes. Com isso, este trabalho terá apenas o ataque SA-3 como foco.

O ataque SA-3 considera ambientes com mobilidade para realizar as suas ações maliciosas. Além disso, este ataque quando comparado com o SA-1 e 2 resulta em maiores dificuldades de detecção. Isto ocorre devido aos recursos de dispositivos móveis não possuir uma topologia fixa e um histórico de comportamento da rede. Portanto, estratégias designadas para este tipo de ataque são consideradas complexas de se construir. Apesar do ataque SA-3 ter uma detecção complexa, algumas estratégias foram desenvolvidas a fim de detectar ou limitar o comportamento do ataque Sybil, no entanto tais estratégias desconsideram algumas características da IoT, como a heterogeneidade dos dispositivos, por exemplo.

2.3.2 Vulnerabilidades da disseminação de conteúdo na IoT

As redes IoT apresentam limitações que são inerentes aos dispositivos presentes. Estas restrições ocasionam em uma série de desafios como a minimização do consumo de recurso e maximização da performance de segurança, a susceptibilidade à ataques passivos e ativos e a inviabilidade de usar mecanismos de segurança tradicionais em redes cabeadas [55]. Os usuários maliciosos exploram essas vulnerabilidades através de ataques e assim comprometer os serviços oferecidos por ela.

Com o intuito de sanar esses desafios e vulnerabilidades a IETF pospõe uma lista de requisitos de segurança os quais serão descritos a seguir. Os requisitos de segurança propostos pela IETF estão divididos em duas classes: segurança da informação e segurança da rede. Para a segurança da informação consideram os quesitos de confidencialidade, autenticidade, integridade e informação recente. Com relação a segurança da rede os atributos considerados são: disponibilidade, resiliência, robustez, resistência, eficiência energética e garantia. Desta forma, o escopo deste trabalho considera confidencialidade, autenticidade, irretratabilidade, e eficiência energética.

A maioria dos ataques contra a segurança do usuário e dos dados na IoT tem efeito destrutivo [55, 56]. Estes ataques acontecem desde a camada física até a camada de aplicação. A Figura 2.3 classifica os ataques presentes na camada de rede do IoT e o comportamento dos mesmos. Nesta figura a classificação dos comportamentos dos nós consistem em egoísta e malicioso. No primeiro comportamento, o nó atacante prejudica um dado serviço cooperando com os seus vizinhos quando este nó desejar, ou estiver disponível. Caso umatacante egoista presente no serviço de disseminação seja escolhido para repassar um fluxo de dados para os seus vizinhos, estes dados não chegarão ao seu destino por que tal nó é egoísta. Já em ataques maliciosos, um nó visa obter uma

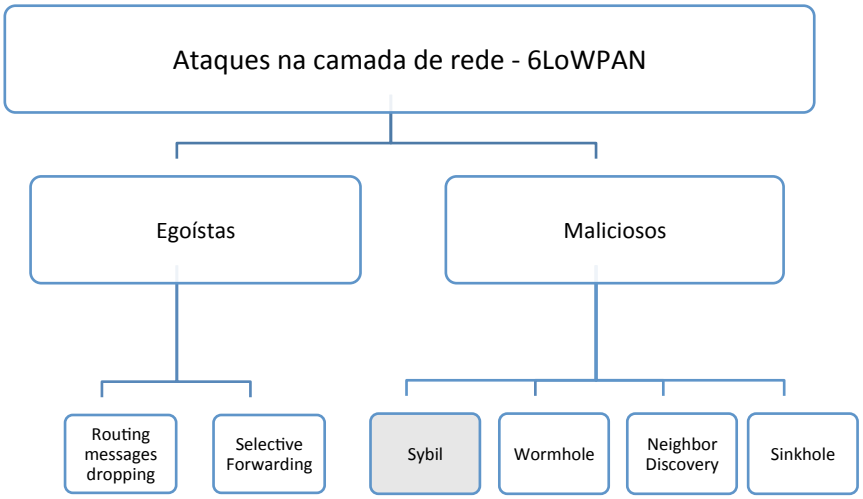


Figura 2.3: Taxonomia de ataques na camada de rede inspirado em [1]

vantagem sobre os nós da rede. Neste mesmo serviço de disseminação, um ataque Sybil emprega identidades fabricadas ou roubadas com o intuito garantir acesso à rede e aos seus serviços, infligindo a confidencialidade e a privacidade dos dados trafegados.

2.4 Resumo

Este capítulo apresentou os fundamentos sobre a Internet das coisas, mostrando as suas características, o serviço de disseminação de dados e o encaminhamento de conteúdo. Além disso, foram descritos alguns requisitos de segurança necessários para a comunicação segura. Dentre esses requisitos a confidencialidade e o não repúdio, quando desconsiderados promovem a existência do ataque Sybil. Por fim, o ataque Sybil (SA) foi contextualizado, categorizado e o seu funcionamento foi exemplificado por meio de figuras.

CAPÍTULO 3

DETECÇÃO DO ATAQUE SYBIL E TÉCNICAS DE TRANSMISSÃO SEGURA

Este capítulo apresenta os principais trabalhos existentes na literatura para detectar o ataque Sybil (SA) e de técnicas para garantir a legitimidade de uma identidade numa rede. A Seção 3.1 introduz as técnicas de detecção de um SA's, de onde elas serão classificadas, definidas, e explicadas, evidenciando seus pontos positivos e negativos. Em seguida, a Seção 3.2 mostra os trabalhos que usam a transmissão segura para garantir e a comprovar de identidades de modo à identificar de forma única na rede um nó garantindo a sua legitimidade na rede.

3.1 Abordagens contra ataque Sybil

A disseminação de conteúdo é dinâmica na forma de prover seus serviços numa rede IoT. Por exemplo, serviços como a localização de objetos, o monitoramento de dados vitais, a estimativa da temperatura de um cômodo de uma residência, entre outros. Logo após a inicialização dos nós rede algumas vulnerabilidades podem comprometer estes serviços, como a presença de atacantes, a falha dos nós, a heterogeneidade deles, e até o esgotamento de recursos energéticos destes nós. Além disso, o meio de comunicação sem fio está exposto a interferências, colisões o que pode dificultar a qualidade de um serviço prestado. Diante dessa diversidade de serviços que podem ser prestados por uma rede IoT, um ataque Sybil pode comprometer a confidencialidade dos dados disseminados, quebrando assim a privacidade dos nós/usuários desta rede, onde ele obtém acesso à rede por meio de identidades roubadas e fabricadas.

Dado o contexto de detecção de SA's em redes sem fio, diversas técnicas são encontradas na literatura. Essas técnicas são classificadas em: baseadas nas características em comum da rede [21], em criptografia [23], e no relacionamento entre os vizinhos [25]. A técnica de características em comum das redes considera aspectos dos nós, como a força do sinal recebido e da mobilidade para identificar o ataque. Apesar de levar em conta a restrição de recursos dos dispositivos da IoT, esta técnica não é eficaz contra o ataque Sybil [28]. A técnica de criptografia emprega o uso de chaves simétricas e assimétricas para garantir a irretratabilidade das identidades legítimas de uma rede. No entanto, essa técnica requer uma constante atualização dos novos pares de chaves, o que ocasiona uma sobrecarga na rede. Já a técnica do relacionamento entre os vizinhos analisa as opiniões sobre um nó emitidas por seus vizinhos. Contudo, um nó malicioso que simule um com-

portamento legítimo pode ludibriar as opiniões dos vizinhos, se mantendo na rede. Logo, há a necessidade de uma solução eficaz a este ataque e que considere as restrições de recursos dos nós da IoT.

3.1.1 Características das redes

A detecção baseada nas características da rede usa os atributos da rede e dos nós a fim de detectar um ataque Sybil. Esta técnica torna-se viável em redes com restrição de recursos, visto que não é necessário uma técnica ou um mecanismo adicional para a detecção. No entanto, ela é vulnerável a interferências eletromagnéticas e a identificação de um nó numa rede exige uma série de avaliações do seu RSS para estimar a localização de um dado nó. A seguir esta técnica será detalhada, evidenciando os seus pontos chaves e as suas desvantagens.

O LSD (do inglês,*Lightweight Sybil Detection*) é um mecanismo de detecção de SA's para MANETS. A Figura 3.1 ilustra a detecção do SA a partir da técnica das características das redes. Nesta figura, um nó (n_i) identifica um atacante a partir da sua área de cobertura, e do RSS do nó solicitante. Este nó será monitorado a partir do momento que ele atravessar a área de cobertura de n_i. Assim que o nó solicitante realizar associação, ele deve enviar a sua identidade dentro da área pontilhada de n_i. Então n_i concede acesso à rede ao nó solicitante. Em seguida n_i armazena o RSS e a identidade do nó solicitante numa lista composta pela tupla $< RSS, ID >$. A detecção do SA ocorre quando o nó solicitante exibir mais de uma identidade na área pontilhada de n_i ou apresentar uma identidade diferente daquela associada ao seu RSS.

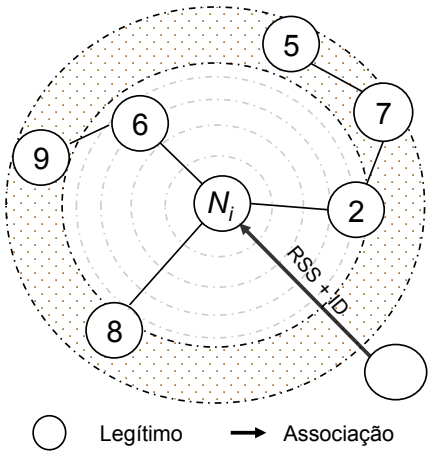


Figura 3.1: Detecção realizada pela técnica características das redes

Já o LSDF (do inglês, *Lightweight Sybil Detection Framework*) [21] considera apenas o RSS para identificar SA's. A complexidade para localizar com precisão um dispositivo atacante a partir do RSS está retratada neste trabalho. Nele, a precisão é obtida através de análises estatísticas, onde elas necessitam de um intervalo de confiança de 99%, o

que requer um número mínimo de amostras. Para isso, um dado nó n_i, por exemplo, monitora um nó solicitante da mesma forma com o que acontece na Figura 3.1. Quando n_i obtém a quantidade necessária de RSS do nó solicitante para obter os 99% do intervalo de confiança do teste de hipóteses. Dessa maneira, um SA é detectado logo após o teste de hipóteses retornar positivo.

As características das redes possibilitam a detecção do ataque Sybil com baixo uso de recursos. Esta técnica identifica os atacantes através do RSS, RSSI, e da mobilidade. Ela dispensa hardwares adicionais como GPS e antenas mais potentes para localizar um atacante Sybil. A mobilidade também é uma característica que pode ser explorada pelos mecanismos de detecção. Quando combinada com o RSS, esta característica possibilita a localização de um atacante por meio de técnicas de triangulação, e distância euclidiana. Com a aplicação desta técnica é possível identificar o ataque Sybil em ambientes que os nós possuam restrições de recursos como a IoT.

As características das redes possuem vulnerabilidades que reduzem a eficácia e a eficiência na detecção do ataque Sybil. Esta técnica requer um período maior de avaliação do RSS quando submetida a interferências eletromagnéticas [42, 21, 57]. Em ambientes com alternâncias de mobilidade, a detecção realizada por n_i pode acarretar uma alta taxa de falsos positivos. O aumento desta taxa acontece por que a autenticação com RSS exige um determinado tempo para localizar um dispositivo. Além disso, o ataque Sybil com o comportamento *churn* pode reduzir ainda mais a energia dos nós da rede. Outro fator prejudicial desta técnica é que ela detecta apenas o ataque Sybil com identidades fabricadas, visto que ela desconsidera o não repúdio. O ataque Sybil sob esta técnica de detecção acarreta uma baixa eficácia, visto que ela desconsidera o não repúdio e possui uma taxa de falsos positivos elevada.

3.1.2 Criptografia

As abordagens de detecção baseadas em criptografia de chaves assimétricas, simétricas, ou relacionamento entre os vizinhos em geral requerem dispositivos sem restrição de recursos. As técnicas de criptografia de chaves assimétricas e simétricas podem limitar a eficiência de uma abordagem de detecção em virtude do alto custo para se gerar chaves seguras e manter atualizações nas listas de identidades. A seguir, será descrito o funcionamento de dois trabalhos recentes em redes sem fio que empregam chaves simétricas e assimétricas. Estes trabalhos se destacam pela acurácia da detecção de SA's.

A Figura 3.2 mostra o funcionamento do LSR (do inglês, *Lightweight Sybil Resistance*) que emprega a criptografia simétrica para identificar o ataque Sybil numa rede. Nesta figura, o esquema de criptografia adotado pelo LSR usa uma autoridade certificadora (AC), que concede e revoga as chaves para os nós da rede. Cada nó obtém um par de chaves Pk_i gerado pela AC. A comunicação entre os nós somente se inicia quando a AC

tiver distribuída as chaves para todos os nós e as suas respectivas listas de identidades estiverem atualizadas. A medida que um novo nó se associa à rede, os nós já associados recebem da AC o Pk_i para a atualização das suas listas de identidades. A detecção do ataque Sybil feita pelo LSR é orientada a eventos. Um evento na rede consiste de uma ação realizada por um nó, onde elas variam desde um requisição de associação até a solicitação de uma tarefa para um conjunto de nós. Deste modo, a identificação de um ataque Sybil ocorre no momento da ocorrência de eventos simultâneos por um nó numa rede.

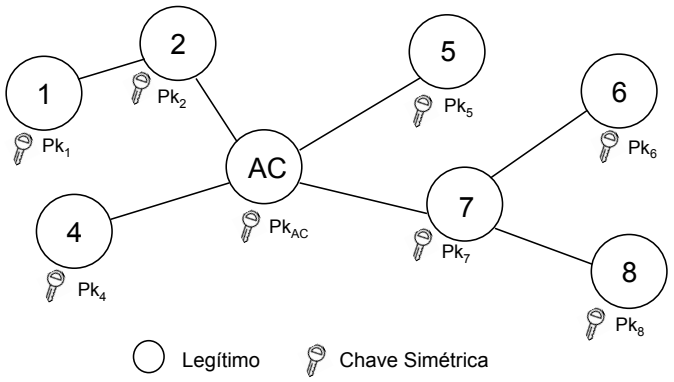


Figura 3.2: Detecção realizada pelo LSR

Como o LSR necessita de um gerenciamento de chaves através de uma AC para identificar o ataque Sybil, o uso de uma AC para a distribuição de chaves limita a escalabilidade na rede por precisar gerar uma chave para todos os nós. Além disso, ela propicia uma sobrecarga na rede devido às constantes atualizações nas listas de identidades dos nós. Logo, ele não é adequado para redes cujos os dispositivos possuam limitação de recursos de comunicação e de processamento. Por outro lado, o uso da criptografia simétrica pelo LSR permite a identificação de ataques Sybil com identidades roubadas e fabricadas. Além disso, como o LSR é orientado a eventos, ele requer apenas a verificação da identidade associada ao evento em sí, o que permite a obtenção de uma alta de detecção. A mobilidade dos nós também não limita a detecção do LSR, por que o seu processo de autenticação desconsidera a localização do nó.

A Figura 3.3 ilustra funcionamento do mecanismo do DAS (do inglês, *Defense Against Sybil Attack*) proposto por [58]. O DAS emprega a criptografia com chaves assimétricas e faz uso de unidades de rodovias (RSU) que realizam a autenticação dos nós da rede por meio de certificados temporários. Quando um nó solicita acesso à rede, a RSU autentica este nó emitindo certificados temporários assinados pela sua chave privadapk_rsu. Em seguida, a RSU que autenticou esse nó compartilha com as outras RSU's o certificado relativo ao nó autenticado. O DAS explora as capacidades espaciais, temporais e a correlação entre os nós da rede para determinar um nó como atacante, assumindo que um nó não pode estar em dois lugares no mesmo tempo. Dessa maneira, um ataque Sybil é

identificado quando um certificado é exibido no mesmo tempo em mais de um lugar da rede.

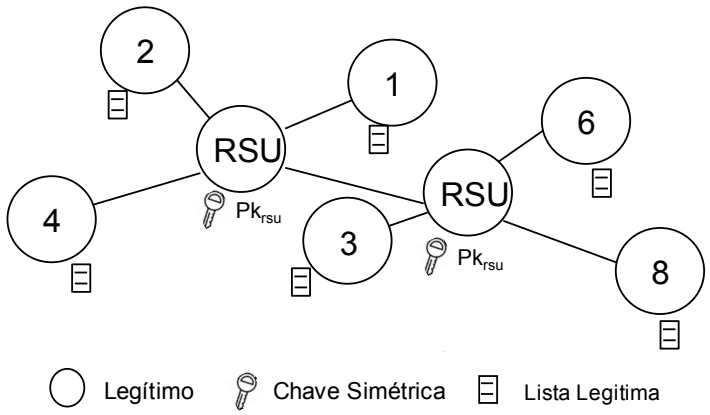


Figura 3.3: Detecção realizada pelo DAS

A necessidade de uma manutenção constante dos certificados dos nós legítimos e dos novos nós prejudica a eficácia do DAS visto que ele precisa destes certificados atualizados para detectar corretamente os atacantes. Logo, se um atacante conseguir um novo certificado antes que todos as RSU's revogue-o, ele pode ser bem sucedido. Para evitar essa falha, o tempo de sincronização entre as RSU's deve ser menor que o tempo de autenticação de um nó. Em redes IoT, a sincronização entre as RSU's torna-se uma tarefa mais difícil de alcançar devido a densidade da rede, compostas por diferentes dispositivos. No entanto, o DAS identifica ambos os tipos de ataque Sybil. Por empregar chaves assimétricas o DAS garante o não repúdio, requisito necessário para a detecção do ataque Sybil com identidades roubadas. Assim, um certificado assinado pela chave privada de uma RSU garante a veracidade daquele certificado. O DAS também possui RSU distribuídos, o que permite uma detecção escalável, mas não resolve a questão da sincronização visto que os certificados são temporários.

3.1.3 Relacionamento entre vizinhos

A Figura 3.4 ilustra o esquema proposto por [25] intitulado MobID que identifica o ataque Sybil através do relacionamento entre vizinhos. Nesta figura, os nós da rede possuem duas listas de identidades, a dos nós legítimos, e a dos intrusos. Em cada uma destas listas estão contidas as identidades dos nós e a sua reputação na rede num dado momento. Um nó ganha reputação a medida com que ele vai cooperando com os outros nós da rede, encaminhando pacotes, realizando sensoriamento, por exemplo. Caso um nó deixe de colaborar, ele perde reputação. A detecção feita pelo MobID requer uma constante atualização da reputação dos nós a partir das opiniões dos seus vizinhos. Assim, a identificação do atacante Sybil acontece quando a parte majoritária dos vizinhos de N_i classificam este nó com uma baixa reputação.

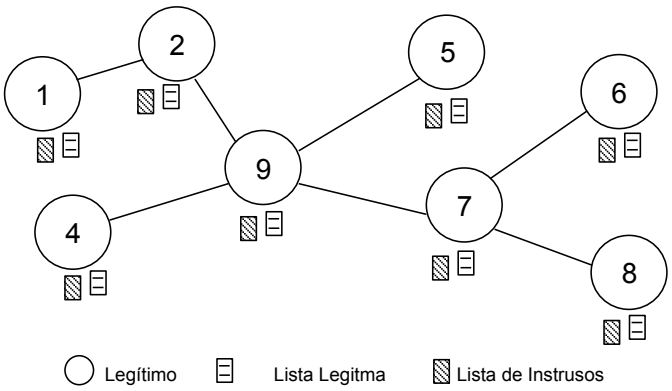


Figura 3.4: Detecção realizada pelo MobID

O relacionamento entre os vizinhos próximos proporciona uma classificação dos nós através das opiniões de vizinhos. Contudo, esta classificação demanda uma sobrecarga na comunicação dos nós da rede, que reduz o tempo de bateria dos nós da rede. No MobID [25], por exemplo, para cada tarefa executada por um nó é necessário a opinião de seus vizinhos sob o comportamento daquele nó, demandando uma comunicação adicional na rede. Além disso, um nó atacante pode enganar o MobID agindo de forma maliciosa, isto é, cooperando com os nós da rede até atingir uma alta reputação. Dessa maneira, um atacante com alta reputação se mantem na rede ludibriando o MobID, obtendo assim informações confidenciais da rede. Por outro lado, como o MobID usa as opiniões dos vizinhos de um nó para a detecção, isto permite uma adaptabilidade e uma rápida atualização do sistema, visto que ele emprega um único parâmetro e ao mesmo tempo tal informação pode ser obtida de qualquer tipo de rede. Embora o MobID possua uma alta acurácia, ela é decorrente do uso de um treinamento offline dos comportamentos maliciosos de modo a calibrar o mecanismo de detecção. Tal estratégia torna-se inadequada para redes IoT.

A detecção baseada no relacionamento entre vizinhos também pode ser aplicada em outros contextos. Nas redes sociais, por exemplo, o mecanismo DSybil [31] detecta SA's baseado nas seguintes asserções: a divisão da rede em dois tipos de comunidade, *Sybil* e usuários legítimos. A maneira com que o DSybil identifica SA's parte do mesmo princípio que o MobID, realizando o monitoramento dos novos nós de modo à detectar possíveis intrusos. Diante do monitoramento das ações de um novo nó, o conjunto dos nós legítimos que realizou a avaliação da conduta deste novo nó julga se ele faz parte da comunidade *Sybil* ou legítima. Caso este nó seja um SA, sua identidade será divulgada na rede e ele será desassociado, caso contrário ele terá continuará presente na rede até um próximo monitoramento.

3.2 Requisitos e métodos de transmissão seguras

A segurança da transmissão de contéudo de uma rede necessita de requisitos e métodos para salvaguardar seus dados. Dentre os requisitos de segurança, o estabelecimento de um canal seguro disponta como uma das alternativas para prevenir o acesso à informações confidenciais dos dispositivos da rede. Este método engloba os princípios de segurança integridade e confidencialidade onde para cada um destes princípios existe uma técnica específica, descritas no decorrer desta subseção. Os outros métodos detalhados nesta dissertação evidenciam a segurança das identidades dos dispositivos da rede. A comprovação e a garantia da identidade são métodos que extraem informações dos próprios dispositivos assegurando os princípios de integridade e confidencialidade. A seguir, as formas encontradas na literatura para garantir os requisitos através dos métodos de transmissões seguras serão apresentados.

3.2.1 Estabelecimento do canal seguro

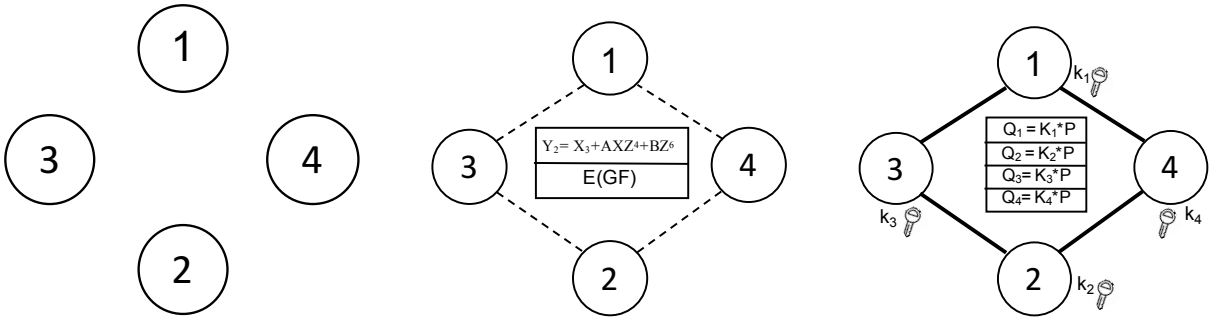
A comunicação entre os dispositivos numa rede necessita de segurança para garantir a privacidade dos dados trafegados. Para que estes dados sejam disseminados de forma segura é preciso estabelecer um canal seguro entre os componentes da rede. Um canal seguro propicia a disseminação de dados confidenciais, onde apenas os dispositivos em comum acordo de chaves e segredos tem acesso à informação. Em redes sem fio, o estabelecimento de um canal seguro tem sido uma alternativa para os dispositivos das soluções trocarem informações de controle e configuração, impedindo que dispositivos não autorizados obtenham essas informações, prejudicando o funcionamento da rede.

Dentre os requisitos de segurança alcançados no estabelecimento de um canal seguro estão a confidencialidade e a integridade. Tanto confidencialidade quanto integridade fazem parte dos três pilares da segurança [59]. O princípio da confidencialidade visa salvaguardar as informações trafegadas na rede, onde apenas dispositivos legítimos ou os que possuam acesso aquela informação a obtenham. Com a confidencialidade é possível garantir a privacidade dos dados de um dispositivo e as suas informações pessoais só serão acessadas apenas pelos que este dispositivo permitir acesso. A integridade lida com o conteúdo da informação garantindo que ela não seja modificada ou alterada. Logo, as técnicas para o estabelecimento de um canal seguro são fundamentadas a partir desses princípios assegurando o funcionamento dos serviços de uma rede de forma segura.

A criptografia de chaves simétricas, assimétricas e de curvas elípticas garantem a confidencialidade, enquanto o hash assegura a integridade da mensagem trafegada pela rede. A criptografia de chaves simétricas é o tipo mais simples de criptografia, já que tanto o emissor quanto o receptor da mensagem possuem a mesma chave, ou seja, a mesma chave é usada tanto na codificação quanto na decodificação. Diferentemente da

chave simétrica, as chaves assimétricas utilizam duas chaves, uma pública e uma privada. A chave pública é usada para encriptar o texto ou para verificar uma assinatura digital. Já a chave privada é usada para a operação oposta, isto é, decriptar o texto cifrado ou para criar uma assinatura digital. A autenticação de mensagens visa aplicar o hash à mensagem para produzir um "resumo", e encriptar o resumo com a chave privada para produzir uma assinatura digital. Dessa forma, é possível verificar essa assinatura, computando o hash da mensagem, e decriptando a assinatura com a chave pública do signatário de modo à comparar o resumo computado com o resumo decriptado.

A Figura 3.5 ilustra o estabelecimento de um canal seguro de modo à garantir a confidencialidade das mensagens trafegadas entre os nós N_1, N_2, N_3, N_4,. Os nós desta Figura 3.5(a) inicializam a rede para que eles possam trocar informações. Com a comunicação estabelecida o primeiro passo para o estabelecimento de um canal seguro é definir a técnica empregada. Para este exemplo uma curva elíptica E foi definida, representada pela a equação $Y^2 = X^3 + AXZ^4 + BZ^6$. Em seguida, um grupo de pontos $E(GF)$ é escolhido de modo à gerar os pares de chaves dos nós dessa rede. O ultimo passo está representado na Figura 3.5(c), onde os pares de chaves são estabelecidos para cada um dos nós da rede através dos pontos obtidos em $E(GF)$ para a chave privada, e $Q_{N_k} = K_{N_k} \times p$ alcançando assim a sua chave pública.



(a) Inicialização dos nós (b) Estab. da curva elíptica (c) Estab. dos pares de chave

Figura 3.5: Estabelecimento de um canal seguro

As características da IoT demandam requisitos para o estabelecimento de um canal seguro. Nesta rede, os dispositivos possuem restrições de recursos, são heterogêneos, e se locomovem com diferentes velocidades. O emprego de técnicas que garantem a confidencialidade e a integridade num estabelecimento de um canal seguro, deve levar em consideração esses requisitos. A criptografia com curvas elípticas tem sido uma alternativa para o estabelecimento de um canal seguro, garantindo assim os princípios de confidencialidade e integridade.

3.2.2 Comprovação e garantia da identidade

A identidade de um dispositivo numa rede garante a sua legitimidade perante aos outros dispositivos contidos nela. Esta legitimidade permite associar ações na rede a um dispositivo assegurando responsabilidade aquela identidade. Os sistemas de detecções de intrusões, por exemplo, usam a identidade de um dispositivo para identificá-lo na rede monitorando assim a sua conduta. Caso este dispositivo realize uma ação maliciosa, a identidade associada a ele sera detectada como uma ameaça à rede. Assim, com a identidade de um dispositivo é possível garantir o princípio da irretratabilidade e assim identificar possíveis atacantes ou ameaças numa dada rede.

A legitimidade da identidade de um dispositivo pode ser alcançada a partir da comprovação de identidades. Nesta técnica, um dispositivo são levados em consideração características que permitem diferenciar este dispositivos dos demais. A função não clonável (PUF) [60, 61] propicia um conjunto de dados obtidos através de ciclos de clocks do processador, por exemplo, identificando de maneira única um dado dispositivo. Outra maneira de assegurar a veracidade de uma identidade consiste no emprego da criptografia baseada na identidade [62, 63, 64]. Nessa prática, a identidade de um dispositivo esta associada a uma chave publica, dispensando mecanismos de autenticação. Assim, a prática de comprovação de identidades em redes tem sido aplicadas com o objetivo de proteger os dados da falsificação e roubo.

O funcionamento da comprovação por meio da PUF está representado na Figura 3.6. Nesta figura, o nó N_4 extrai do seu hardware, neste exemplo um conjunto de dados dos ciclos de clocks do seu processador. Ao obter este conjunto de dados, o nó N_4 pode comprovar a veracidade da sua identidade, garantindo assim a legitimidade desta identidade. Em seguida, a PUF gerada por N_4 então pode servir como uma chave privada do dispositivo, assim como ocorrem na criptografia baseada em identidades, ou até estar associada a uma outra técnica de segurança, como a técnica de recibos por exemplo.

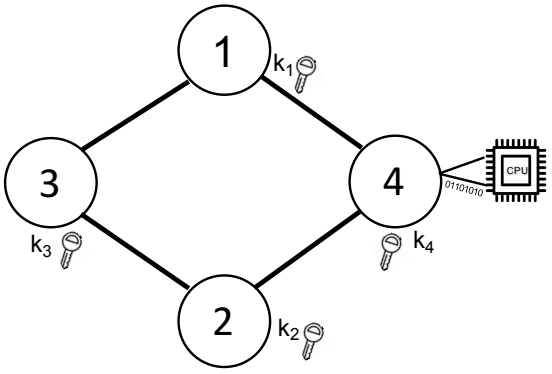


Figura 3.6: Comprovação da identidade

Para garantir a legitimidade das identidades dos dispositivos de uma dada rede a comprovação de identidades precisa lidar com os custos referentes ao processo. Esta técnica

é considerada leve, pois ela simplifica o gerenciamento de chaves publicas por eliminar o uso de certificados digitais, além de reduzir a sobrecarga de comunicação com trocas de mensagens de verificação de certificados e o tempo de resposta das aplicações. Contudo, a comprovação de identidades requer a existência de um canal seguro impossibilitando os atacantes obter essas informações. Na PUF, por exemplo, caso um atacante obtenha o conjunto de dados equivalente a identidade é necessário substituir o processo de geração da comprovação de identidade.

Enquanto a comprovação de identidades ocorre no dispositivo, a garantia da identidade acontece através de uma terceira parte. Na garantia de identidades, uma terceira entidade gera ou certifica a identidade de um dispositivo legítimo assegurando o princípio da irretratabilidade. O recibo de uma identidade gerado por uma central geradora de chaves (KDC), por exemplo, garante a legitimidade da identidade de um dispositivo da rede. Nesta técnica, um dispositivo já conhecido pela rede envia a sua comprovação da identidade, uma chave ou a PUF, e assim o dispositivo KDC da rede emite um recibo de legitimidade daquela identidade. O dispositivo legítimo então pode apresentar a garantia da sua identidade quando for solicitado uma tarefa ou até na sua associação à rede.

A técnica de recibos de identidades tem como objetivo garantir a legitimidade daquela identidade por meio de uma terceira parte. A Figura 3.7 mostra o funcionamento da técnica de recibos [65, 66, 67]. O nó N_4 como nos exemplos anteriores, Figuras 3.5 e 3.6, envia a sua comprovação da identidade (PUF), representada por um conjunto de dados por meio de um canal seguro para N_1. Este nó então atua como uma terceira parte, ou seja, uma entidade legítima da rede que participa do processo de geração do recibo. Ao receber o código PUF de N_4, o nó N_1 executa uma multiplicação entre o código PUF e uma constante qualquer, obtendo o recibo R_4. Em seguida, este nó envia R_4 para o seu respectivo nó. Com R_4 o nó N_4 pode comprovar que a sua identidade é verídica, uma vez que ela já foi gerada por um nó legitimo da rede. A garantia de identidade reduz a

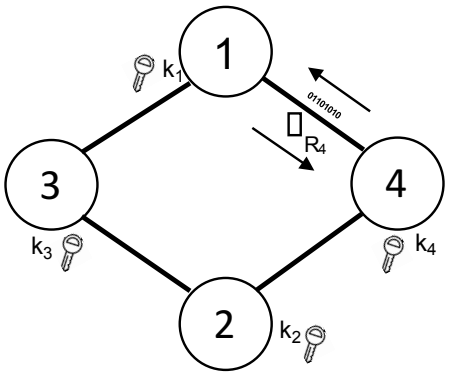


Figura 3.7: Comprovação da identidade

complexidade de verificação da legitimidade de uma identidade, contudo, ela requer uma fase de inicialização. A redução da complexidade acontece por que na garantia de identi-

dade apenas um parâmetro é solicitado, por exemplo, um recibo ou um certificado. Isto diminui a quantidade de passos necessários para se identificar um atacante ou um intruso. Em contrapartida, o estabelecimento de um canal seguro, e uma fase de configuração são necessários para utilizar a técnica de garantia de identidade.

3.3 Resumo

Este capítulo apresentou um estudo sobre os mecanismos de detecção do ataque Sybil (SA), apresentando uma classificação baseada nas técnicas de características da rede, criptografia, e relacionamento entre os vizinhos próximos. Em seguida, estas técnicas são definidas e exemplificadas por meio dos principais trabalhos encontrados na literatura. Além disso, os requisitos de segurança e os métodos para uma transmissão segura foram evidenciados, mostrando a necessidade de se estabelecer um canal seguro para que informações sobre a identidade de um nó sejam compartilhadas de forma confidencial e assim ser gerado a garantia desta identidade.

CAPÍTULO 4

SA^2CI: UM MECANISMO DE DISSEMINAÇÃO SEGURA NA PRESENÇA DE ATAQUES SYBIL PARA A IOT

Este capítulo descreve um mecanismo de controle de associações, chamado SA^2CI (***S**ybil **A**ttack **A**ssociation **C**ontrol for **I**oT*), para prover segurança contra ataques Sybil na disseminação de dados da IoT. A Seção 4.1 apresenta uma visão geral do mecanismo proposto, apresentando onde o SA^2CI atua, as suas formas de detecção, e as suas características. A Seção 4.2 descreve a composição da rede IoT e do serviço de disseminação assumido para a atuação do SA^2CI. A Seção 4.3 discorre sobre o comportamento do ataque Sybil considerado. A Seção 4.4 detalha os componentes do SA^2CI, a operação de cada fase evidenciando as técnicas empregadas para alcançar a disseminação segura de conteúdo. A Seção 4.5 exibe o funcionamento do SA^2CI diante de ataques Sybil.

4.1 Visão geral

O mecanismo proposto tem como objetivo identificar tentativas maliciosas de acesso à rede, realizadas por atacantes Sybil no serviço de disseminação de conteúdo da Internet das coisas (IoT).O SA^2CI atua como um *middleware*, entra as camadas de rede e aplicação, e assegura que os dispositivos, além disso, este mecanismo considera que os nós presentes na rede sejam **heterogêneos**, isto é, apresentam ou não restrições de recursos. A disseminação de dados ocorre de maneira à maximizar o tempo de vida dos nós com limitação recurso, uma vez que o envio de pacotes é uma das tarefas básicas que demanda mais recurso de um nó. Essas características possibilitam a atuação do SA^2CI de forma efetiva numa rede IoT. Como também, o mecanismo usa informações da camada de rede, como o encaminhamento de dados entre os seus nós, e da camada de aplicação, como a troca de chaves e o estabelecimento de segredos compartilhados.

A arquitetura do SA^2CI está organizada em três fases, a inicialização da rede, a configuração da rede, e a gerência da disseminação. A primeira fase tem como objetivo criar um grupo de pontos base para o estabelecimento dos pares de chave dos nós. Nesta fase, os nós da rede entram em acordo para que o grupo de pontos seja compartilhado e cada nó possua uma parte deste, o qual contém os pontos para gerar seus pares de chaves e dos nós. A segunda fase do SA^2CI visa configurar os nós legítimos da rede, gerando a garantia e a confirmação de uma identidade de um nó. Para que isto ocorra, os nós trocam informações de controle para compartilhar informações de segurança de modo a garantir a irretratabilidade dos nós configurados, possibilitando a distinção de uma identidade

legítima de uma forjada. A fase de gerência da disseminação consiste em monitorar e controlar as associações à rede, uma vez que os nós da rede cooperam entre si mensurando o comportamento de uma nova associação ou uma reassociação de um dado nó. A detecção de um ataque Sybil acontece quando uma identidade exibida na associação não condiz com o a garantia da identidade apresentada, ou quando durante uma nova associação um dado nó apresenta um comportamento malicioso.

O SA^2CI também apresenta duas propriedades que auxiliam nas suas etapas. A auto-organização auxilia a fase de configuração da rede. Esta propriedade garante a coordenação e cooperação dos nós da rede para formar um encaminhamento de dados numa disseminação. Já a propriedade de auto-reparação ajuda a gerência da disseminação a manter o controle das associações e restaurar a disseminação na presença de ataques Sybil. Tais propriedades garantem a continuidade da disseminação mesmo com desassociações dos nós móveis e SA's realizando ataques à rede.

4.2 Modelo da rede

A rede IoT é composta por um conjunto de n nós, móveis ou fixos, denotado por $\mathcal{N} = \{N_1, N_2, ..., N_n\}$. Esses nós possuem um comportamento *legítimo* ($\mathcal{N}_L$) ou um comportamento Sybil ($\mathcal{N}_S$), sendo que $\mathcal{N}_L \subseteq \mathcal{N}$, $\mathcal{N}_S \subseteq \mathcal{N}$ e $\mathcal{N}_L \cup \mathcal{N}_S = \mathcal{N}$. Um nó ($\mathcal{N}_L$) não se torna um ($\mathcal{N}_S$) ao longo do tempo, enquanto que ($\mathcal{N}_S$) pode se passar por legítimo. Cada nó legítimo N_i possui apenas uma identidade, denotada por Id_i. O conjunto de todas as identidades do sistema é denotado por Id. A notação utilizada para modelar as entidades do SA^2CI está detalhada na Tabela 4.1.

O conjunto dos nós legítimos $\mathcal{N}_L$ é composto por nós que não possuem restrição de recursos e por nós móveis com recursos limitados, denotados por $\mathcal{N}_{KDC}$ e $\mathcal{N}_{MOV}$ respectivamente. A relação $\mathcal{N}_{KDC} \cap \mathcal{N}_{MOV}$ não existe, pois um dado nó $N_x \in \mathcal{N}_{KDC}$ não pode ser membro de $\mathcal{N}_{MOV}$, e vice-versa. Os nós do conjunto $\mathcal{N}_{KDC}$ são chamados de nós N_{KDC} enquanto os demais são denominados de nós N_{MOV}. O relacionamento entre um nó N_{KDC} e um N_{MOV} ocorre a partir de uma função sobrejetora $F : \mathcal{N}_{KDC} \rightarrow \mathcal{N}_{MOV}$, onde os elementos do subconjunto $\mathcal{N}_{MOV}$ estão associados a um elemento de $\mathcal{N}_{KDC}$. Por outro lado, não existe uma função $F : \mathcal{N}_{MOV} \rightarrow \mathcal{N}_{KDC}$, visto que os nós $\mathcal{N}_{KDC}$ não podem se associar aos nó $\mathcal{N}_{MOV}$ por conta das suas limitações de recursos.

O meio de transmissão dos dados é sem fio, baseado no padrão 802.15.4. A comunicação acontece a partir de um canal assíncrono sujeito à perda de pacotes devido à mobilidade. Os nós da rede, $\mathcal{N}_{MOV}$ e $\mathcal{N}_{KDC}$, disseminam um dado conteúdo para uma origem, onde o modo de disseminação não impõe restrições na capacidade de detecção do SA^2CI. O raio de comunicação de cada nó varia entre 10 e 100 metros, dependendo da capacidade de transmissão de sua antena. A disseminação dos dados ocorre através do envio de fluxos de dados de 64 *bytes*, partindo de uma ou mais origens até um destino.

Tabela 4.1: Notação utilizada no modelo da rede

Notação	Descrição
$\mathcal{N}$	Conjunto de nós da rede
$\mathcal{N}_L$	Nós com comportamento legítimo
$\mathcal{N}_S$	Nós com comportamento Sybil
$\mathcal{N}_{kdc}$	Nós sem restrição de recursos
$\mathcal{N}_{mov}$	Nós com restrição de recursos
Id	Conjunto das identidades da rede
Id_x	Identidade do nó N_x
Id_ρ	Identidades roubadas
Id_φ	Identidades fabricadas
p e q	Dois números primos grandes
K_x	Chave privada do nó N_x
Q_x	Chave pública do nó N_x
$GF(p)$	Corpo finito sobre p
S_x	Segredo do nó N_x compartilhado com o seu KDC
PUF_x	Código PUF do nó N_x
R_{N_x}	Recibo de identidade do nó N_x emitido por seu KDC

A Figura 4.1 mostra o funcionamento do serviço de disseminação. O serviço de disseminação de conteúdo na IoT precisa levar em consideração as características desta rede, uma vez que nela existiram nós com limitação de recursos. Para evitar que os nós do conjunto $\mathcal{N}_{mov}$ gastem seus recursos utilizando o flooding, o modelo da rede adota uma disseminação baseada nas capacidades dos dispositivos [14]. O nó N_5 desta figura dissemina dados para um destino N_{12} tomando como base a transmissão para um nó $\mathcal{N}_{KDC}$. Este nó então dissemina um dado conteúdo para o nó N_6, que repassa para os nós $\mathcal{N}_{KDC}$ N_3 e N_1 e assim o dado chega ao N_{12} destino da disseminação. Dessa maneira, este modelo de disseminação propicia a economia de recursos dos nós $\mathcal{N}_{mov}$ garantindo um maior tempo de sobrevivência na rede.

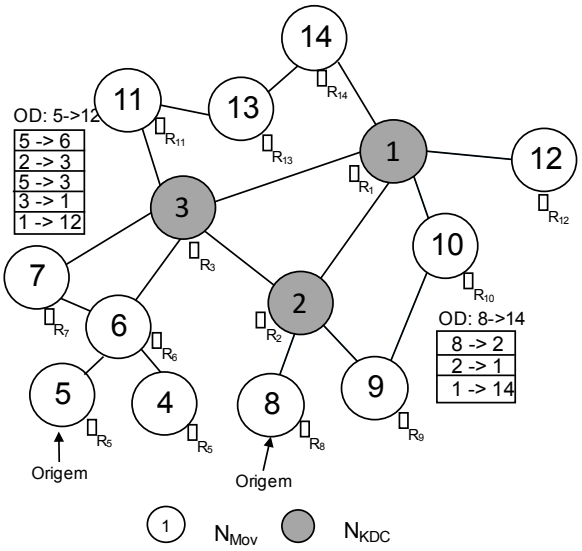


Figura 4.1: Disseminação numa rede IoT

4.3 Modelo do ataque

Um serviço de disseminação de dados na IoT é vulnerável a diversos tipos de ataques. Entre esses, encontra-se o ataque Sybil, em que um nó adversário cria uma ou mais identidades com o objetivo de obter acesso não autorizados ao serviço. Como estas identidades falsas são apresentadas como legítimas, elas violam os princípios da confidencialidade, autenticidade e irretratabilidade, necessários para garantir a segurança da rede. Tais identidades falsas podem ser roubadas (Id_ρ) ou fabricadas (Id_φ), sendo que $Id_\rho \cup Id_\varphi$ compreende o conjunto das identidades forjadas pelos atacantes. Note que $Id_\rho \in Id$ pois foram roubadas de nós legítimos. Por outro lado, $Id_\varphi \notin Id$, visto que é uma identidade fabricada e não está associada a nenhum nó único. Contudo, ambas as identidades estão sob a custódia de um atacante, e o seu uso deve ser impedido pelo SA^2CI. Neste trabalho um ataque Sybil consiste de um nó adversário que cria uma ou mais identidades com o objetivo de obter acesso à disseminação de conteúdo na IoT. Como estas identidades falsas são apresentadas como legítimas, elas violam os princípios da confidencialidade, autenticidade e irretratabilidade, necessários para garantir a segurança da rede.

Um nó Sybil pode apresentar duas formas de comportamento, o primeiro é chamado de *churn* e o segundo de múltiplas identidades. No comportamento *churn* um atacante deve possuir apenas uma identidade falsa, e ele pode entrar e sair muitas vezes da rede, de forma dinâmica, imprevisível, e arbitrária. Nesta conduta, um nó atacante busca promover o esgotamento dos recursos de um nó que realiza a autenticação, e também praticar uma força bruta na tentativa de forjar uma identidade legítima. Já no comportamento de múltiplas identidades, um dado nó atacante deve possuir diversas identidades, solicitando associação à rede. Um atacante com este comportamento se passa por mais de um nó legítimo apresentando identidades aos nós autenticadores com uma frequência baixa, e tentando reproduzir um dispositivo legítimo. Logo, ambos os comportamentos visam ludibriar um nó que executa a autenticação na rede.

A Figura 4.2 ilustra a manipulação de identidades feita por atacantes Sybil, onde as identidades entre chaves (**{}**) foram adulteradas para o acesso à rede. Um atacante com acesso garantido pode prejudicar o resultado de uma votação, obter recursos não autorizados comprometendo a confidencialidade e a privacidade dos dados disseminados. Além disso, um nó Sybil pode apresentar dois tipos de comportamentos: (i) possuir apenas uma identidade falsa mas entrar e sair muitas vezes da rede, de forma dinâmica e imprevisível, ou; (ii) possuir múltiplas identidades falsas. Neste trabalho, o primeiro grupo é chamado de *churn* enquanto o segundo de ataque Sybil com múltiplas identidades. Ao adotar um comportamento *churn*, um atacante entra e sai da rede em um curto período de tempo, sempre solicitando a associação através de uma identidade falsa. Já um atacante com múltiplas identidades solicita associação se passando por mais de um nó legítimo da rede.

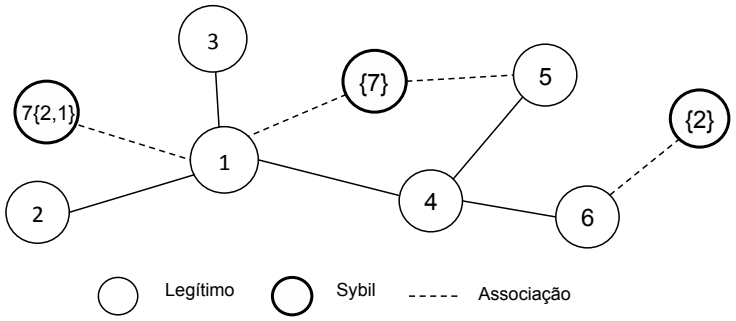
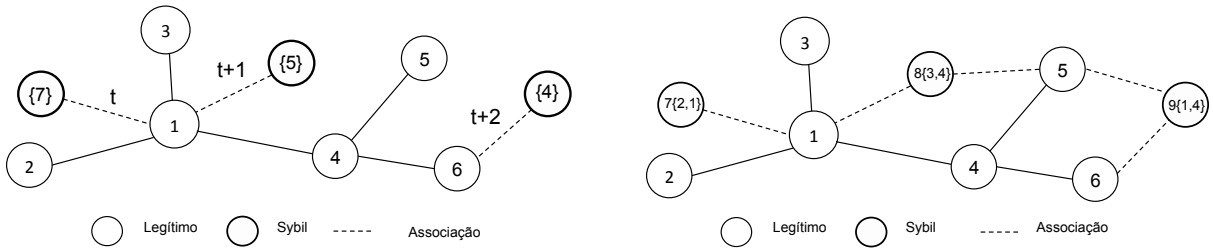


Figura 4.2: Ataque Sybil com ID roubada e fabricada sob a rede IoT

A Figura 4.3(a) exemplifica o comportamento *churn*. Assim, num dado instante de tempo t, o nó atacante 7 seleciona uma identidade, Id_ρ ou Id_φ, e solicita associação ao nó N_1. Caso ele não consiga o acesso, o atacante sai da rede e escolhe uma nova identidade $\{5\}, \{4\}$ respectivamente, para recomeçar o ataque. Nos instantes seguintes, $t+1$ e $t+2$, o atacante executa o mesmo procedimento de entrada e saída da rede, solicitando, em seguida, a associação de sua identidade falsa aos nós N_1 e N_6, respectivamente. Logo, o comportamento *churn* visa ao acesso à rede e também causa o esgotamento dos recursos da rede devido às diversas requisições seguidas.



(a) Churn (b) Múltiplas Identidades

Figura 4.3: Comportamentos do Ataque Sybil

A Figura 4.3(b) ilustra a conduta dos atacantes Sybil apresentando múltiplas de identidades. Nela, os atacantes solicitam associação à rede com mais de uma identidade para N_1, N_5 e N_6. O atacante N_8, por exemplo, com a tupla de identidades Id_3 e Id_4, atua na rede assumindo a identidade Id_3, e posteriormente com a identidade Id_4. Assim, o ataque Sybil com multiplas identidades afeta a confidencialidade da disseminação de conteúdo na rede, tal que ele se beneficia com os dados obtidos pelas multiplas identidades.

4.4 Descrição das fases

O mecanismo de controle de associações para IoT, SA^2CI, baseia-se em três princípios: a função não clonável (PUF) [68], a criptografia de curvas elípticas (ECC) [69], e a técnica de recibos [67]. Nele, a capacidade de detecção de ataques Sybil não é afetada pelo modo de disseminação. Durante a fase de inicialização os nós sem restrição de recursos

formam um KDC, de forma autônoma e distribuída. Para isso, eles estabelecem um curva elíptica e compartilham as informações dessa curva entre si. As curvas elípticas requerem um baixo custo computacional para a distribuição de chaves e possibilitam a criação de canais seguros, sendo atrativas para as IoTs.Na fase de configuração, os nós KDC emitem as chaves públicas e privadas. Essas chaves são geradas para todos os nós, N_{KDC} e N_{MOV}. Em seguida, os N_{KDC} estabelecem chaves de sessão (simétrica) com os seus respectivos nós N_{MOV} a partir das chaves públicas e privadas e de pontos da curva elíptica. As chaves de sessão são utilizadas para a transferência de dados entre um nó N_{MOV} e o seu respectivo N_{KDC}. Ainda nesta fase, um nó computa sua PUF, envia ao N_{KDC}, que gera um recibo associado a esta PUF e à identidade do nó. Na fase de gerência, são realizadas as associações de nós ao serviço de disseminação, considerando a PUF e o recibo de um dado nó, bem como o seu comportamento.

4.4.1 Inicialização

A inicialização da rede tem como objetivo de estabelecer uma ECC entre os nós $\mathcal{N}_{KDC}$. Nesta fase, apenas os $\mathcal{N}_{KDC}$ atuam na rede trocando informações de pares de chaves e do acordo comum de uma curva E por meio de um canal seguro. Este canal seguro só é necessário apenas uma vez, visto que informações confidenciais e de controle são trocadas entre os participantes da rede e não podem ser obtidas por atacantes. O intuito desta fase consiste em gerar uma curva E para que um par de chaves de cada nó $\mathcal{N}_{KDC}$ da rede seja estabelecido.

. .

O estabelecimento dos numeros de uma curva geralmente, A, B, x e y são reais $\mathbb{R}$, complexos $\mathbb{C}$, racionais $\mathbb{Q}$, ou um corpo finito K. Uma dada curva E é um conjunto sobre dois pontos primos p e q de um corpo finito GF. O grupo $E(GF)$ corresponde ao grupo de pontos pertencente à curva E com coordenadas em GF. Um dado ponto $G \in E(GF)$ é um ponto da curva E e a sua ordem é o menor inteiro positivo k tal que $k.p = \infty$. Além disso, a ordem do ponto G sempre divide a ordem do grupo $E(GF)$, obtendo assim um subgrupo base para um conjunto de coordenadas projetivas que dão origem à curva E.

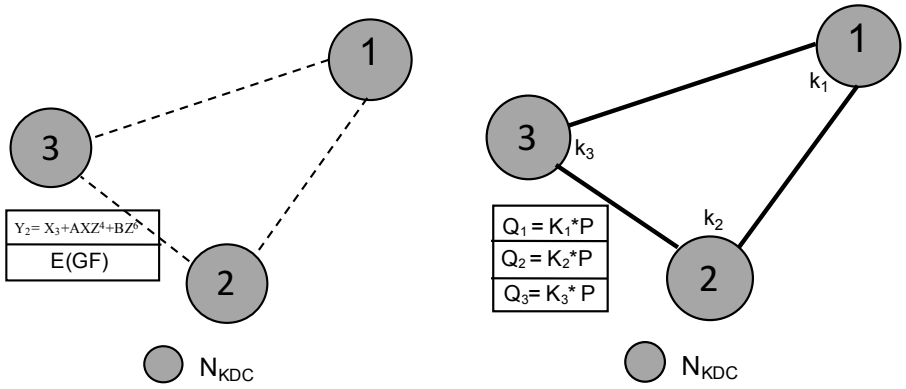
A forma mais comum de se expressar uma curva elíptica é utilizando a equação de Weierstrass [70]. Ela é alcançada por $y^2 = x^3 + Ax + B$, onde A e B são constantes. Geralmente, A, B, x e y são elementos reais, complexos, racionais, e infinitos. Uma curva E é definida sobre dois pontos primos p e q tal que os dois pontos foram obtidos através de um corpo finito GF. O grupo $E(GF)$ corresponde aos pontos pertencentes a E com coordenadas em GF. Um dado ponto $G \in E(GF)$ está contido em E e a sua ordem consiste de um inteiro positivo k tal que $k.p = \infty$. O ponto G também é a ordem dos pontos que divide a ordem do grupo $E(GF)$, obtendo assim um subgrupo base para um conjunto de coordenadas projetivas os quais darão origem a curva E.

A inicialização da rede tem como objetivo estabelecer uma curva elíptica entre os nós $\mathcal{N}_{KDC}$. Nesta fase, apenas os nós $\mathcal{N}_{KDC}$ atuam, trocando informações e estabelecendo uma curva E por meio de um canal seguro. Este canal seguro só é necessário apenas uma vez, visto que informações confidenciais e de controle são trocadas entre os participantes da rede e não podem ser obtidas por atacantes. Desta maneira a curva elíptica é expressa pela equação de Weierstrass, $y^2 = x^3 + Ax + B$, em que A e B são constantes [71]. Geralmente, A, B, x e y são números reais $\mathbb{R}$, complexos $\mathbb{C}$, racionais $\mathbb{Q}$, ou um corpo finito K.

A curva E é um conjunto sobre dois pontos primos p e q de um corpo finito GF. O grupo $E(GF)$ corresponde ao grupo de pontos pertencente à curva E com coordenadas em GF. Um dado ponto $G \in E(GF)$ é um ponto da curva E e a sua ordem é o menor inteiro positivo k tal que $k.p = \infty$. Além disso, a ordem do ponto G sempre divide a ordem do grupo $E(GF)$, obtendo assim um subgrupo base para um conjunto de coordenadas projetivas que dão origem à curva E.

O SA^2CI considera um sistema de coordenadas projetivas jacobianas [71]. Este tipo de coordenada possibilita a representação dos pontos de E em um espaço projetivo P_k, evitando assim multiplicações no grupo $E(GF)$. Isto permite gerar uma curva com menos recursos computacionais quando comparados com o plano de coordenadas homogêneas. No sistema de coordenadas jacobiana um ponto (x, y) é representado por $(X : Y : Z) = (\lambda_x^2, \lambda_y^3, \lambda)$ para todo $\lambda \neq 0$. O ponto ∞ é dado por $(\lambda^2 : \lambda^3 : 0)$. Neste sistema as coordenadas X e Y possuem peso 2 e 3. Assim, a curva E gerada pelos nós $\mathcal{N}_{KDC}$ é alcançada a partir da seguinte equação $Y^2 = X^3 + AXZ^4 + BZ^6$.

Na inicialização, Figura 4.4(a), uma curva E é obtida por meio de um acordo entre os nós $\mathcal{N}_{KDC}$. Para isso, os nós trocam informações sobre os valores x, y, z, a, b. Um dado nó $\mathcal{N}_{KDC}$ gera esta curva por meio da equação $Y^2 = X^3 + AXZ^4 + BZ^6$ já definida.



(a) Geração da Curva Elíptica

(b) Estabelecimento dos pares de chave

Figura 4.4: Inicialização da rede pelos nós $\mathcal{N}_{KDC}$

Em seguida, ele compartilha os valores da curva E, isto é, x, y, z, a, b para os demais nós

$\mathcal{N}_{KDC}$. Com a curva E compartilhada entre os nós $\mathcal{N}_{KDC}$, o próximo passo consiste em configurar os pares de chaves de $\mathcal{N}_{KDC}$ e $\mathcal{N}_{MOV}$, o que ocorre na configuração.

Uma vez gerada a curva, os nós $\mathcal{N}_{KDC}$ utilizam o canal seguro de modo a propagar as chaves obtidas por meio da curva. A Figura 4.4(b) ilustra o processo de obtenção das chaves respectivas aos nós $\mathcal{N}_{MOV}$. Nesta figura, um dado nó N_2 gera os pares de chaves públicas dos nós N_1 e N_3 através do produto k_n * P, onde k equivale a chave privada e P representa um ponto da curva E. Por fim, as chaves públicas e privadas são passadas por meio do canal seguro para os respectivos nós, e assim a rede pode ser inicializada.

Algoritmo 1 Acordo distribuído dos pontos da curva elíptica

```
 1: procedure INICIACURVA(p, q)
 2:     E← {p, q}     // Inicialização da curva
 3:     para cada N_x ∈ N_kdc faça
 4:     N_KDC_x ← {E}     // Atribuição da curva para os nós
 5:     fim para cada
 6:
 7: end procedure
 8:
 9: procedure DISTRIBUIPARTEDACURVA(A, B, x, y)
10:     E(GF)← {A, B, x, y}     para cada N_x ∈ N_kdc faça
11:     N_KDC_x ← {E(GF)}     // Atribuição dos pontos respectivos de cada nó
12:     fim para cada
13: end procedure
```

Na fase de inicialização, Algoritmo 1, uma curva E passa por um acordo entre $\mathcal{N}_{KDC}$ nós. Para isso, os nós trocam informações sobre os valores x, y, z, aeb. Um dado nó $\mathcal{N}_{KDC}$ gera esta curva pela equação já definida: $Y^2 = X^3 + AXZ^4 + BZ^6$. Então, ele compartilha os valores x, y, z, a, b da curva E para os outros $\mathcal{N}_{KDC}$ nós. A segunda parte do Algoritmo 1 consiste em distribuir os valores gerados (l.10) para o $\mathcal{N}_{KDC}$ que participam da primeira parte (l.11). Com a curva E compartilhada entre $\mathcal{N}_{KDC}$ nós, o próximo passo consiste em definir os pares de chaves de $\mathcal{N}_{KDC}$ e $\mathcal{N}_{MOV}$, que ocorre na fase de configuração.

4.4.2 Configuração

A configuração da rede tem o objetivo de estabelecer pares de chaves entre os nós $\mathcal{N}_{MOV}$ e os seus respectivos $\mathcal{N}_{KDC}$, para que sejam transportados de forma segura a PUF e o recibo de cada nó $N_x \in \mathcal{N}_{MOV}$. Nesta fase, os dois tipos de nós, isto é $\mathcal{N}_{MOV}$ e$\mathcal{N}_{KDC}$, participam da configuração. Um nó pode ser configurado na rede através de duas formas: a direta e a indireta. Na primeira forma, um nó $\mathcal{N}_{KDC}$ realiza a configuração de um novo nó. Já na segunda forma, um $\mathcal{N}_{MOV}$ já associado na rede atua como intermediário na configuração entre o novo nó e o seu respectivo $\mathcal{N}_{KDC}$.

Com uma curva elíptica E criada e compartilhada entre os $\mathcal{N}_{KDC}$, o próximo passo consiste em obter os pares de chaves para seus respectivos nós $\mathcal{N}_{MOV}$. Inicialmente, cada nó $N_k \in \mathcal{N}_{KDC}$ gera a sua chave privada através de um ponto $k_{N_x} \in GF(p)$. A chave

pública deste nó é computada por meio da sua chave privada multiplicado pelo ponto $p \in GF$ $Q_{N_x} = K_{N_x} \times p$. Em seguida, os nós $\mathcal{N}_{KDC}$ realizam o mesmo processo de gerar um par de chaves para cada nó $\mathcal{N}_{MOV}$ que esteja próximo da sua área de cobertura.

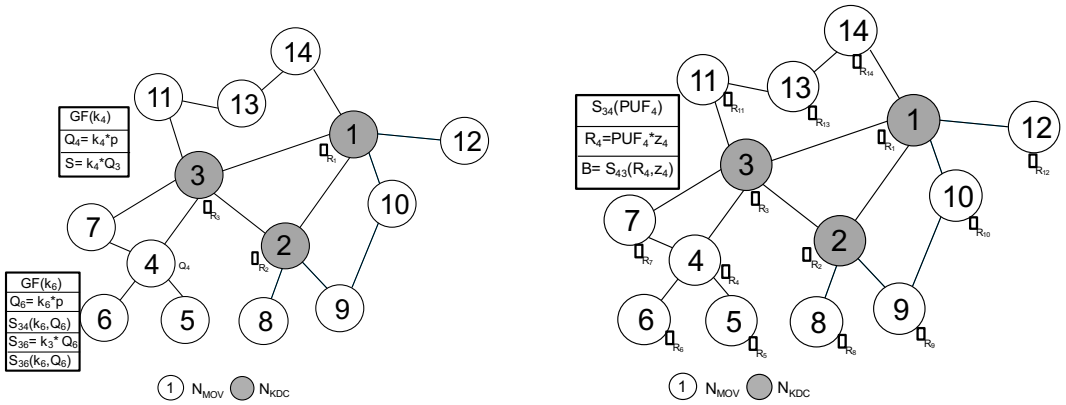
Logo após os o processo de obtenção do par de chaves (K e Q) dos nós $\mathcal{N}_{MOV}$, o nó KDC estabelece um segredo com cada um dos nós $\mathcal{N}_{MOV}$. Para cada nó $N_x \in \mathcal{N}_{MOV}$, o nó KDC correspondente calcula o segredo $S_x = Q_{N_x} \times K_{kdc}$, em que Q_{kdc} é a chave pública do nó KDC disponível publicamente. O estabelecimento do segredo entre um nó $\mathcal{N}_{MOV}$ e seu respectivo $\mathcal{N}_{KDC}$ visa a proteção do código PUF de um nó contra ataques de *Man in the Middle*, escutas, entre outros. Assim, a configuração do recibo de um dado nó $\mathcal{N}_{MOV}$ inicia quando, este nó cifra $S_x = (PUF_x)$ e envia para o seu respectivo $\mathcal{N}_{KDC}$.

Com o segredo compartilhado entre um nó e o seu respectivo KDC, o próximo passo consiste em cada nó $\mathcal{N}_{MOV}$ enviar o seu código PUF_x ao nó KDC, comprovando a sua identidade. A PUF dos nós é um código único extraído do hardware destes nós que permite a identificação única deste nó. Este código é computado através da diferença de ciclos de clocks do processador, ou até das imperfeições geradas no processo de fabricação de um componente do hardware deste nó. Assim, cada nó $N_x \in \mathcal{N}_{MOV}$ envia sua PUF_x cifrada com o segredo (S_x) compartilhado com o seu respectivo KDC através de um canal seguro estabelecido por meio deste segredo.

O nó KDC recebe então a PUF de cada nó $N_x \in \mathcal{N}_{MOV}$, e com este códigos gera os respectivos recibos para seus nós. Este nó gera o recibo de identidades a partir da PUF de um dado N_x e com um ponto $z \in E$, obtendo $R_{N_x} = \text{PUF}_x \times z$. Em seguida, cada KDC cifra o R_{N_x} com o segredo compartilhado dos seus N_x e os envia juntamente com o ponto z da curva. Ao final deste processo, cada nó N_x recebe o seu R_{N_x} e com ele um nó pode obter acesso à rede IoT e seus serviços. Por fim, os nós KDC's da rede atualizam a sua lista de recibos gerados de modo que todos os KDC's possuam os R_{N_x} legítimos, permitindo a sua verificação a partir de qualquer requisição de um dado nó da rede.

A Figura 4.7 ilustra o funcionamento da configuração dos nós $\mathcal{N}_{MOV}$ realizada pelos nós $\mathcal{N}_{KDC}$. No exemplo da Figura 4.5(a), N_3 gera um par de chaves privada K_4 e pública Q_4 para N_4. Com a chave pública de N_4, N_3 emite um segredo S_4 e compartilha com N_4 para que eles possam trocar informações de forma segura. Este processo acontece para todo $N_i \in \mathcal{N}_{MOV}$. Em seguida, N_4 usa o segredo S_4 para cifrar a sua PUF_4 e enviá-la à N_3. Ao receber a PUF_4 de N_4, N_3 emite o recibo de identidade para esse nó (Figura 4.5(b)). Para gerar o recibo de N_4, o nó N_3 escolhe aleatoriamente um ponto de E no qual será multiplicado pela PUF_4, e obtém R_{N_4}. Logo após criar R_4, N_3 envia a garantia da identidade ao nó N_4. O processo de configuração que foi descrito para o nó N_4 acontece para todos os restantes N_x da rede. Assim que o nó for configurado, ele pode utiliz para realizar uma requisição de acesso à rede, comprovando a legitimidade da sua identidade.

O Algorítmo 2 mostra a configuração de um nó na rede. Inicialmente um dado $\mathcal{N}_{MOV}$



(a) Comprovação da Identidade (b) Garantia da Identidade

Figura 4.5: Configuração dos nós $\mathcal{N}_{MOV}$

precisa receber o seu par de chaves, na qual as linhas ($l.2$) a ($l.7$) demonstram o processo de estabelecimento deste par de chaves a um nó N_x. Com o seu par de chaves, este

Algoritmo 2 Garantia da irretratabilidade dos nós da rede

1: **procedure** CONFIGURAPARDECHAVES($GF(p)$)
2: **para cada** $N_x \in N_{mov}$ **faça**
3: $K_{N_x} \leftarrow \{GF(p)\}$ $Q_{N_x} \leftarrow \{K_n \times p\}$
4: $Pardechaves_n \leftarrow \{K_n, Q_n\}$ // Estabelecimento do par de chaves de um nó
5: **fim para cada**
6: **retorna**
7: $Pardechaves_n$
8: **end procedure**
9:
10: **procedure** CONFIGURASEGREDO(Q_n)
11: **para cada** $N_x \in N_{mov}$ **faça**
12: $S_{n,kdc} \leftarrow \{Q_{N_x} \times K_{N_kdc}\}$ // Segredo compartilhado entre um nó e seu kdc
13: $S_{kdc,n} \leftarrow \{K_{N_x} \times Q_{N_kdc}\}$ // Segredo compartilhado entre um kdc e seu nó
14: $envia(S_{n,kdc}, N_x, N_{kdc})$ // Envio do segredo compartilhado entre um kdc e seu nó
15: $envia(S_{n,kdc}, N_{kdc}, N_x)$ // Envio do segredo compartilhado entre um kdc e seu nó
16: **fim para cada**
17:
18: **end procedure**
19:
20: **procedure** CONFIGURARECIBO(Q_n)
21: **para cada** $N_x \in N_{mov}$ **faça**
22: $envia(S_{n,kdc}(PUF_{N_x}))$
23: $decript_{kdc}(S_{n,kdc})$ // Recebimento e decriptação do segredo entre um kdc e um nó
24: $z_{N_x} \leftarrow \{E(GF)\}$
25: $R_{N_x} \leftarrow \{PUF_{N_x} \times z_{N_x}\}$ // Criação do recibo
26: **fim para cada**
27: **retorna** $envia(S_{kdc,n}, (R_{N_x}, z_{N_x}))$
28: **end procedure**
29:

nó em conjunto com o seu $\mathcal{N}_{KDC}$ emitem um segredo compartilhado, criando assim um canal seguro entre eles. Em seguida, este nó criptografa a sua PUF e envia para o seu respectivo $\mathcal{N}_{KDC}$, ($l.20$) que irá configurar o recibo deste nó. O nó $\mathcal{N}_{KDC}$ gera o R_{N_x}

através da PUF deste nó com o ponto z_{N_x}. Por fim, este nó retorna o uma dupla para N_x, (l.25), contendo R_{N_x} e z_{N_x}.

4.4.3 Gerência da disseminação

A fase de gerência da disseminação realiza o monitoramento das requisições de associações dos nós $\mathcal{N}_{MOV}$ e dos novos nós que desejam o acesso à disseminação através do uso de identidade e do recibo. Uma associação à rede consiste de uma requisição de acesso, onde o nó solicitante envia a sua identidade e seu recibo, no caso de reassociação, ou apenas envia uma nova associação se este nó seja novo na rede. Diante disso, um atacante Sybil visa o acesso à disseminação utilizando identidades roubadas ou fabricadas com comportamentos churn e com múltiplas identidades. A forma como os atacantes obtém identidades não tem impacto no mecanismo. Um ataque Sybil não pode se tornar legítimo, ou seja, ter um comportamento legítimo durante a associação. Dessa maneira, esta fase identifica ataques Sybil por meio de requisições de associação à rede através da análise do comportamento e de recibo de identidades.

Quando um nó que não foi configurado e deseja acesso à rede, ele realiza uma nova associação. Numa nova associação, inicialmente este nó, N_x, deve ser avaliado para que o seu comportamento não seja malicioso, isto é, churn ou multiplas identidades. Para isso, tanto um $\mathcal{N}_{MOV}$ quanto o $\mathcal{N}_{KDC}$ monitoram o comportamento durante à associação deste nó à rede, verificando se este comportamento é ou não malicioso através das assinaturas maliciosas conhecidas por tais nós. Tais assinaturas consistem em entrar e sair várias vezes da rede mudando de identidade sempre quando o SA realizar uma nova associação ou exibir múltiplas identidades. Uma nova associação enviada por N_x compreende de apenas um campo, a identidade $< id_n >$ de N_x. Este nó também pode ser autenticado de forma direta e indireta. Assim, N_x tem acesso concedido à rede se este nó tiver comportamento legítimo, ele será configurado na rede, recebendo um recibo equivalente aquela identidade apresentada.

O Algoritmo 3 detalha como acontece a detecção de um atacante por meio de novas associações e reassociações. A confirmação da identidade (l.3) verifica se a identidade apresentada na solicitação já existe na rede, caso exista ela será tratada como reassociação, se não existir esta associação é nova. Para uma reassociação um dado mov_i já possui R_{N_x}, id_n, e comportamento conhecidos. Assim, é preciso verificar a veracidade de R_{N_x} com id_n (l.12) feita de forma direta ou indireta. Enquanto que numa nova associação o comportamento de um nó mov_i é desconhecido, e sendo necessário o seu monitoramento. Dessa maneira, um dado nó autenticador monitora o comportamento de R_{N_x} a partir das assinaturas conhecidas de SA's com churn, $\delta_{solicitacao} > t$, e múltiplas identidades,$qtd_{id} \leq 1$, descritas na (l.25). Caso R_{N_x} tenha um comportamento legítimo ele será configurado. Diante disso, o SA^{2}CI identifica SA's com identidades roubadas e fabricadas e também

com os comportamentos churn e múltiplas identidades. A próxima Seção descreve a operação deste mecanismo desde a fase de inicialização até a detecção de SA's na fase de gerência.

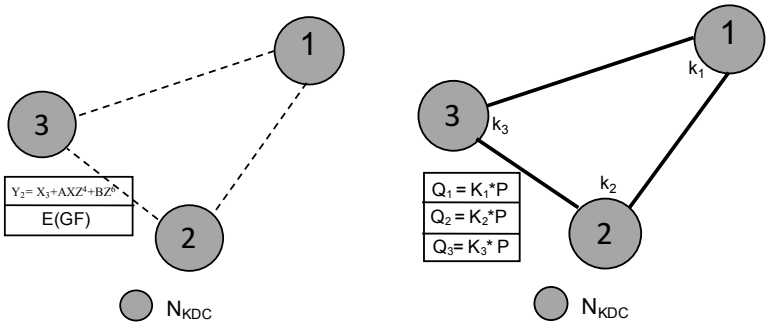
Algoritmo 3 Controle de Associações

```
1: procedure ConfirmacaodaIdentidade(id)
2:     solicitacao ← {id_i, R_{N_x}, z_{N_x}}
3:     se id_i ∈ Id então    // verificação da identidade de um nó mov_i
4:     Vreq ← (solicitacao)
5:     senão
6:     Novaassociacao ← (solicitacao)
7:     fim se
8: end procedure
9:
10: procedure ControledaRequisicao(solicitacao)
11:     para cada solicitacao faça
12:     se R_{N_x} ⊂ id_i então
13:     autentica ← (mov_i)
14:     senão
15:         Id ← id_i − {R_{N_x}}    // desassocia a id_i do recibo apresentado
16:     desassocia ← (mov_i)
17:     fim se
18:     fim para cada
19:
20: end procedure
21:
22: procedure Novaassociacao(solicitacao)
23:         qtd_id ← ∑ id_i
24:     para cada mov_i ∈ N_mov faça
25:     se (qtd_id ≤ 1) ou ( δ_solicitacao > t ) então    // verificação do comportamento de mov_i
26:     configura ← (mov_i)    // Fase de configuração do nó para obter o recibo
27:     senão
28:     desassocia ← (mov_i)
29:
30: end procedure
```

4.5 Funcionamento

A inicialização da rede feita pelo SA^2CI inicia a partir da comunicação entre os nós $\mathcal{N}_{KDC}$ da rede de modo a criar uma curva elíptica E compartilhada entre estes nós. Nesta fase apenas os nós $\mathcal{N}_{KDC}$ participam da inicialização da rede. A Figura 4.6 mostra o processo de formação de E estabelecida por meio de um canal seguro entre estes nós. Logo após o canal seguro ser estabelecido, em um tempo t, os nós N_1, N_2, N_3 entram em acordo para construir uma curva elíptica E através da equação de Weierstrass $Y^2 = X^3 + AXZ^4 + BZ^6$. O nó N_1 no tempo $t + 1$ escolhe os pontos p e q por meio do grupo $E(GF)$ e define a curva base para o calculo do par de chaves destes nós.

Com a curva E estabelecida, os nós $\mathcal{N}_{KDC}$ realizam o calculo dos seus pares de chave. O nó N_1, seguindo o exemplo, obtêm a sua chave privada K_1 e dos respectivos vizinhos

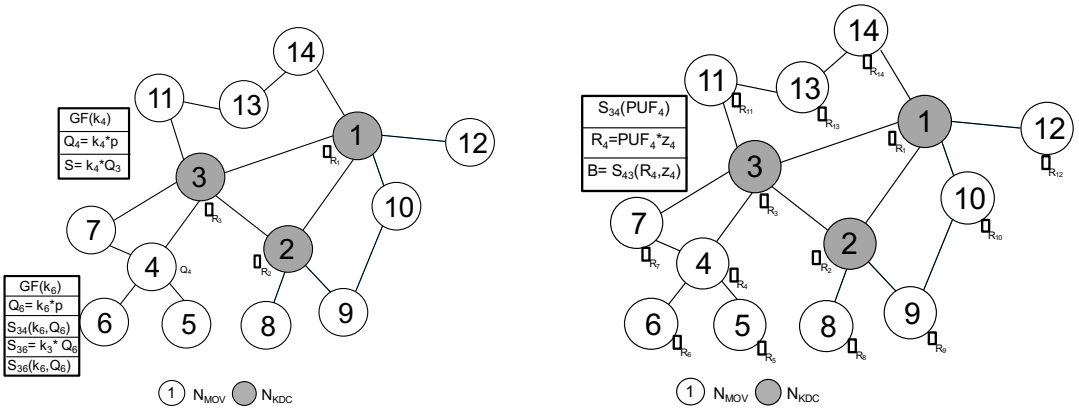


(a) Estab. do canal seguro (b) Criação do recibo

Figura 4.6: Acordo distribuído dos pontos da curva elíptica

K_2, K_3 através do grupo E(GF). Em seguida, ele computa a chave pública Q_1, Q_2, e Q_3. A curva E compartilhada entre os nós N_1, N_2, N_3 permite a configuração de novos pares de chaves e seus respectivos nós $\mathcal{N}_{MOV}$. Assim, estas chaves quando estabelecidas possibilitam a criação de um segredo entre um $\mathcal{N}_{KDC}$ e seu $\mathcal{N}_{MOV}$ de modo que tal nó receba o seu recibo de identidade.

A Figura 4.7 ilustra o funcionamento da configuração dos nós $\mathcal{N}_{MOV}$ realizada pelos nós $\mathcal{N}_{KDC}$. Nesta fase, os pares de chaves de $\mathcal{N}_{MOV}$ são gerados e distribuídos. Diante



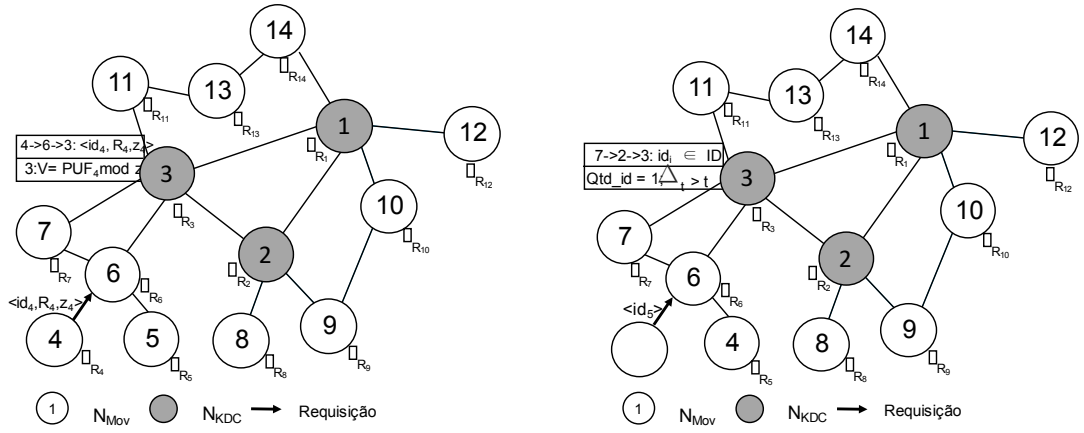
(a) Distribuição dos Pares de Chave (b) Criação do recibo

Figura 4.7: Estabelecimento do recibo

disso, na Figura 4.7 (a) N_3 gera um par de chaves, privada K_4 e pública Q_4 para N_4. Com a chave pública de N_4, N_3 emite um segredo S_4 e compartilha com N_4 para que os dois nós troquem informações sob um canal seguro. Este processo acontece para todo $N_i \in \mathcal{N}_{MOV}$, e ocorre de forma direta ou indireta. Em seguida, N_4 usa o segredo S_4 para cifrar a sua PUF_4 e enviá-la à N_3. Ao receber a PUF_4 de N_4, N_3 emite o recibo de identidades deste nó. Para gerar o recibo de N_4, o nó N_3 escolhe aleatoriamente um ponto de E no qual será multiplicado pela PUF_4 de modo à obter R_{N_4}. Logo após criar R_4, N_3 envia a garantia da identidade à N_4. Com a sua garantia da identidade o nó N_4 pode realizar uma requisição de acesso à rede, e assim comprovar a legitimidade da sua

identidade com o seu recibo.

Com os nós $\mathcal{N}_{MOV}$ configurados, o serviço de disseminação inicia e também a gerência das associações à rede do SA^2CI. A Figura 4.8 mostra o funcionamento da gerência da disseminação, onde os nós da rede autenticam as reassociações e as novas associações, evitando que ataques Sybil consigam acesso à rede e ao serviço de disseminação. Para uma reassociação, N_4, por exemplo, faz uma requisição ao nó autenticador, N_1, contendo uma tripla, a sua Id_4, o seu respectivo recibo R_{N_4}, e o ponto z_4 usado para gerar o seu recibo. O nó N_1 então verifica se a identidade apresentada na requisição equivale ao recibo,R_{N_4}. Esta verificação acontece através de $V = PUF_{N_4} mod z_{N_4}$, onde ela resulta na veracidade do recibo. Se o recibo apresentado na requisição for verdadeiro, N_1 concede o acesso deste nó à rede, caso contrário um ataque é identificado e este nó é desassociado da rede. Já em uma nova associação, o nó N_5, por exemplo, não possui recibo nem seu comportamento é conhecido na rede. Diante disso, a sua conduta deve ser avaliada pelo nó autenticador por meio de assinaturas maliciosas como, o churn, e exibindo múltiplas identidades conhecidas pela rede. Ao avaliar a conduta de N_5, vide Figura 4.8 (b), o nó N_1 pode detectar um comportamento malicioso dessociando este nó, ou caso contrário, ele será configurado na rede de forma direta ou indireta.



(a) Reassociação (b) Nova Associação

Figura 4.8: Monitoramento das associações da rede

A detecção do ataque Sybil realizada pelo SA^2CI está representada na Figura 4.9. O nó N_4, identifica um SA, S_1, no momento que este nó exibe múltiplas identidades através de uma tripla $< id_2, id_5, id_4 >$ durante uma associação à rede. A detecção deste nó acontece quando N_4 monitora a conduta de S_1 verificando as assinaturas maliciosas conhecidas por ele, isto é, churn ou múltiplas identidades. O nó N_4 então detecta uma requisição maliciosa e desassocia esse S_1da rede. Um SA também pode utilizar o comportamento churn para realizar uma associação à rede. Diante disso, os nós id_{10} e id_{12} identificam essa conduta maliciosa uma vez que nos tempos t e $t+1$ o nó S_2 realizou associações num tempo menor que a assinatura $\delta_{solicitacao} > t$. Por fim, o SA S_3 visa acesso ao serviço de disseminação por meio de uma identidade forjada id. Assim, o nó N_9 detecta o S_3 de modo indireto, ou seja, este nó envia a tupla $< id, R_n >$ para o nó KDC N_9 cifrada com o seu segredo $S_{9,2}$ para que ele verifique a veracidade de R_n.

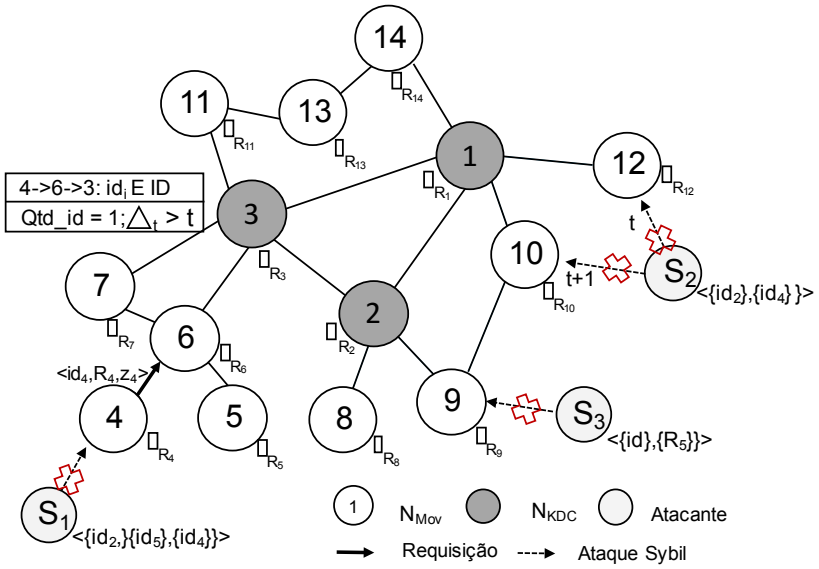


Figura 4.9: Detecção do SA

4.6 Resumo

Este capítulo apresentou a descrição do mecanismo SA^2CI para o controle de associações resistente ao ataque Sybil para IoT. O modelo de rede e do ataque foram descritos, mostrando as suas características, e a disseminação de dados. Em seguida, o mecanismo de detecção do ataque Sybil foi especificado a partir das suas três etapas. Por fim, a operação do SA^2CI foi demonstrada evidenciando as três fases e a detecção de SA's com identidades roubadas e fabricadas e com o comportamento churn e múltiplas identidades.

CAPÍTULO 5

AVALIAÇÃO DO SA^2CI

Este capítulo descreve a avaliação do mecanismo SA^2CI para o controle de associações à disseminação de conteúdo da IoT. A avaliação considera métricas de desempenho quanto e segurança de modo à mensurar a adequabilidade com a IoT e a detecção do ataque Sybil. A Seção 5.1 descreve o cenário utilizado para a simulação. A Seção 5.2 apresenta os parâmetros utilizados na simulação e as métricas empregadas na para aferir o desempenho e a segurança dos mecanismos SA^2CI e o LSD. Por fim, a Seção 5.3 apresenta uma análise onde se discute os resultados obtidos nos cenários avaliados.

5.1 Cenário da simulação

A avaliação de desempenho do SA^2CI e do LSD (Lightweight Sybil Attack Detection) [42] foi conduzida no simulador de redes NS3, versão 3.24, onde foram utilizados a biblioteca crypto++, versão 5.63, para a implementação das curvas elipticas, e a classe *energy model* para o consumo energético, assim como a função PUF. Os cenários de avaliação representam ambientes realísticos a uma rede IoT como, uma residência inteligente *SmartHome* e um hospital *eHealth*. Nestes cenários os objetos e dispositivos disseminam dados sob a presença do ataque Sybil (SA) decorrentes de identidades fabricadas e roubadas, e possuindo comportamentos churn e exibição de múltiplas identidades. Nesta avaliação, assume-se que o modo de disseminação não impõe restrições na capacidade de detecção dos mecanismos, e a forma como os atacantes obtém as identidades não tem impacto neles. Os cenários ilustrados nas Figuras 5.1 e 5.2, onde estão presentes os dispositivos e objetos respectivos a cada um destes ambientes.

Os mecanismos foram avaliados num cenário residencial como o descrito em [72], onde assume-se que o modo de disseminação não impõe restrições na capacidade de detecção dos mecanismos, e na forma como os atacantes obtém as identidades. Neste cenário, os objetos, por exemplo, refrigerador, televisão, e *smartphone*, representam os nós da rede. Estes nós disseminam um fluxo de dados a um destino que os encaminham para aplicações na Internet, de modo a prover serviços em tempo real. Um fluxo de dados, neste ambiente, consiste no envio de uma mensagem de 127 bytes, isto é, *payload* e cabeçalhos que seguem o padrão das redes 6LoWPAN. A escolha dos nós origem e de um nó destino dos fluxos acontece de forma aleatória e os nós origem não podem ser o destino. Os nós atacantes visam o acesso à disseminação através do uso de identidades forjadas, com comportamentos churn e exibindo múltiplas identidades.

A avaliação conduzida no cenário hospitalar está representada pela Figura 5.2. Neste ambiente, os objetos e dispositivos equivalem à *smartphones*, tablets, equipamentos hospitalares com poder computacional, os quais para esta avaliação representam os nós da rede IoT. Eles disseminam fluxos de dados até um destino, o qual irá interagir com aplicações e usuários finais provendo serviços especializados, como o monitoramento dos dados vitais, e até a telemedicina.

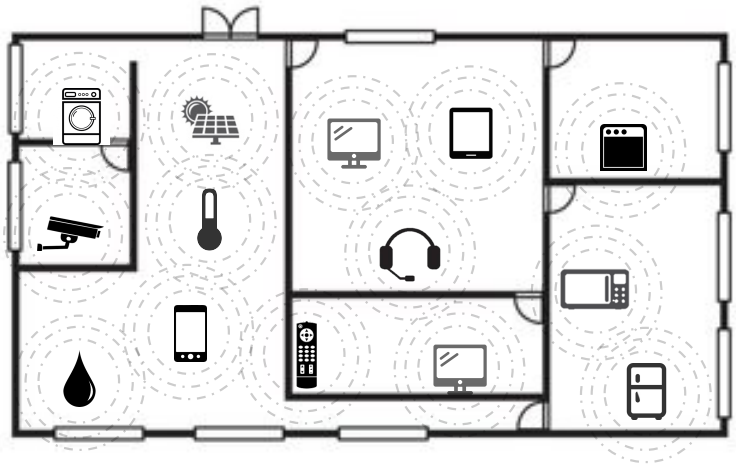


Figura 5.1: Cenário SmartHome

Um fluxo de dados disseminados consiste do envio de mensagens de 127 bytes a um destino. Ademas, o cenário *eHealth* difere do primeiro cenário em questões dimensionais, onde para este ambiente a área é de 250m x 250 m enquanto que o cenário *Smart Home* possui 25m x 25 m.

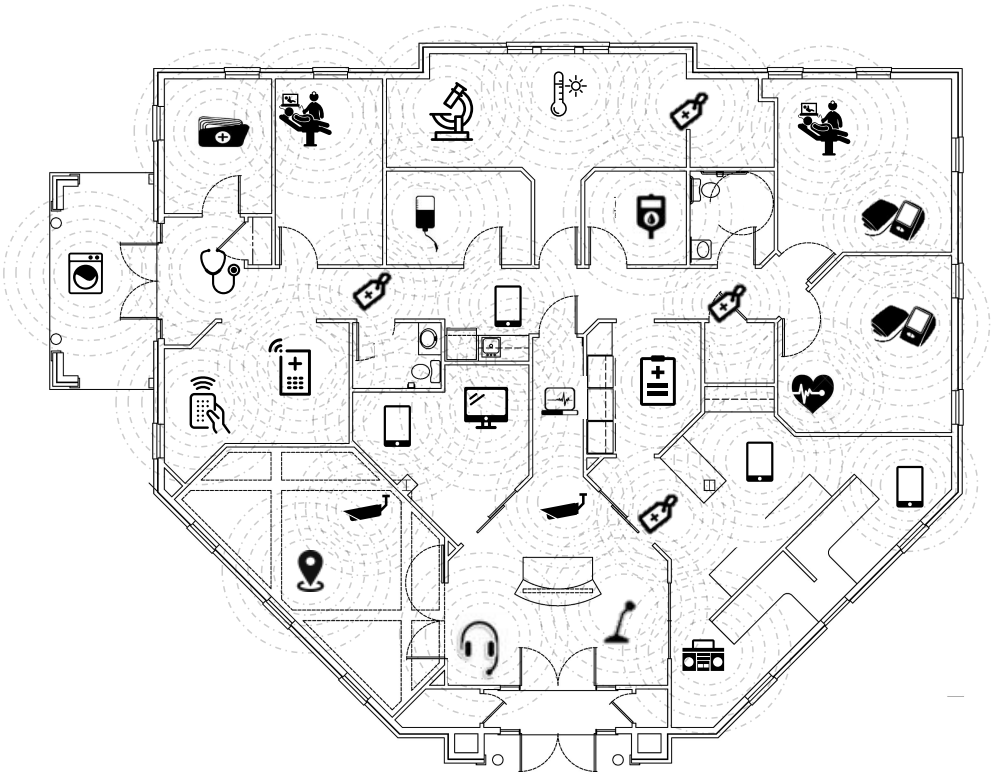


Figura 5.2: Cenário eHealth

5.2 Parâmetros e métricas

Nos cenários avaliados os parâmetros foram configurados pelas perspectivas da rede e do SA. Os parâmetros relacionados à rede IoT e do SA foram obtidos nos trabalhos encontrados na literatura, os quais diz respeitam a IoT e seus ambientes, como saúde [73], cidade inteligente [74], e veicular [75], assim como os do SA [42, 21, 19, 58]. Os oito parâmetros da rede IoT considerado nesta avaliação são, a *Área*, a *Quantidade de nós*, o *Raio de alcançe*, o *Modelo de mobilidade*, a *Velocidade dos nós*, o *Tempo de simulação*, o *Tamanho do pacote*, e a *Tecnologia*. Para o SA, dois parâmetros são considerados, a porcentagem dos *Nós Sybil*, e a *Quantidade de Multiplas ID's*.

A Tabela 5.1 resume os parâmetros usados na configuração da rede IoT e do ataque Sybil. A quantidade de nós variou entre 20, 40, e 60. Estes nós podem apresentar mobilidade $\mathcal{N}_{MOV}$ ou serem fixos $\mathcal{N}_{KDC}$, e se deslocam usando o modelo de mobilidade aleatória com velocidades variando entre 0.2m/s a 2m/s. A comunicação entre os nós da rede adota o padrão 802.15.4, visto que é o padrão mais usado considerando as características das redes IoT. A simulação foi executada 30 vezes com o intervalo de confiança de 95%, e cada rodada durou 600 segundos. Nos parâmetros relacionados ao ataque Sybil, a quantidade de atacantes compreende 10% do total de nós, e o comportamento do ataque com múltiplas identidades varia entre uma à cinco identidades por ataque.

Parâmetro	**Valores**
Área	$25m$x$25m$
Quantidade de nós	20,40,60
Raio de alcance	$10m$ e $100m$
Modelo de mobilidade	Random Waypoint
Velocidade dos nós	0,2m/s a 2m/s
Tempo de Simulação	600 s
Tam. do pacote	127 Bytes
Tipo do pacote	UDP
Protoc. de roteamento	RPL
Período transiente	40s
Protoc. de enlace	IEEE 802.15.4
Nós Sybil	10%
Quant. Múltiplas IDs	1 a 5

Tabela 5.1: Parâmetros de Simulação

As métricas utilizadas na avaliação da eficácia do mecanismo SA^2CI e do LSD são: ***Taxa de Detecção*** (T_{det}), ***Acurácia*** (A_c), e ***Falsos Positivos*** (T_{fp}), o ***Tempo médio entre falhas*** ($MTBF$), e o ***Tempo médio de reparo*** ($MTTR$)d. Já ***Consumo Energético*** (CE) e a ***Sobrecarga do SACI*** (SS) medem a eficiência destes mecanismos. Dessa maneira, estas métricas serão detalhadas a seguir.

A ***Taxa de detecção*** (T_{det}) contabiliza os ataques Sybil identificados corretamente pelo SA^2CI a partir de reassociações e novas associações. O cálculo da T_{det} corresponde a razão entre o total de detecções, det_{ni}, e quantidade de ataques, $Tatq$, (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 avaliado.

$$T_{det} = \frac{\sum det_{ni}}{Tatq} \tag{5.1}$$

A segunda métrica, ***Acurácia*** A_c, indica a precisão da detecção do SA^2CI. 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 A_c também resulta em valores discretos e seus valores diz respeitam a precisão na detecção dos mecanismos avaliados.

$$A_c = \frac{\sum det_{ni} + \sum det_{na}}{Treq} \tag{5.2}$$

A ***Taxa de falsos positivos*** T_{fp} determina a quantidade de vezes que o SA^2CI identificou um ataque Sybil quando não existia o ataque. O seu cálculo acontece através da divisão entre a quantidade de detecções, det_{ni}, pelo total de requisições legítimas, $Treq_l$, (Eq. 5.3).

$$T_{fp} = \frac{\sum det_{ni}}{Treq_l} \tag{5.3}$$

O ***Tempo médio entre falhas*** $MTBF$ identifica o intervalo de tempo entre falhas do mecanismo na detecção de um ataque. O $MTBF$ é alcançado através de um intervalo de tempo T em que uma falha ocorre até o seu fim em relação ao número de falhas d eq.(5.4). Assim, é possivel avaliar a confiabilidade dos sistemas sob a presença de ataques Sybil.

$$MTBF = \frac{T}{d} \tag{5.4}$$

O ***Tempo médio de reparo*** $MTTR$ calcula o intervalo de tempo gasto para se recuperar uma falha causada por um atacante. O calculo do $MTTR$ é realizado por meio da quantidade de tempo T_i que o sistema ficou reparando uma falha d eq. 5.5. Esta métrica afere a capacidade do sistema se restabelecer na presenca de falhas.

$$MTTR = \frac{\sum_{i=1}^{d} T_i}{d} \tag{5.5}$$

O ***Consumo energético*** CE determina o gasto energético dos nós da rede com o mecanismo SA^2CI. Esta métrica é obtida com o somatório da energia inicial dos nós da rede, TE_i, subtraído do total restante de energia destes nós, TE_r, (Eq. 5.6). Diante disso, o impacto do SA^2CI na rede é mensurado através desta métrica, e assim saber a sua adequabilidade com a IoT devido ao consumo demandado pelas fases do SA^2CI.

$$CE = \sum (TE_i - TE_r) \tag{5.6}$$

A métrica SS indica a ***Sobrecarga do SA^2CI*** na rede. O calculo da SS é alcançada a partir do total de pacotes trafegados na rede sem o SA^2CI, $Tpct_r$, menos o somatório dos pacotes com

o mecanismo na rede, (Eq. 5.7). Esta métrica apresenta valores discretos, os quais computam os pacotes adicionais de controle do SA^2CI, evidenciando a eficiência do mecanismo avaliado.

$$SS = \sum(Tpct_{sc} - Tpct_r) \tag{5.7}$$

5.3 Análise de um cenário doméstico

Os resultados obtidos na avaliação dos mecanismos SA^2CI e LSD em um cenário doméstico estão divididos em resultados de eficácia e de eficiência. Para a primeira parte da avaliação, isto é, eficácia, os dois mecanismos de detecção de SA's foram avaliados e comparados. Já na parte de eficiência, o SA^2CI foi avaliado individualmente, com o objetivo de mostrar a adequabilidade deste mecanismo com a IoT. Diante disso, os resultados serão descritos na subseção a seguir.

5.3.1 Confidencialidade

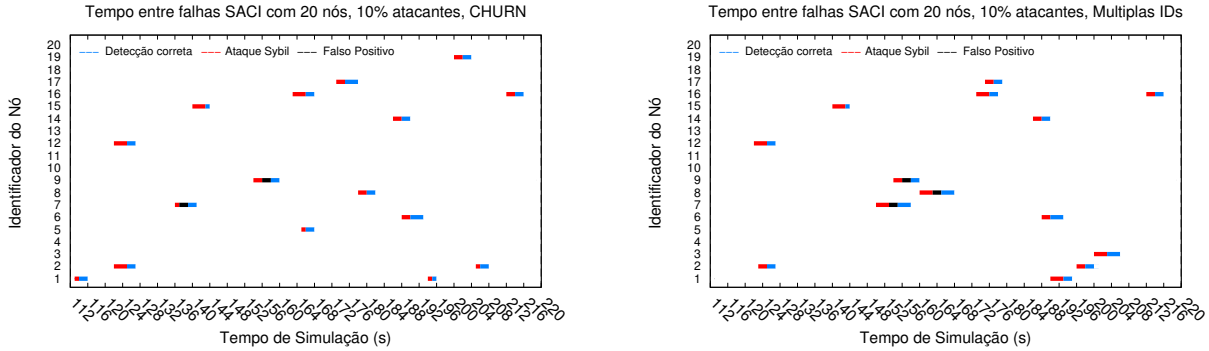
Ataques de detecção falhas de SA^2CI e LSD são mostrados em gráficos da Fig. 5.3. Esses gráficos descrevem um intervalo de tempo de operação do mecanismo, no qual os atacantes se fazem passar por usuários legítimos. Os pontos vermelhos significam o tempo entre o início de um ataque eo seu reconhecimento pelo mecanismo. Os pontos pretos significam o tempo de uma detecção errada até que SA^2CI reconheça o diagnóstico errado. Os pontos azuis significam o intervalo de tempo entre uma detecção de ataque correta e sua recuperação. Nos gráficos, note que SA^2CI detecta uma presença maliciosa e um curto período de tempo (cerca de 2 segundos - pontos azuis). Por outro lado, o LSD precisa de mais tempo para identificar o ataque, uma vez que requer as medidas de RSS por vizinhos durante a autenticação. Além disso, uma vez que o LSD executa uma autenticação incorreta, requer mais tempo para recuperar a falha e remover o ataque (pontos negros). Isso acontece como conseqüência do atraso da recepção de valores RSS. Em SA^2CI, falso positivo ocorreu em $\mathcal{N}_{MOV}$ nós, com restrições de energia ou com muitas perdas de conexão devido à mobilidade. Tabela 5.2 mostra o $MTBF$ eo $MTTR$ de dois mecanismos. Esta tabela apresenta que a freqüência de falha eo tempo de recuperação são menores em S A^2 CI do que no LSD, independente do número de nós.

A Tabela 3 exibe o $MTBF$ e o $MTTR$ dos dois mecanismos na qual a frequência de falhas e o tempo de recuperação delas são menores no SA^2CI do que no LSD independente da quantidade de nós.

Tabela 5.2: Tempo entre falhas e recuperação do SA^2CI e LSD

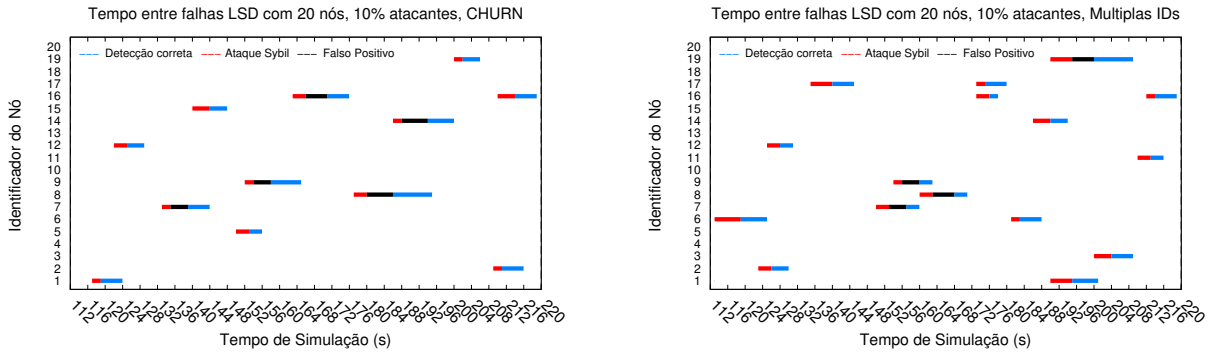
Qtd. Nós	MTBF – SA^2CI	MTTR – SA^2CI	MTBF – LSD	MTTR – LSD
20	66.7 s	2.3 s	22.2 s	5.566 s
40	69.3 s	2.5 s	23.4 s	5.89 s
60	70.1 s	2.5 s	24.2 s	5.93 s

A resistência ao comportamento dos ataques Sybil é mostrada nos gráficos da Figura 5.4, onde a quantidade de ataques com sucesso é contabilizada ao longo do tempo. Nesta figura, percebe-se que independente do comportamento, os ataques Sybil são mais difíceis de serem



(a) Fabricada

(b) *Roubada*

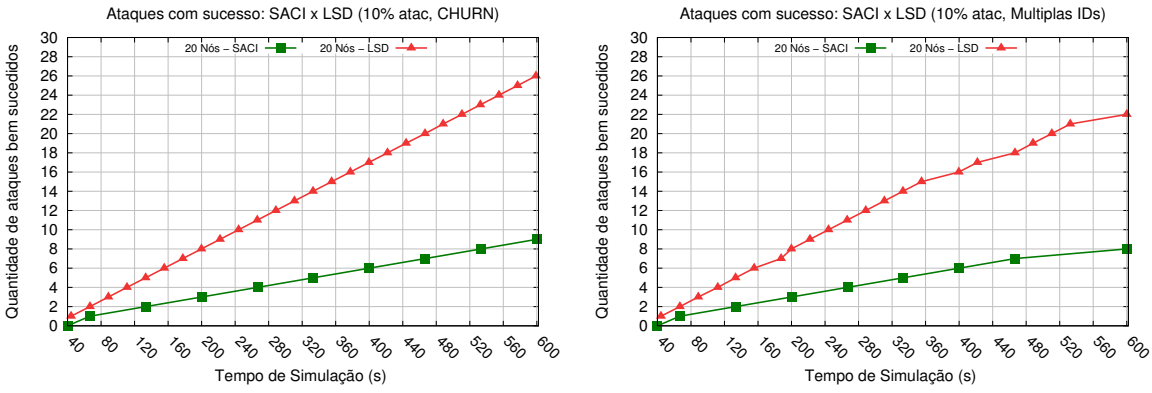


(c) Fabricada

(d) *Roubada*

Figura 5.3: Falhas do SA^2CI e LSD diante de ataques Sybil

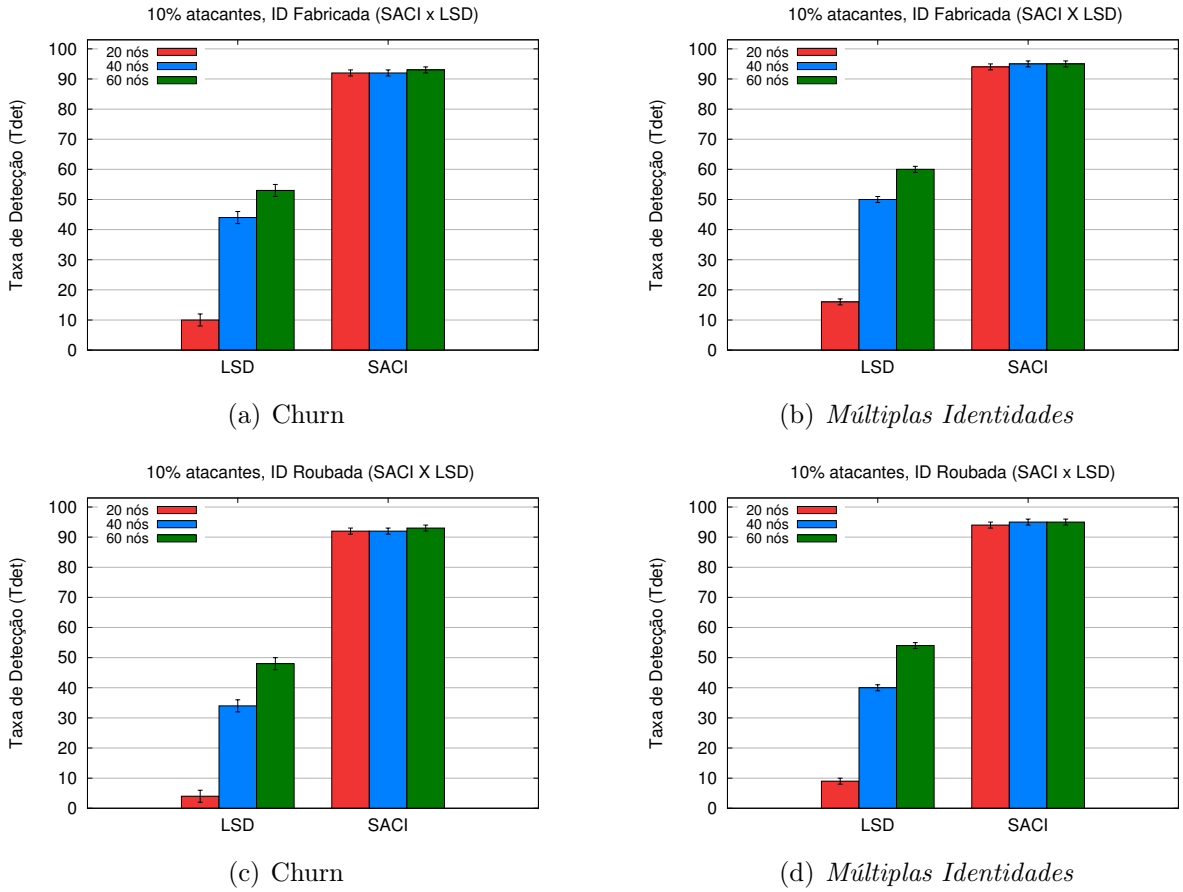
detectados pelo LSD. Isto deve-se ao LSD demandar de constantes avaliações do RSS do nó durante o seu processo de autenticação, exigindo assim um maior custo na detecção do ataque Sybil. O gráfico 5.4(a) mostra que no SA^2CI apenas nove ataques obtiveram sucesso. Enquanto que no mecanismo LSD vinte e nove investidas feitas pelos atacantes foram bem sucedidas. Os atacantes Sybil empregando múltiplas identidades foram menos efetivos do que aqueles com o comportamento churn, como mostrado no Gráfico 5.4(b). Dessa maneira, percebe-se que o SA^2CI identifica melhor as ameaças independente do comportamento do atacante, enquanto o LSD possui uma maior oscilação.



(a) *Churn*

(b) Múltiplas Identidades

Figura 5.4: Efetividade do Ataque Sybil no SA^2CI e no LSD



(a) Churn (b) *Múltiplas Identidades*

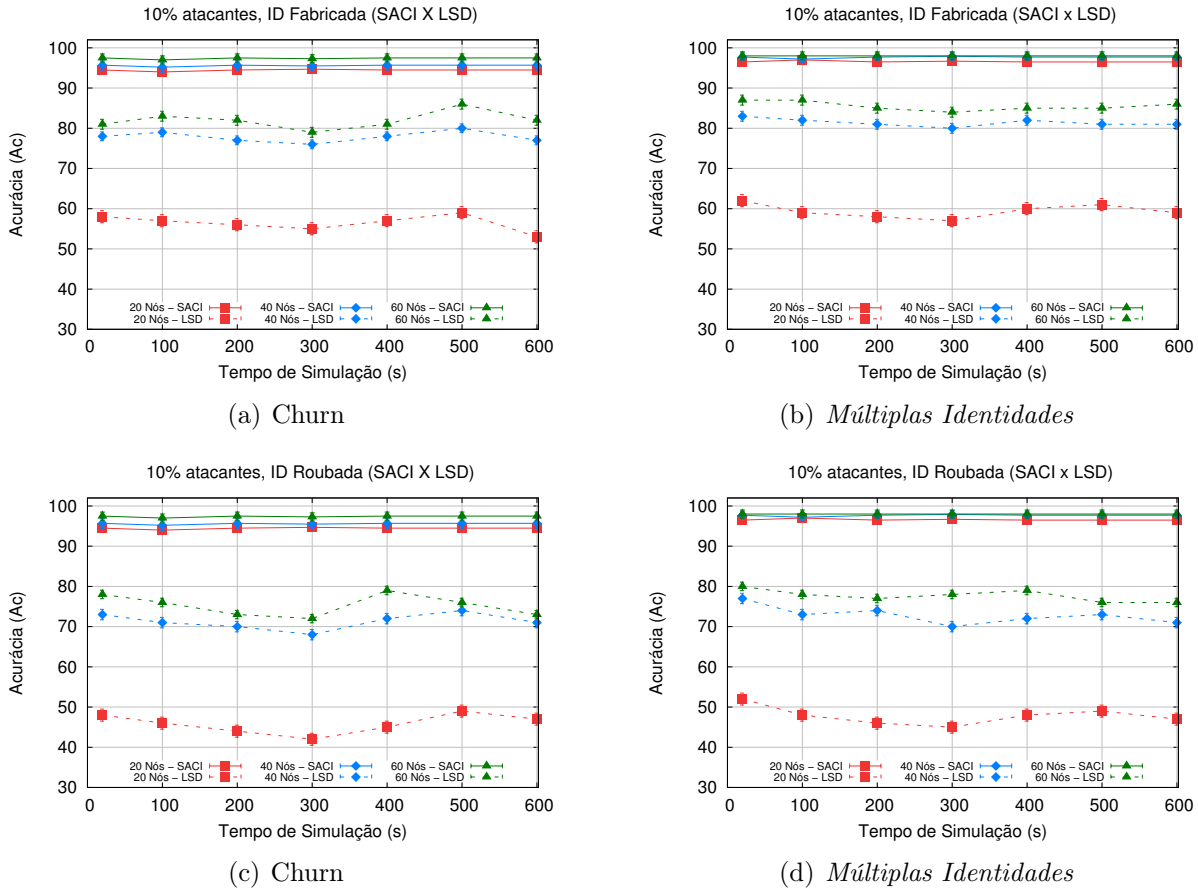
(c) Churn (d) *Múltiplas Identidades*

Figura 5.5: Taxas de detecção do SACI x LSD

Os gráficos da Figura 5.5 mostram a T_{det} do SA^2CI e do LSD diante de ataques Sybil com os comportamentos churn e múltiplas identidades. As características da rede empregadas pelo LSD limitam a detecção de atacantes, principalmente num ambiente móvel, pois ele requer análises constantes dos vizinhos do RSS de um dado nó autenticado. O comportamento, o tipo de identidade, e a densidade da rede influenciam na detecção do LSD, onde este mecanismo apresentou o pior desempenho num cenário esparso uma vez que a quantidade de nós vizinhos para realizar a detecção é menor, reduzindo então a efetividade. Além disso, nota-se influência do ataque Sybil com identidades roubadas na T_{det}, aonde este mecanismo apresentou apenas 5% com 20 nós. Já a T_{det} do SA^2CI alcançou 92% por que o SA^2CI emprega recibos de identidade, e isto garante a irretratabilidade dos nós. Antes de cada associação de um nó à rede, a sua conduta é verificada, evitando que um atacante apresente uma identidade falsa independente do comportamento churn ou de múltiplas identidades. O uso de recibos possibilita a identificação de forma única de um nó, isto é, caso um atacante Sybil fabrique ou roube uma identidade, o recibo desta identidade não será o mesmo.

.

Os gráficos da Figura 5.6 mostram a A_c dos mecanismos SA^2CI e LSD. O comportamento constante da A_c do SA^2CI ocorre em razão da técnica empregada necessitar apenas do recibo de identidades para realizar a detecção. A forma de detecção utilizada pelo LSD difere do SA^2CI técnica empregada pelo LSD, que requer uma constante mensuração do RSS dos nós. Além disso,



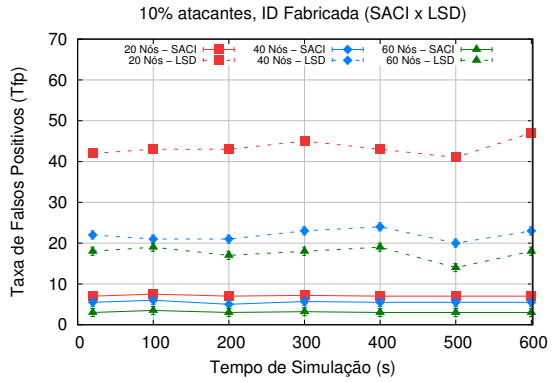
(a) Churn (b) *Múltiplas Identidades*

(c) Churn (d) *Múltiplas Identidades*

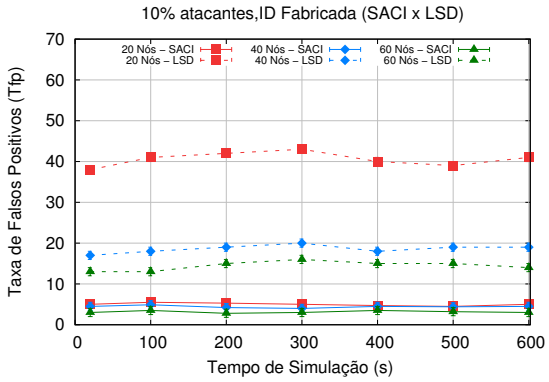
Figura 5.6: Comparativo entre as acurácias

o comportamento de uma atacante durante uma associação interfere muito pouco na acurácia do SA^2CI, onde ela reduz 3% em cenários menos densos. Já quando os atacantes empregam o churn no lugar de múltiplas identidades a A_c tende o mesmo comportamento, seja ela em cenários mais ou menos densos. Já o LSD possui uma A_c próxima dos 90% no cenário mais denso, 60 nós. Contudo, em cenários menos densos a precisão tende a diminuir, visto que o LSD desconsidera a irretratabilidade das identidades dos nós e possui menos vizinhos para auxíliar na detecção

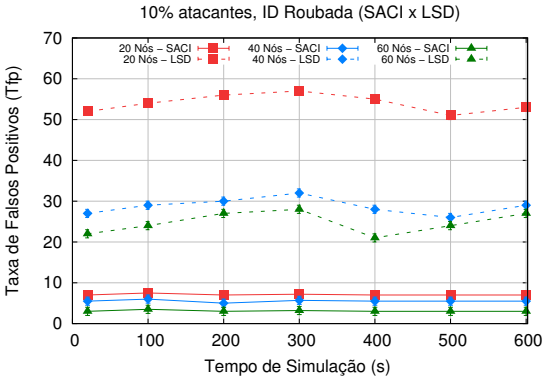
Os gráficos da Figura 5.7 mostram as T_{fp} do SA^2CI e do LSD. No SA^2CI esta taxa varia entre 4% à 7% para todos os cenários, enquanto que no LSD esta variação é de 20% à 60%. Ambos os mecanismos possuem uma maior valor de T_{fp} quando um atacante utiliza o comportamento churn, devido a sua maneira de associações e desassociações à rede, e isto prejudica a distinção entre um nó atacante e um nó legítimo. O SA^2CI possui uma taxa de falsos positivos menor, sofrendo também menos oscilações do que o LSD, principalmente em cenários esparsos, uma vez que o mecanismo LSD requer de analises constantes do RSS dos vizinhos do nó autenticado. Estas análises demandam uma quantidade maior de nós para que sejam precisas.Por outro lado, os ataques Sybil com o comportamento churn aumentam a t T_{fp} de ambos os mecanismos em relação ao ataques de multiplas identidades.



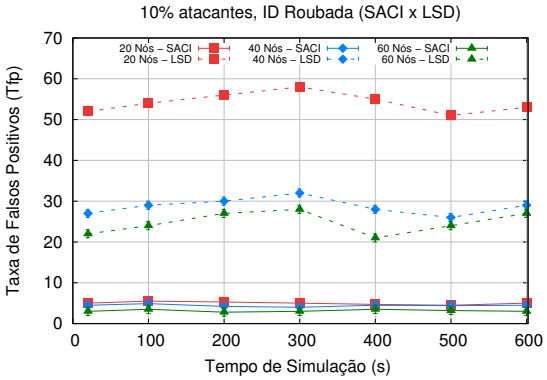
(a) Churn



(b) *Múltiplas Identidades*



(c) Churn



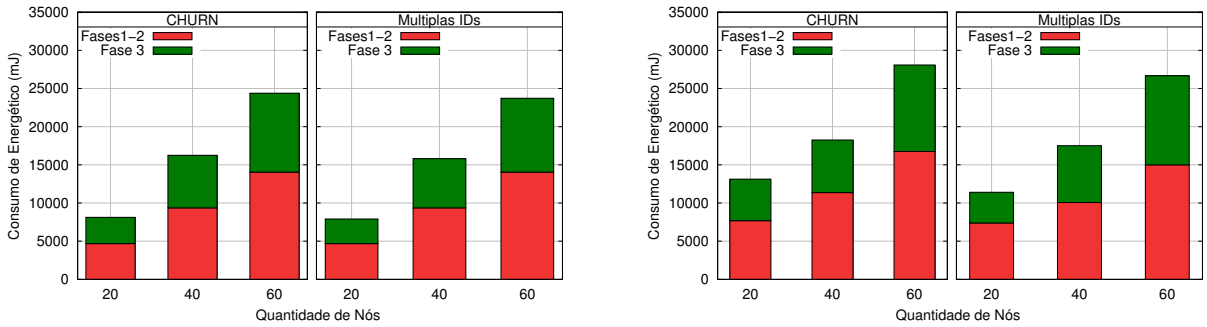
(d) *Múltiplas Identidades*

Figura 5.7: Comparativo entre os falsos positivos

5.3.2 Desempenho

Os Gráficos 5.8(a) e 5.8(b) mostram o *CE* do SA^2CI mediante ao ataque Sybil numa rede IoT. Este mecanismo possui um gasto energético semelhante para os dois tipos de comportamento e identidades adotados por um atacante Sybil. Contudo, o comportamento churn demanda um gasto energético maior, uma vez que os nós autenticadores do SA^2CI precisam monitorar as constantes associações e desassociações de um atacante com este comportamento. Já o tipo de identidade utilizada por um SA também não influencia no seu *CE*, onde para ambos os tipos o SA^2CI obteve o mesmo consumo, por que ele requer apenas o recibo de uma identidade para identificar uma associação maliciosa.

Os gráficos da Figura 5.8 mostram o Consumo energético *CE* do SA^2CI na detecção de ataques Sybil, e compreende o custo da sua inicialização e configuração (barras vermelhas), e a fase de gerencia das associações (barras verde). Percebe-se que O SA^2CI consome mais energia para detectar ataques com comportamento churn, uma vez que neste comportamento um dado atacante realiza constantes associação e desassociação. Ainda sobre o comportamento churn, nota-se que este comportamento em conjunto com o roubo de identidades demanda uma maior *CE*, onde no Gráfico 5.8(b) é possível observar o aumento desta métrica em relação ao Grático 5.8(a). No entanto, na preseça de ataques com multiplas identidades, além de consumir menos energia, o SA^2CI obteve o mesmo consumo enérgetico, visto que ele precisa apenas do recibo de identidade para determinar uma associação maliciosa.



(a) Fabricada (b) *Roubada*

Figura 5.8: Consumo energético do SA^2CI diante de ataques Sybil

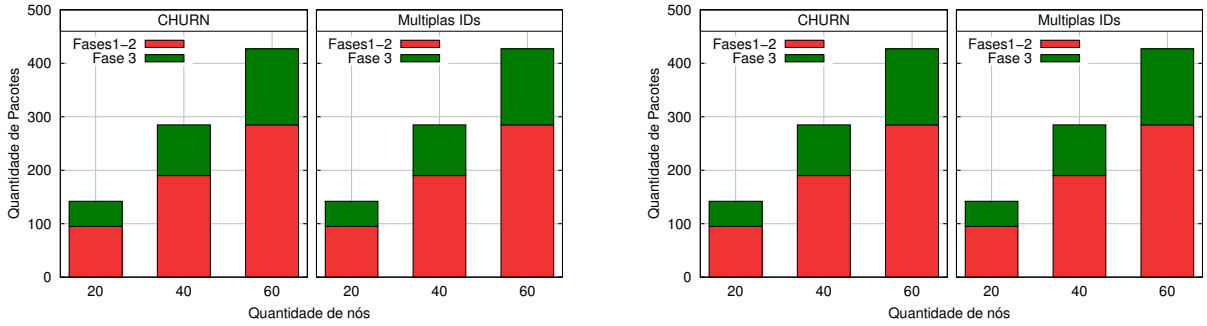
A Tabela 5.3 contém o *CE* para as operações feitas pelo SA^2CI durante a detecção do SA. As quatro primeiras operações equivalem a fase de inicialização e configuração da rede, enquanto que as três últimas diz respeito a gerência da disseminação. As fases de inicialização e configuração demandam mais energia devido à necessidade de inicialmente criar uma curva elíptica entre os nós N_{KDC}, em seguida, compartilhar os pontos da curva entre todos os nós da rede, configurar, isto é, enviar a PUF dos nós sob um canal seguro através de chaves criptográficas, e por fim gerar os segredo e os recibos. Durante à fase de gerência, a função do SA^2CI consiste em monitorar as associações dos nós à rede. O monitoramento destas associações demanda um menor consumo de recurso quando comparado as duas primeiras fases, por que tal ação requer gasto energético apenas com a comunicação e a verificação de um dado recibo, obtendo um menor consumo. Assim, o SA^2CI identifica associações de ataque Sybil a disseminação de conteúdo com um gasto energético constante independente do tipo de identidade empregada por um atacante.

Tabela 5.3: Consumo de energia para operações do SA^2CI no cenário doméstico

FUNÇÕES	CUSTO
Gerar curva elíptica	75.29 mJ
Geração de par de chaves	75.92 mJ
Geração do segredo	82.02 mJ
Geração do recibo	76.23 mJ
Verificação do recibo	90.55 mJ
Monitoramento de múltiplas identidades	70.6 mJ
Monitoramento do comportamento churn	81.6 mJ

Os Gráficos 5.9(a) e 5.9(b) mostram a *SS* do SA^2CI numa rede IoT. A quantidade de pacotes adicionais transmitida por este mecanismo em cada uma das suas fases possui uma pequena variação de acordo com o tipo de comportamento empregado por um nó atacante. Diante disso, um atacante com o comportamento churn demanda uma maior *SS* para ser identificado, devido a sua conduta durante uma associação. As fases de inicialização e de configuração possuem uma maior *SS* em virtude da quantidade mensagens trocadas necessárias para, gerar a curva, curva elíptica, distribuir os pontos, a PUF, e os recibos. Enquanto que na fase de gerência da disseminação o SA^2CI requer apenas a verificação do recibo de identidade a partir de uma

requisição de associação a rede.



(a) Fabricada (b) *Roubada*

Figura 5.9: Sobrecarga do SA^2CI na rede IoT

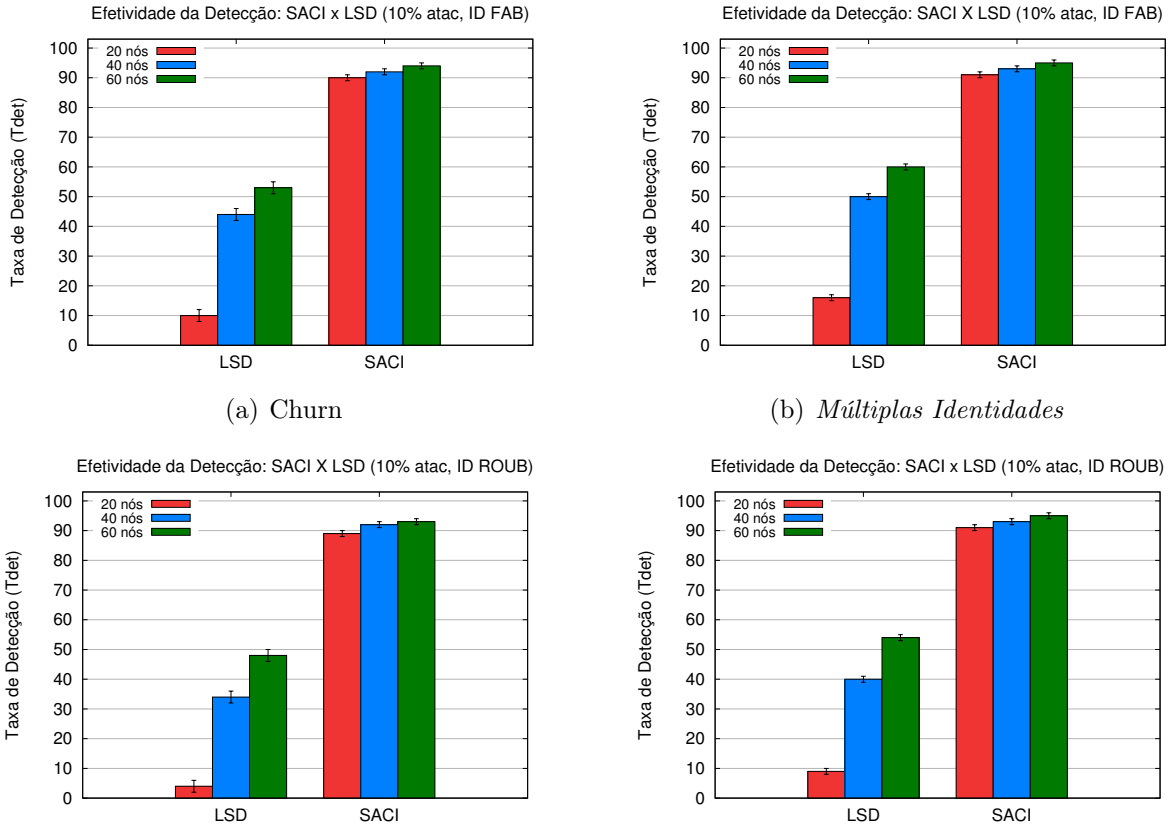
5.4 Análise de um cenário hospitalar

Os resultados obtidos na avaliação dos mecanismos SA^2CI e LSD em um cenário hospitalar ou *eHealth* como descrito na Seção 5.2 também estão divididos em resultados de segurança e de desempenho. Na avaliação de segurança, tanto o SA^2CI quanto o LSD foram avaliados por meio de três métricas que mensuram a efetividade de detecção de SA's destes dois mecanismos. Já a avaliação do desempenho visa mostrar a eficiência do SA^2CI de forma individual com o objetivo de demonstrar a aplicação deste mecanismo não só em ambientes domésticos ou de pequenas dimensões. Diante disso, os resultados deste cenário serão descritos na subseção a seguir.

5.4.1 Confidencialidade

Os Gráficos 5.10(a), 5.10(b), 5.10(c),e 5.10(d) mostram a T_{det} do SA^2CI e do LSD diante de SA's com os comportamentos churn e múltiplas identidades. Mesmo num ambiente maior, o SA^2CI atingiu uma T_{det} de 92%. Isto ocorre por que a autenticação dos nós consiste apenas do ponto z e do recibo respectivo aquela identidade. Quando a rede torna-se mais esparsa o comportamento da detecção tende a reduzir em relação aos mais densos devido à quantidade de associações diretas feitas aos nós KDC. No entanto, tal redução não compromete a confidencialidade do conteúdo trafegado pela rede. No Gráfico 5.10(c) é possivel ver a influência do SA utilizando o comportamento churn, onde o SA^2CI apresentou em média 90% para os três parâmetros de densidade da rede, isto é 20, 40 e 60 nós. Mesmo considerando a irretratabilidade das identidades dos nós, um SA com o comportamento churn pode reduzir a T_{det} de ambos os mecanismos, isto é, do SA^2CI, e do LSD. Apesar de ter uma T_{det} menor que a do cenário doméstico, o SA^2CI mostrou uma constante detecção de SA's, independente do tamanho do cenário.

O mecanismo LSD em um cenário demograficamente maior apresentou uma redução na sua T_{det}. Por ter como princípio a técnica de características em comum da rede, este mecanismo requer análises constantes do RSS pelos vizinhos do nó autenticado. Diante disso, a detecção realizada pelo LSD de um ataque Sybil numa rede esparsa é ainda mais comprometida quando



(a) Churn

(b) *Múltiplas Identidades*

(c) Churn

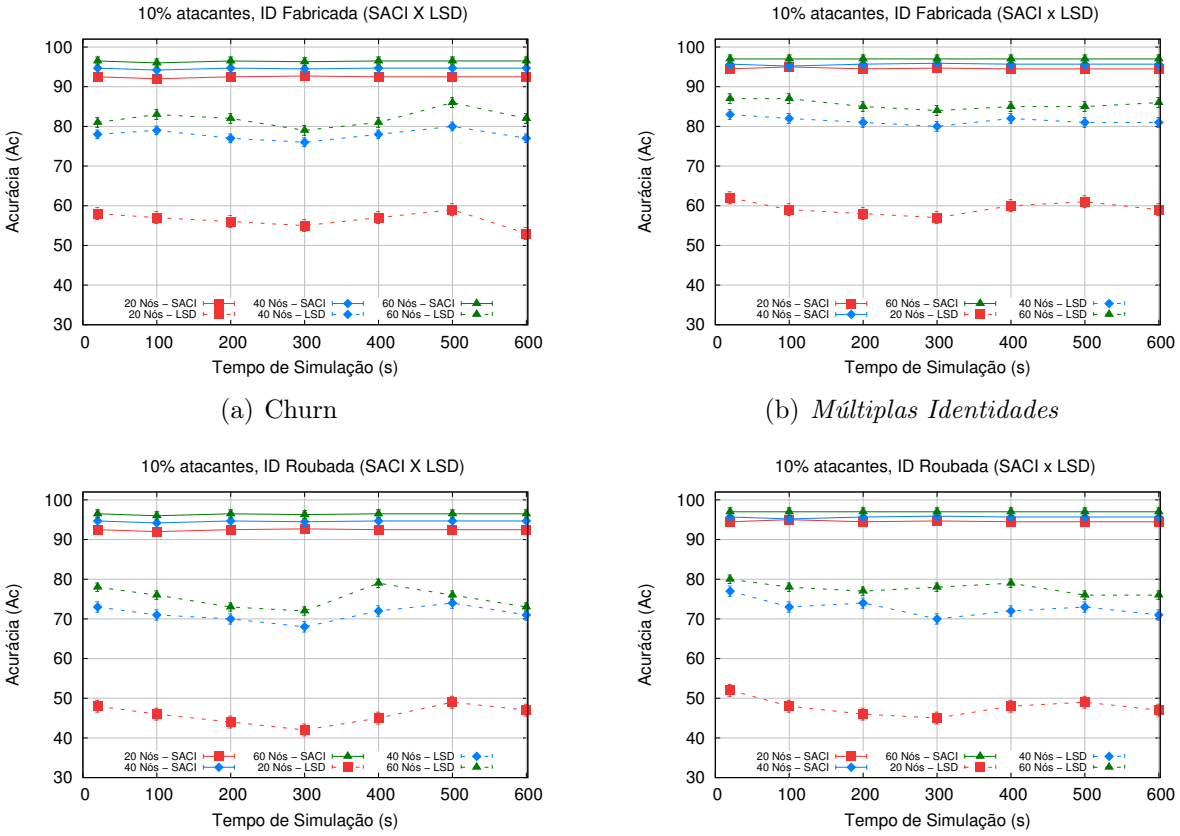
(d) *Múltiplas Identidades*

Figura 5.10: Taxas de detecção do SACI x LSD

este atacante emprega o comportamento churn. Em todos os gráficos é possível observar que o LSD apresenta uma T_{det} abaixo dos 15% a medida que a rede torna-se esparsa. Desta forma, a identificação realizada pelo SA^2CI supera o LSD principalmente em cenários mais esparsos, uma vez que este mecanismo requer de uma maior quantidade de nós vizinhos para obter uma maior precisão de detecção de ataques Sybil.

Apesar da T_{det} do SA^2CI reduzir no cenário hospitalar, o mesmo não acontece com a A_c deste mecanismo. Esta métrica métrica apresenta um comportamento constante quando comparado ao cenário anterior por conta da função verificadora executada por um nó autenticador. Tal função necessita de apenas uma tripla $< id, z, R_n >$ para autenticar uma reassociação de um nó, onde um dado nó tem acesso à rede quando $R_n \in Id$. Já o LSD teve uma pequena redução da sua A_c devido à dimensão do cenário e da quantidade de nós para localizar um dado SA através do seu RSS. Além disso, pode-se observar uma oscilação no comportamento da A_c deste mecanismo. Isto acontece em razão da localização feita pelo LSD por meio do RSS em conjunto da mobilidade de um ataque Sybil na rede. Note que tal esta oscilação tende a ser maior quando um ataque Sybil adota o comportamento churn, nos Gráficos 5.11(a)e 5.11(c).

Os Gráficos 5.12(a), 5.12(b), 5.12(c), e 5.12(d) mostram as T_{fp} do SA^2CI e do LSD quando submetidos à ataques Sybil numa rede IoT. O mecanismo SA^2CI apresentou uma T_{fp} variando entre 3% à 9%. O acréscimo desta taxa aconteceu por conta da redução sua T_{det}, influenciando no aumento T_{fp}. Este aumento acontece por que T_{det} e T_{fp} são inversamente proporcionais, ou



(a) Churn (b) *Múltiplas Identidades*

(c) Churn (d) *Múltiplas Identidades*

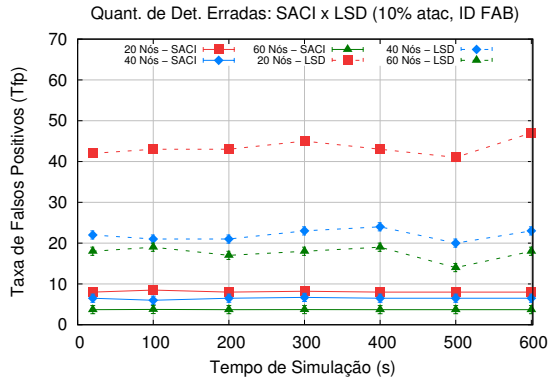
Figura 5.11: Comparativo entre as acurácias

seja, quanto maior a T_{det} menor é a T_{fp}. A T_{fp} do LSD variou entre 20% à 60%, sofrendo uma grande variação principalmente quando um SA faz requisições com identidades roubadas, vide Gráficos 5.12(c), e 5.12(d).

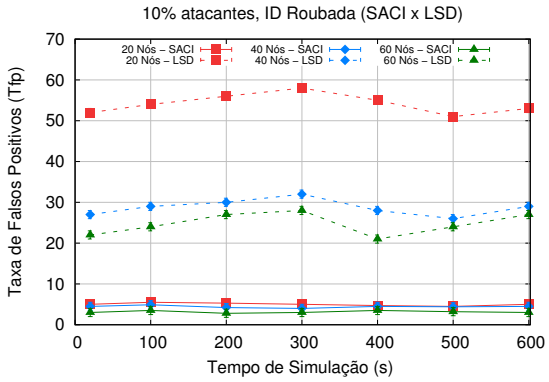
5.4.2 Desempenho

Os Gráficos 5.13(a) e 5.13(b) ilustram o consumo energético *CE* do SA^2CI mediante ao ataque Sybil numa rede IoT. Um cenário demograficamente maior demanda mais energia, uma vez que em um ambiente móvel os nós precisam manter os serviços da rede que são prejudicados pela mobilidade.Diante disso, o *CE* dos SA^2CI aumentou quando comparado ao do cenário domestico. No entanto, ele possui um gasto energético semelhante para os dois tipos de comportamento e identidades adotados por um atacante Sybil. Contudo, o comportamento churn demanda um gasto energético maior, por que os nós autenticadores do SA^2CI precisam monitorar as constantes associações e desassociações de um atacante com este comportamento. Já o tipo de identidade utilizada por um SA também não influencia no seu *CE*, onde para ambos os tipos o SA^2CI obteve o mesmo consumo, por que ele requer apenas o recibo de uma identidade para identificar uma associação maliciosa.

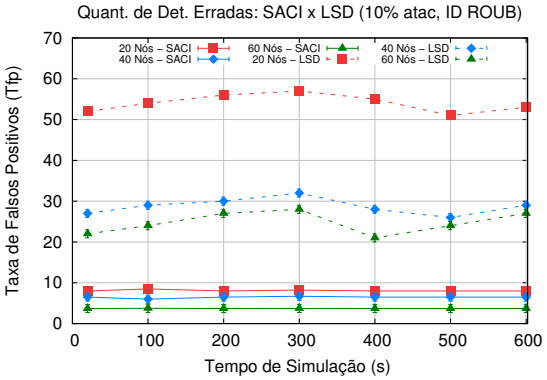
A Tabela 5.4 contém o *CE* para as operações feitas pelo SA^2CI durante a detecção do SA no cenário *eHealth*. Os valores obtidos por estas funções são iguais aos do cenário anterior. Contudo,



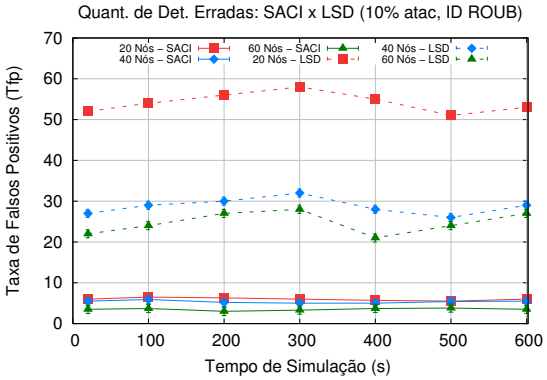
(a) Churn



(b) *Múltiplas Identidades*

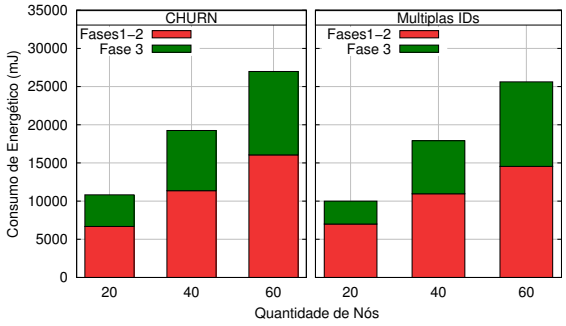


(c) Churn

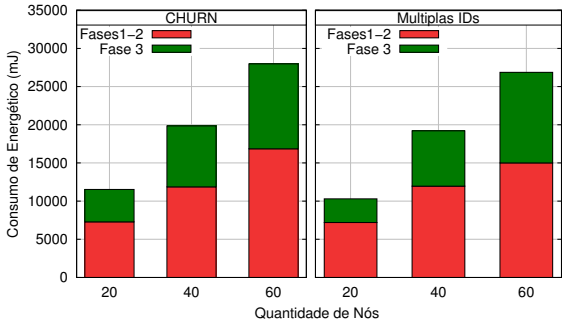


(d) *Múltiplas Identidades*

Figura 5.12: Comparativo entre os falsos positivos



(a) Fabricada



(b) *Roubada*

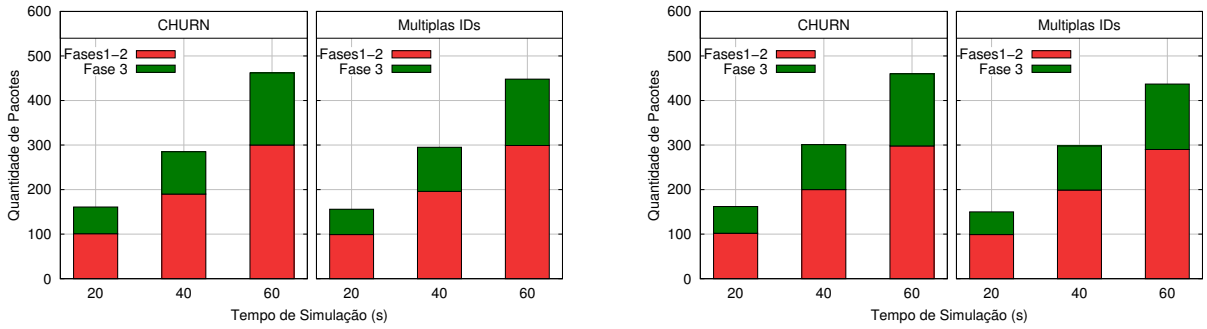
Figura 5.13: Consumo energético do SA^2CI diante de ataques Sybil

o *CE* do SA^2CI aumentou por conta da quantidade de pacotes trocados ser maior devido as desassociações dos nós da rede. Com isso, o custo para configurar um dado nó aumentou uma vez que durante este processo, caso tal nó saia do raio de ação da rede ou do nó autenticador a sua configuração deve ser reiniciada.

Os Gráficos 5.14(a) e 5.14(b) mostram a *SS* do SA^2CI numa rede hospitalar da IoT. A sobrecarga na rede aumentou quando comparado a um cenário doméstico, uma vez que a quantidade de desassociações é maior devido à razão dimensão/densidade da rede. Note que o comportamento churn de um SA ainda demanda uma maior *SS* para ser identificado, devido a sua conduta

Tabela 5.4: Consumo de energia para operações do SA^2CI no cenário hospitalar

FUNÇÕES	CUSTO
Gerar curva elíptica	75.29 mJ
Geração de par de chaves	75.92 mJ
Geração do segredo	82.02 mJ
Geração do recibo	76.23 mJ
Verificação do recibo	90.55 mJ
Monitoramento de múltiplas identidades	70.6 mJ
Monitoramento do comportamento churn	81.6 mJ



(a) Fabricada (b) *Roubada*

Figura 5.14: Sobrecarga do SA^2CI na rede IoT

durante uma associação, como também acontece no cenário doméstico. As fases 1 e 2 continuam demandando uma troca de pacotes maior por causa das configurações da curva E, da PUF_n, do R_n, e dos pares de chaves. Enquanto que a fase de gerência necessita apenas das verificações feitas por meio de uma requisição composta por uma tripla $< id, z_n, R_n >$.

5.5 Resumo

Este capítulo apresentou uma avaliação do comportamento e desempenho dos mecanismo SA^2CI e LSD, onde eles foram analisados e comparados. Foram utilizadas três métricas de eficácia, a taxa de detecção T_{det}, a acurácia A_c, e a taxa de falsos positivos T_{fp}, as quais mostraram que a operação do SA^2CI identifica SA's com os comportamentos churn e com múltiplas identidades. Também mostrou-se a adequabilidade deste mecanismo com a IoT, onde mesmo em um ambiente hospitalar oSA^2CI obteve uma boa eficácia e eficiência. O funcionamento do SA^2CI foi mais estável que o LSD e apresentou resultados sempre superiores a este mecanismo.

CAPÍTULO 6

CONCLUSÃO

A Internet das Coisas (IoT) concentra um grande número de objetos heterogêneos conectados, os quais podem ser estacionários ou móveis e ter restrição de recursos. Um atacante pode explorar estas características tornando-as em vulnerabilidades as quais podem comprometer a qualidade dos serviços prestados nesta rede. Dessa maneira, o ataque Sybil quando presente numa rede IoT inflinge a confidencialidade dos dados trafegados, inibe um dipositivo de receber conteúdo, uma votação, por exemplo, pode ser compromedita por este ataque uma vez que ele atua na votação se passando por mais de um dispositivo da rede.

As soluções encontradas na literatura apresesentam métodos, esquemas, e mecanismos que identificam ataques Sybil sobre redes MANETs e VANETs. Uma classificação destas soluções pode ser feita pela perspectiva da técnica empregada, as quais são: Características das redes, Criptografia, e Relacionamento entre os vizinhos. Contudo, estas soluções quando aplicadas para a IoT geram problemas para a rede, como ineficácia na detecção dos ataques Sybil ,elevadas taxas de falsos positivos, alto consumo de energia, entre outros. Dessa maneira são necessárias soluções para a segurança dos serviços que levem em conta a eficácia e a eficiência na detecção de ataques Sybil da IoT.

O mecanismo SA^2CI (Sybil Attack Association Control for IoT) foi proposto com o objetivo de identificar associações de SA's para o serviço de disseminação da IoT. Para detectar SA's, o SA^2CI utiliza curvas elípticas (ECC) gerando um par de chaves para cada nó da rede e provendo assim um canal seguro para a comunicação dos nós. Com o canal seguro estabelecido, os nós da rede podem trocar informações seguras, e assim enviar os seus códigos PUF para o nó KDC mais próximo. Em seguida, os nós KDC's geram o recibo de identidade destes nós, os quais podem utilizá-lo para garantir a legitimidade de sua identidade. Logo após os nós serem configurados, o serviço de disseminação inicia e o SA^2CI atua nos nós da rede monitorando as reassociações de nós já conhecidos pela rede, como também as novas associações. A cada reassociação um nó deve apresentar informação na qual será avaliada de forma direta ou indireta. O SA^2CI usa curvas elípticas, PUF, recibos de identidades, e avalia o comportamento de uma nova associação de modo à prevenir a rede e o serviço de disseminação de SA's.

A avaliação do SA^2CI e LSD foi conduzida no simulador de redes NS3 aonde os ambientes onde os ambientes doméstico e hospitalar foram considerados. Estes mecanismos foram implementados, bem como os ataques Sybil e seus comportamentos. Além disso, a confidencialidade e o desempenho dos mecanismos foram mensurados por meio de sete métricas. Por empregar a técnica baseada em caractéristicas das redes, o LSD apresentou menores taxas de confidencialidade, aonde destaca-se a taxa de detecção (T_{det}). A T_{det} do LSD possui menores taxas quando uma rede é esparsa, demonstrando que características da redes não são adequadas para redes menos densas. O SA^2CI alcançou taxas de confidencialidades constantes, isto é, independente da densidade da rede este mecanismo desempenhou o mesmo comportamento de detecção. O

SA^2CI tambem reduziu os efeitos adversos como a sobrecarga na rede e o consumo de energia, comprovando a adequabilidade da criptografia de curvas elipitcas no contexto da IoT.

Desta forma, concluímos que é possível alcançar uma disseminação segura à ataques Sybil para a IoT. Este objetivo foi alcançado pelo o SA^2CI uma vez que ele detecta ataques Sybil de forma escalar, distribuída, adaptativa, e ainda considera a heterogeneidade dos dispositivos. O SA^2CI garante a confidencialidade do serviço de disseminação alcançando taxas de detecção, precisão, e falsos posistivos, satisfatórias pois ele leva em conta o princípio de irretratabilidade podendo identificar tanto o SA's com identidades fabricadas quanto roubadas. Seguindo a ideia de tornar o dia-a-dia cada vez mais prático, a IoT requer mecanismos e sistemas confiáveis e seguros. Assim, este trabalho contribuiu com o detalhamento do SA e dos seus comportamentos, do serviço de disseminação e uma solução para uma disseminação segura contra ataques Sybil na IoT.

6.1 Trabalhos futuros

A demanda de serviços personalizados no cotidiano das pessoas tem aumentado cada vez mais necessidade de se disseminar conteúdos. O provimento de serviços na IoT, como o monitoramento de funções vitais, temperaturas de ambientes, por exemplo, são formas de disseminação de conteúdo utilizadas numa rede IoT. Contudo, este serviço requer desdobramentos no âmbito da segurança dos dados trafegados, visto que a insegurança destes conteúdos reduzem a qualidade do serviço prestado. Além disso, uma outra preocupação diz respeito ao desempenho, uma vez que os conteúdos trafegados podem ser sensíveis para a mensuração de um dado serviço.

No âmbito de segurança, o SA^2CI foi avaliado em um ambiente aonde a quantidade de atacantes Sybil equivale à 10% do total de dispositivos da rede IoT. Dentre os três pilares da segurança, a disponibilidade, a integridade, e a confidencialidade, o SA^2CI trata deste ultimo.Este mecanismo pode receber novos módulos que visam atender a disponibilidade e a integridade. Assim, o serviço de disseminação de conteúdo estará seguro diante de ameaças contra a segurança evitando a redução da qualidade do serviço prestado pela rede.

Uma vez que o SA^2CI avalia o comportamento durante a associação à rede, outros tipos de ataques podem ser detectados. No âmbito da disponibilidade, um novo módulo no qual visa a interceptação de ameaças ao funcionamento da rede. Tal medida se desenvolvida permitirá o desenvolvimento dos serviços de uma rede IoT de forma ineterrupta, aonde a trasmissão de dados vitais de um paciente para um hospital, por exemplo, não será interrompida. Logo, a adição deste módulo permitirá a serviços os quais os dados são sensíveis uma maior qualidade de serviço, visto que estes dados estarão disponíveis.

A disseminação de conteúdo promovida pelo SA^2CI pode extendida de modo à garantir a integridade dos dados trafegados. O modulo para a preservação da intregridade dos conteúdos visará salvaguardar a transmissão de dados de um dispositivo origem até um dado destino. Esta medida propocionará uma melhoria na corretude dos conteúdos disseminados, garantindo que eles serão veridicos e não foram violados. Dessa maneira, uma votação realizada entre os dispositivos da rede não poderia ser fraudada, visto que este módulo garantirá a integridade do conteúdo

disseminado.

A IoT é uma rede híbrida, aberta, e dinâmica o que demanda sistemas computacionais leves, eficazes, e seguros. Este tipo de rede também necessita de sistemas eficientes, uma vez que não basta um dado sistema ser seguro, ou seja, ele deve ser adequado a diversidade de dispositivos da IoT. Tendo isto em vista, esta dissertação deixa em aberto a avaliação do SA^2CI em ambientes estritamente limitados de recursos.

Com a convergência dos ambientes da IoT as cidades inteligentes surgirão, bem como as vulnerabilidades à ataques Sybil. Como o SA^2CI já foi avaliado nos ambientes doméstico e hospitalar, alcançando resultados satisfatórios, um estudo de caso pode ser realizado com o SA^2CI em uma área equivalente à uma cidade inteligente. Assim, a partir dos resultados obtidos será possível mensurar o comportamento e o desempenho do SA^2CI por completo, desde uma residencia até uma cidade inteligente.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Bing Wu, Jianmin Chen, Jie Wu, and Mihaela Cardei. A survey of attacks and countermeasures in mobile ad hoc networks. In *Wireless Network Security*, pages 103–135. Springer, 2007.

[2] Ovidiu Vermesan, Peter Friess, Patrick Guillemin, Sergio Gusmeroli, Harald Sundmaeker, Alessandro Bassi, Ignacio Soler Jubert, Margaretha Mazura, Mark Harrison, M Eisenhauer, et al. Internet of things strategic research roadmap. *O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, et al., Internet of Things: Global Technological and Societal Trends*, 1:9–52, 2011.

[3] Péter Baranyi, Adam Csapo, and Gyula Sallai. Cognitive capabilities in the future internet. In *Cognitive Infocommunications (CogInfoCom)*, pages 173–185. Springer, 2015.

[4] Roy Want, Bill N Schilit, and Scott Jenson. Enabling the internet of things. *Computer*, (1):28–35, 2015.

[5] Shancang Li, Li Da Xu, and Shanshan Zhao. The internet of things: a survey. *Information Systems Frontiers*, pages 1–17, 2014.

[6] Sheik Mohammad Mostakim Fattah, Muhammad Golam Kibria, Kwanghyeon Jeong, and Ilyoung Chong. Knowledge driven architectural model to support smart emergency service in web of objects based iot environment. *J. Korean Inst. Commun. Inf. Sci*, 40:408–418, 2015.

[7] Christian Cervantes, Diego Poplade, Michele Nogueira, and Aldri Santos. Um sistema de detecç ao de ataques sinkhole sobre 6lowpan para internet das coisas.

[8] Yen-Kuang Chen. Challenges and opportunities of internet of things. In *Design Automation Conference (ASP-DAC), 2012 17th Asia and South Pacific*, pages 383–388. IEEE, 2012.

[9] Salvatore Distefano, Nilanjan Banerjee, and Antonio Puliafito. Smart objects, infrastructures, and services in the internet of things. *International Journal of Distributed Sensor Networks*, 2016, 2016.

[10] Antonio Skarmeta, José L Hernández-Ramos, and Jorge Bernal Bernabe. A required security and privacy framework for smart objects. 2015.

[11] Stephen Kent. Ip authentication header. 2005.

[12] Linus Wallgren, Shahid Raza, and Thiemo Voigt. Routing attacks and countermeasures in the rpl-based internet of things. *International Journal of Distributed Sensor Networks*, 2013, 2013.

[13] Mohit Sethi, Pranvera Kortoci, Mario Di Francesco, and Tuomas Aura. Secure and low-power authentication for resource-constrained devices. In *Internet of Things (IOT), 2015 5th International Conference on the*, pages 30–36. IEEE, 2015.

[14] Viet-Duc Le, Hans Scholten, and Paul Havinga. Unified routing for data dissemination in smart city networks. In *Internet of Things (IOT), 2012 3rd International Conference on the*, pages 175–182. IEEE, 2012.

[15] Anuj Sehgal, Vladislav Perelman, Siarhei Kuryla, and Jürgen Schönwälder. Management of resource constrained devices in the internet of things. *Communications Magazine, IEEE*, 50(12):144–149, 2012.

[16] Wai Chen, Ratul K Guha, Taek Jin Kwon, John Lee, and Yuan-Ying Hsu. A survey and challenges in routing and data dissemination in vehicular ad hoc networks. *Wireless Communications and Mobile Computing*, 11(7):787–795, 2011.

[17] Shahid Raza, Linus Wallgren, and Thiemo Voigt. Svelte: Real-time intrusion detection in the internet of things. *Ad hoc networks*, 11(8):2661–2674, 2013.

[18] Seokung Yoon, Haeryong Park, and Hyeong Seon Yoo. Security issues on smarthome in iot environment. In *Computer Science and its Applications*, pages 691–696. Springer, 2015.

[19] Ruixia Liu and Yinglong Wang. A new sybil attack detection for wireless body sensor network. In *Computational Intelligence and Security (CIS), 2014 Tenth International Conference on*, pages 367–370. IEEE, 2014.

[20] Yong Ho Hwang. Iot security & privacy: threats and challenges. In *Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security*, pages 1–1. ACM, 2015.

[21] P Raghu Vamsi and Krishna Kant. A lightweight sybil attack detection framework for wireless sensor networks. In *Contemporary Computing (IC3), 2014 Seventh International Conference on*, pages 387–393. IEEE, 2014.

[22] Salavat Marian and Popa Mircea. Sybil attack type detection in wireless sensor networks based on received signal strength indicator detection scheme. In *Applied Computational Intelligence and Informatics (SACI), 2015 IEEE 10th Jubilee International Symposium on*, pages 121–124. IEEE, 2015.

[23] Xiaodong Lin. Lsr: mitigating zero-day sybil vulnerability in privacy-preserving vehicular peer-to-peer networks. *Selected Areas in Communications, IEEE Journal on*, 31(9):237–246, 2013.

[24] Bo Yu, Cheng-Zhong Xu, and Bin Xiao. Detecting sybil attacks in vanets. *Journal of Parallel and Distributed Computing*, 73(6):746–756, 2013.

[25] Daniele Quercia and Stephen Hailes. Sybil attacks against mobile users: friends and foes to the rescue. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–5. IEEE, 2010.

[26] Bing-Zhe He, Chien-Ming Chen, Yi-Ping Su, and Hung-Min Sun. A defence scheme against identity theft attack based on multiple social networks. *Expert Systems with Applications*, 41(5):2345–2352, 2014.

[27] Wei Wei, Fengyuan Xu, Chiu C Tan, and Qun Li. Sybildefender: Defend against sybil attacks in large social networks. In *INFOCOM, 2012 Proceedings IEEE*, pages 1951–1959. IEEE, 2012.

[28] Danilo Evangelista, Aldri dos Santos, and Michele Nogueira. Avaliação das técnicas de detecção do ataque sybil na disseminação de conteúdo da internet das coisas. In *XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBseg), 2015*, nov 2015.

[29] Chris Piro, Clay Shields, and Brian Neil Levine. Detecting the sybil attack in mobile ad hoc networks. In *Securecomm and Workshops, 2006*, pages 1–11. IEEE, 2006.

[30] Jesús Ayuso, Leandro Marin, Antonio Jara, and Antonio F Gómez Skarmeta. Optimization of public key cryptography (rsa and ecc) for 16-bits devices based on 6lowpan. In *1st International Workshop on the Security of the Internet of Things, Tokyo, Japan*, 2010.

[31] Haifeng Yu, Chenwei Shi, Michael Kaminsky, Phillip B Gibbons, and Feng Xiao. Dsybil: Optimal sybil-resistance for recommendation systems. In *Security and Privacy, 2009 30th IEEE Symposium on*, pages 283–298. IEEE, 2009.

[32] Gerd Kortuem, Fahim Kawsar, Daniel Fitton, and Vasughi Sundramoorthy. Smart objects as building blocks for the internet of things. *Internet Computing, IEEE*, 14(1):44–51, 2010.

[33] Friedemann Mattern and Christian Floerkemeier. From the internet of computers to the internet of things. In *From active data management to event-based systems and more*, pages 242–259. Springer, 2010.

[34] Jean-Philippe Vasseur and Adam Dunkels. *Interconnecting smart objects with ip: The next internet*. Morgan Kaufmann, 2010.

[35] Hans Schaffers, Nicos Komninos, Marc Pallot, Brigitte Trousse, Michael Nilsson, and Alvaro Oliveira. *Smart cities and the future internet: Towards cooperation frameworks for open innovation*. Springer, 2011.

[36] LA Grieco, A Rizzo, S Colucci, S Sicari, G Piro, D Di Paola, and G Boggia. Iot-aided robotics applications: technological implications, target domains and open issues. *Computer Communications*, 54:32–47, 2014.

[37] Diane Cook and Sajal Das. *Smart environments: technology, protocols and applications*, volume 43. John Wiley & Sons, 2004.

[38] Stefan Poslad. Ubiquitous computing smart devices, smart environments and smart interaction, 2009.

[39] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645–1660, 2013.

[40] Stephen E Deering. Internet protocol, version 6 (ipv6) specification. 1998.

[41] T Winter, P Thubert, T Clausen, J Hui, R Kelsey, P Levis, K Pister, R Struik, and J Vasseur. Rpl: Ipv6 routing protocol for low power and lossy networks, rfc 6550. *IETF ROLL WG, Tech. Rep*, 2012.

[42] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat. Lightweight sybil attack detection in manets. *Systems Journal, IEEE*, 7(2):236–248, 2013.

[43] Angelo Bannack, Eduardo da Silva, Michele Nogueira Lima, Aldri L dos Santos, and Luiz Carlos Pessoa Albini. Segurança em redes ad hoc. *Anais do XXVI Simpósio Brasileiro de Telecomunicaçoes (SBRT?08)*, pages 19–20, 2008.

[44] Jianliang Zheng and Myung J Lee. A comprehensive perfomance study of ieee 802.15.4, 2004.

[45] Wolfram Kluge, Frank Poegel, Hendrik Roller, Matthias Lange, Tilo Ferchland, Lutz Dathe, and Dietmar Eggert. A fully integrated 2.4-ghz ieee 802.15. 4-compliant transceiver for zigbee? applications. *Solid-State Circuits, IEEE Journal of*, 41(12):2767–2775, 2006.

[46] ZigBee Alliance. Zigbee specification, 2006.

[47] Stig Petersen and Simon Carlsen. Wirelesshart versus isa100. 11a: The format war hits the factory floor. *Industrial Electronics Magazine, IEEE*, 5(4):23–34, 2011.

[48] Jianping Song, Song Han, Aloysius K Mok, Deji Chen, Mike Lucas, and Mark Nixon. Wirelesshart: Applying wireless technology in real-time industrial process control. In *Real-Time and Embedded Technology and Applications Symposium, 2008. RTAS'08. IEEE*, pages 377–386. IEEE, 2008.

[49] White Paper, Jonathan Hui, and Arch Rock Corporation. Executive summary, 2009.

[50] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A survey on cyber security for smart grid communications. *Communications Surveys & Tutorials, IEEE*, 14(4):998–1010, 2012.

[51] Oscar Garcia-Morchon, Sandeep Kumar, Rene Struik, Sye Keoh, and Rene Hummen. Security considerations in the ip-based internet of things. 2013.

[52] James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig. The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the 3rd international symposium on Information processing in sensor networks*, pages 259–268. ACM, 2004.

[53] Jaydip Kamani and Dhaval Parikh. A review on sybil attack detection techniques. *Journal for Research| Volume*, 1(01), 2015.

[54] Kuan Zhang, Xiaohui Liang, Rongxing Lu, and Xuemin Sherman Shen. Sybil attacks and their defenses in the internet of things. 2014.

[55] S Park, K Kim, W Haddad, S Chakrabarti, and J Laganier. Ipv6 over low lower wpan security analysis, draft-daniel-6lowpan-security-analysis-05. *Internet Engineering Task Force*, 2011.

[56] Simone Cirani, Marco Picone, Pietro Gonizzi, Luca Veltri, and Gianluigi Ferrari. Iot-oas: An oauth-based authorization service architecture for secure services in iot scenarios. *Sensors Journal, IEEE*, 15(2):1224–1234, 2015.

[57] Chris Piro, Clay Shields, and Brian Neil Levine. Detecting the sybil attack in mobile ad hoc networks. In *SecureComm*, volume 6, pages 1–11, 2006.

[58] Soyoung Park, Baber Aslam, Damla Turgut, and Cliff C Zou. Defense against sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support. *Security and Communication Networks*, 6(4):523–538, 2013.

[59] Algirdas Avižienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr. Basic concepts and taxonomy of dependable and secure computing. *Dependable and Secure Computing, IEEE Transactions on*, 1(1):11–33, 2004.

[60] ST Choden Konigsmark, Leslie K Hwang, Deming Chen, and Martin DF Wong. System-of-pufs: Multilevel security for embedded systems. In *Hardware/Software Codesign and System Synthesis (CODES+ ISSS), 2014 International Conference on*, pages 1–10. IEEE, 2014.

[61] Jason Xin Zheng and Miodrag Potkonjak. A digital puf-based ip protection architecture for network embedded systems. In *Proceedings of the tenth ACM/IEEE symposium on Architectures for networking and communications systems*, pages 255–256. ACM, 2014.

[62] SK Hafizul Islam and GP Biswas. An improved pairing-free identity-based authenticated key agreement protocol based on ecc. *Procedia Engineering*, 30:499–507, 2012.

[63] Kyung-Ah Shim, Young-Ran Lee, and Cheol-Min Park. Eibas: An efficient identity-based broadcast authentication scheme in wireless sensor networks. *Ad Hoc Networks*, 11(1):182–189, 2013.

[64] Liping Zhang, Shanyu Tang, and He Luo. Elliptic curve cryptography-based authentication with identity protection for smart grids. *PloS one*, 11(3):e0151253, 2016.

[65] Joël Alwen, Rafail Ostrovsky, Hong-Sheng Zhou, and Vassilis Zikas. Incoercible multi-party computation and universally composable receipt-free voting. In *Advances in Cryptology–CRYPTO 2015*, pages 763–780. Springer, 2015.

[66] Karthik Jaganathan, Tanmoy Dutta, Eric C Perlin, Steven L Hiskey, and Cezar Ungureanasu. Identification security elevation, September 24 2013. US Patent 8,544,083.

[67] Chia-Chi Wu, Chin-Chen Chang, and Iuon-Chang Lin. New sealed-bid electronic auction with fairness, security and efficiency. *Journal of Computer Science and Technology*, 23(2):253–264, 2008.

[68] ST Choden Konigsmark, Leslie K Hwang, Deming Chen, and Martin DF Wong. System-of-pufs: Multilevel security for embedded systems. In *Hardware/Software Codesign and System Synthesis (CODES+ ISSS), 2014 International Conference on*, pages 1–10. IEEE, 2014.

[69] Parikshit N Mahalle, Bayu Anggorojati, Neeli Rashmi Prasad, and Ramjee Prasad. Identity establishment and capability based access control (iecac) scheme for internet of things. In *Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on*, pages 187–191. IEEE, 2012.

[70] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. CRC press, 2008.

[71] Oriol Pinol Pinol, Shahid Raza, Joakim Eriksson, and Thiemo Voigt. Bsd-based elliptic curve cryptography for the open internet of things. In *New Technologies, Mobility and Security (NTMS), 2015 7th International Conference on*, pages 1–5. IEEE, 2015.

[72] Viet-Duc Le, Hans Scholten, and Paul Havinga. Unified routing for data dissemination in smart city networks. In *Internet of Things (IOT), 2012 3rd International Conference on the*, pages 175–182. IEEE, 2012.

[73] Stepan Ivanov, Christopher Foley, Sasitharan Balasubramaniam, and Dmitri Botvich. Virtual groups for patient wban monitoring in medical environments. *Biomedical Engineering, IEEE Transactions on*, 59(11):3238–3246, 2012.

[74] Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. Sensing as a service model for smart cities supported by internet of things. *Transactions on Emerging Telecommunications Technologies*, 25(1):81–93, 2014.

[75] Wu He, Gongjun Yan, and Li Da Xu. Developing vehicular data cloud services in the iot environment. *Industrial Informatics, IEEE Transactions on*, 10(2):1587–1595, 2014.

ANEXO

Este anexo descreve uma avaliação da eficácia e do desempenho do mecanismo proposto por [42], chamado *Lightweight Sybil Attack Detection Framework* (LSD). O mecanismo foi escolhido por que ele leva em consideração as características de uma rede IoT, como escalabilidade e baixa complexidade computacional. O LSD, que é baseado na técnica de características das redes, foi implementado no simulador de redes (NS3). Inicialmente, ele foi desenvolvido na versão 2.30 do NS3 considerando apenas o ataque Sybil com identidades fabricadas e nesta avaliação, ele foi migrado para a versão 3.21 e adicionado o ataque Sybil com identidades roubadas. .

Avaliação

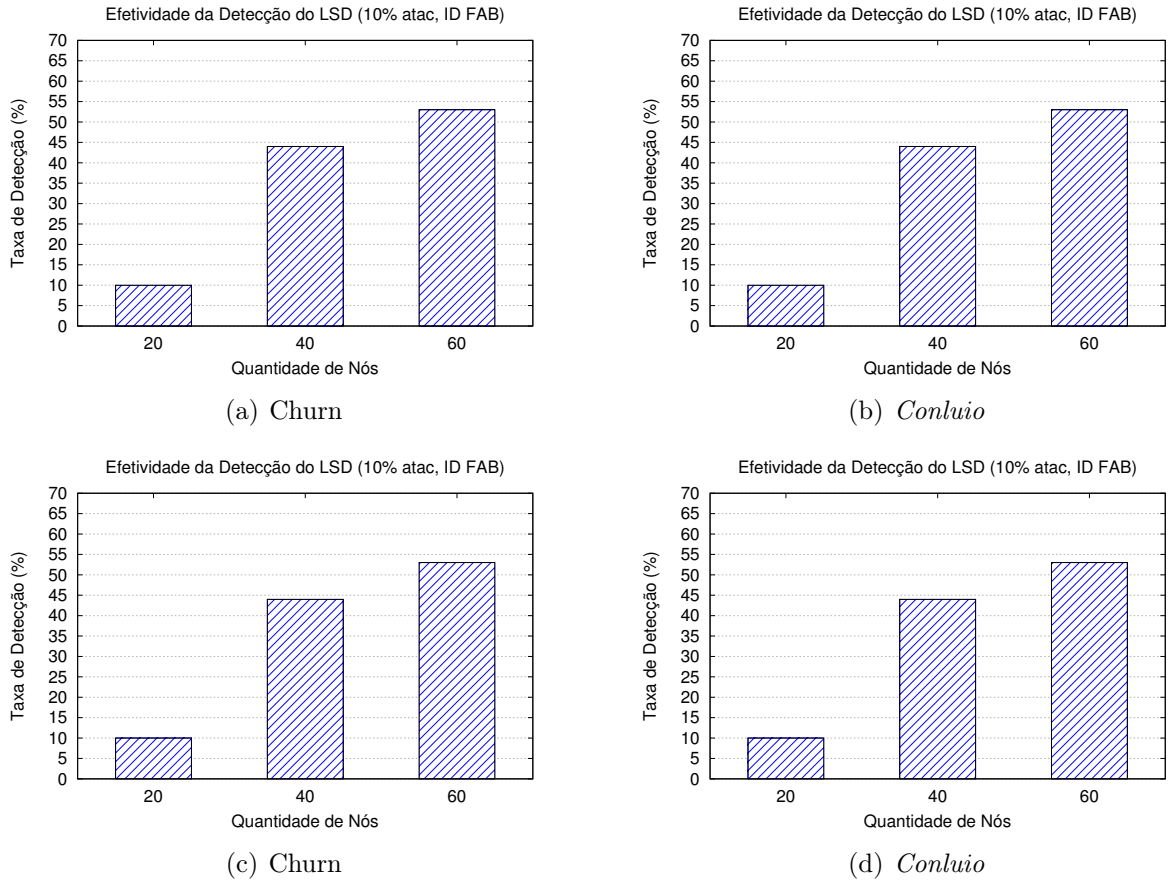
O cenário definido para a avaliação compreende um ambiente equivalente a uma residência. Neste cenário, os nós da rede correspondem à objetos presentes numa residência como geladeira, fogão, televisão, e dispositivos computacionais. Estes nós atuam na rede disseminando um fluxo de dados de forma sequencial para um destino. Um fluxo de dados consiste no envio de uma mensagem de 256 bytes. A escolha de um nó origem e de um nó destino acontece de forma aleatória e o nó origem não pode ser o destino. Assim, o nó origem dissemina um fluxo de dados para os seus vizinhos que encaminham esses dados até o destino. Uma nova disseminação inicia apenas quando todos os dados da disseminação anterior forem entregues ao destino. Já os nós atacantes realizam requisições de associação à rede através de identidades fabricadas e roubadas. A avaliação da eficácia adota requisições de associação de um nó atacante através do comportamento *churn* ou em conluio variando de duas à cinco identidades.

Os parâmetros de simulação usados na configuração da rede IoT consideram a quantidade de nós variando entre 20, 40, e 60. Estes nós podem ser móveis ou fixos, onde os fixos compreendem 25% do total de nós. Eles também emitem a força do sinal recebido (RSS) por até 100 segundos (s) e se deslocam na rede através do modelo de mobilidade aleatório com velocidades entre 0.2m/s a 2m/s. A disseminação de conteúdo realizada pelos nós emprega o padrão 802.15.4. A simulação foi repetida 30 vezes com o intervalo de confiança de 95%, e cada simulação durou 600 segundos. Nos parâmetros do ataque Sybil, o número de atacantes foi fixada em 10% do total dos nós, e o comportamento em conluio solicita associação à rede com até cinco identidades por ataque.

As métricas empregadas na avaliação do mecanismo estão organizadas em eficácia e eficiência do LSD. Na eficácia do mecanismo quatro métricas são adotadas, a ***Taxa de Detecção*** (T_{det}), a ***Acurácia*** (A_c), os ***Falsos Positivos*** (T_{fp}), e a ***Efetividade do Ataque*** (T_{efat}). Já no quesito eficiência, esta avaliação utiliza uma métrica o ***Custo em Tempo de Disseminação*** (C_{diss}). Estas quatro métricas aferem o impacto do atacante no tráfego da rede, e a eficácia do mecanismo na detecção do ataque Sybil. A seguir estas métricas serão apresentadas contextualizando seu objetivo e a forma de obtenção.

Resultados obtidos

Esta subseção descreve os resultados da eficácia e da eficiência do LSD. As Figuras 6.2(a) e 6.2(c) mostram a T_{det} do LSD numa rede sob ataque Sybil com comportamento *Churn*. Nestas figuras, o comportamento *Churn* com identidades roubadas diminuiu a eficácia de detecção do LSD pela metade numa rede esparsa (20 nós). Isto acontece devido à técnica do LSD necessitar da cooperação dos vizinhos para localização de um nó. A redução da eficácia do LSD também ocorre nos cenários mais densos, no entanto ela não é expressiva quanto a de uma rede esparsa. As Figuras 6.2(b) e 6.2(d) mostram a eficácia do LSD sob o ataque Sybil em conluio. Mesmo quando a rede é esparsa, este comportamento tem impacto menor na redução da eficácia do LSD que o *Churn* por que o conluio de identidades não faz associações e dissociações continuas.



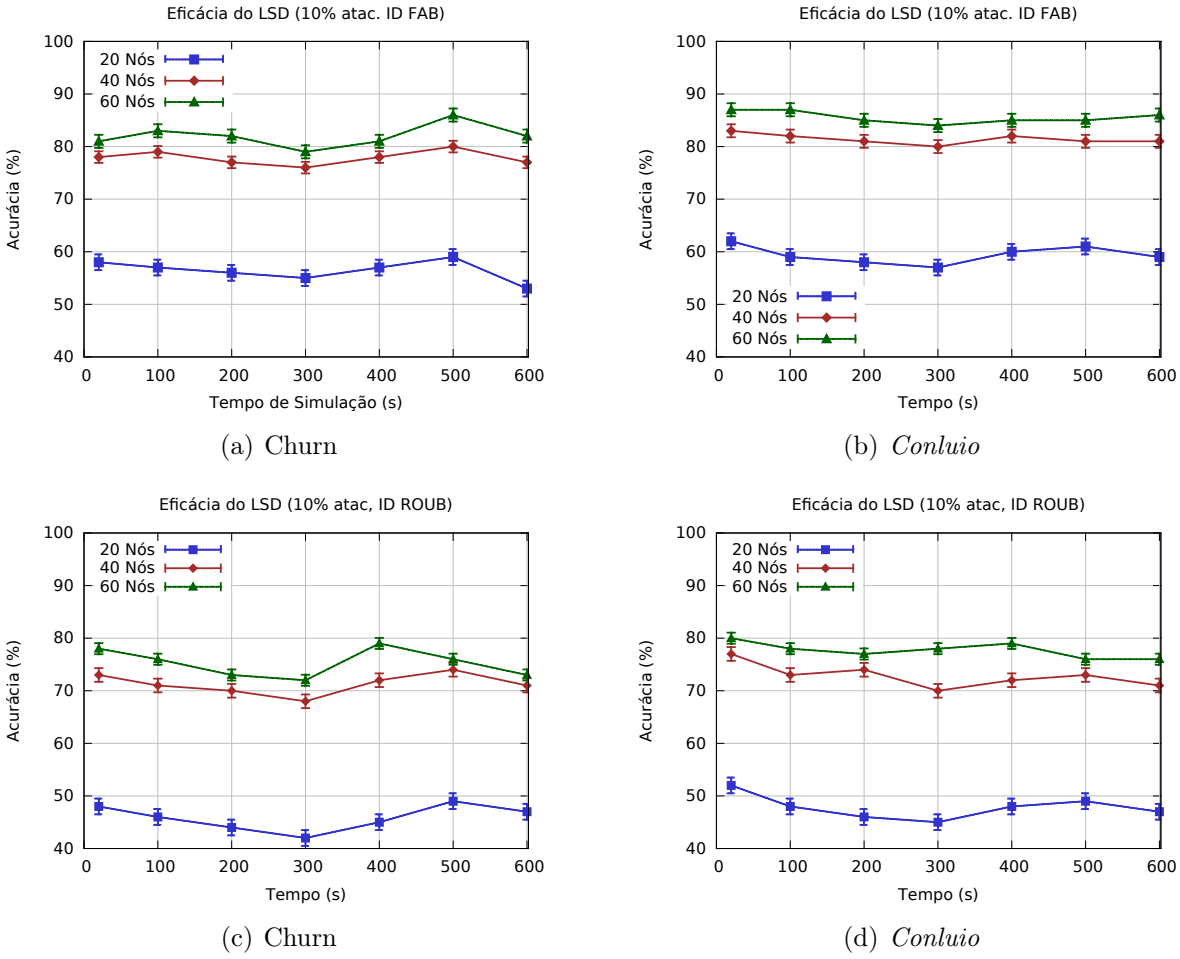
(a) Churn (b) *Conluio*

(c) Churn (d) *Conluio*

Figura 6.1: T_{det} diante do Ataque Sybil com identidades roubadas e fabricadas

As Figuras 6.2(a) e 6.2(b) mostram a acurácia do LSD numa rede sob o ataque Sybil com identidades fabricadas. Nestas figuras, o cenário mais denso, isto é com 60 nós, apresentou uma melhor acurácia, alcançando 81% e 88% respectivamente. Quando a rede torna-se mais esparsa a taxa de detecção é menor devido à quantidade de nós que auxiliam no processo de detecção. Além disso, as precisões das detecções com 20 e 40 nós são menores quando comparada ao cenário mais denso. Isto ocorre devido à variação no intervalo de confiança. As Figuras 6.2(c) e 6.2(d) mostram a acurácia do LSD sob o ataque Sybil com identidades roubadas. Nestas figuras, o comportamento da detecção é inferior à das Figuras 6.2(a) e 6.2(b). A acurácia do

LSD é menor quando o atacante usa identidades roubadas. Esta redução acontece em virtude da técnica de detecção empregada pelo LSD desconsiderar a verificação das identidades legítimas da rede. Logo, ele tem a sua acurácia comprometida quando o ataque Sybil emprega identidades roubadas, o que significa uma maior vulnerabilidade desta técnica na disseminação de conteúdos.



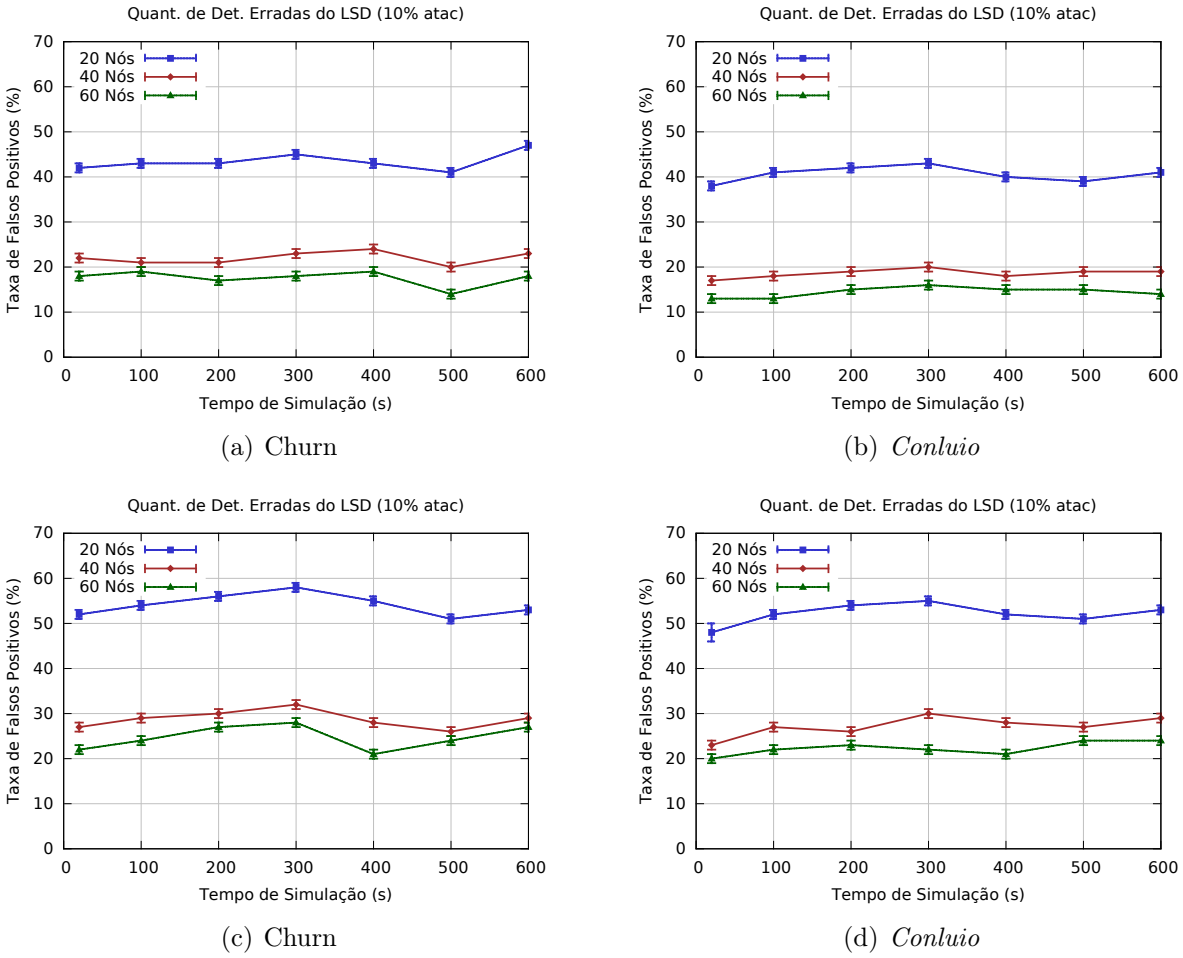
(a) Churn (b) *Conluio*

(c) Churn (d) *Conluio*

Figura 6.2: A_c diante do Ataque Sybil com identidades roubadas e fabricadas

As Figuras 6.3(a) e 6.3(c) mostram o comportamento do LSD numa rede sob o ataque Sybil com o comportamento *Churn*. Ele possui uma alta T_{fp} para ambos tipos de identidades. A medida que a rede torna-se densa, esta taxa diminui, o que mostra a ineficiência do LSD em redes esparsas. Nas Figuras 6.3(b) e 6.3(b), a redução da T_{fp} causada pelo comportamento conluio mostra que o LSD detecta este comportamento com maior efetividade, principalmente quando o ataque usa identidades fabricadas. Logo, o comportamento *Churn* acarreta maiores prejuízos durante a detecção do ataque Sybil na disseminação de conteúdos.

As Figuras 6.4(a) e 6.4(b) mostram a efetividade do ataque Sybil com identidades fabricadas numa rede com o LSD. Nesta figura, a efetividade do ataque num cenário esparso é superior aos dos cenários mais densos, ou seja com 40 e 60 nós. Isto ocorre por que a quantidade de nós que realizam a detecção de um atacante é menor, obtendo uma menor quantidade de detecções. No instante 300 ocorre o ápice de ataques, justificando a redução da acurácia do LSD, vide Figura 6.2(a) instante 300. A efetividade do ataque Sybil com identidades roubadas, Figu-



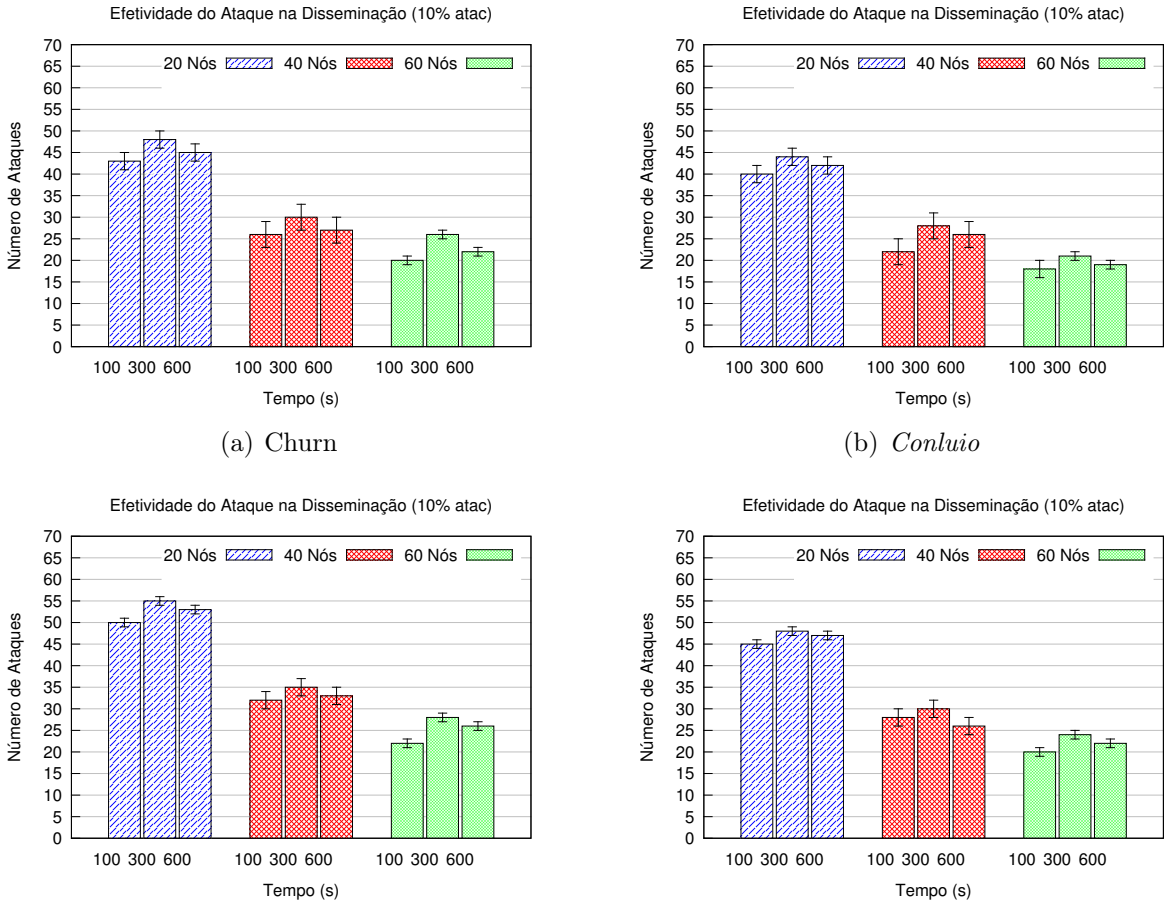
(a) Churn (b) *Conluio*

(c) Churn (d) *Conluio*

Figura 6.3: T_{fp} diante do Ataque Sybil com identidades roubadas e fabricadas

ras 6.4(c) 6.4(d), é ainda maior quando comparado aos resultados das Figuras 6.4(a) e 6.4(b). Os atacantes obtiveram um maior exito por que as identidades foram roubadas de nós legítimos. O ataque Sybil obteve um maior sucesso no cenário mais esparso, visto que o LSD não verifica a veracidade de uma identidade e a quantidade de vizinhos é menor.

A Figura 12 mostra o impacto causado pelos comportamentos do ataque Sybil no desempenho da disseminação de conteúdo. Nestas figuras é possível observar como o comportamento do ataque Sybil influencia na disseminação. No instante 100 segundos da Figura 6.5(c), um dado nó numa rede de 20 nós disseminou um fluxo de dados até um nó destino gastando 0.18 ms. Na Figura 6.5(d), neste mesmo instante um dado nó disseminou o mesmo fluxo em 0.1 ms. O aumento do C_{diss} causado pelo comportamento *churn* do ataque Sybil ocorreu devido à autenticação do LSD necessitar de um tempo hábil para identificar um atacante, pois ele realiza constantes associações e dissociações na rede, o que causa sobrecarrega e aumenta o custo para disseminar um fluxo até um destino. Assim, o ataque Sybil com o comportamento *churn* reduz a eficiência da disseminação de conteúdo acarretando uma redução na qualidade de serviços.



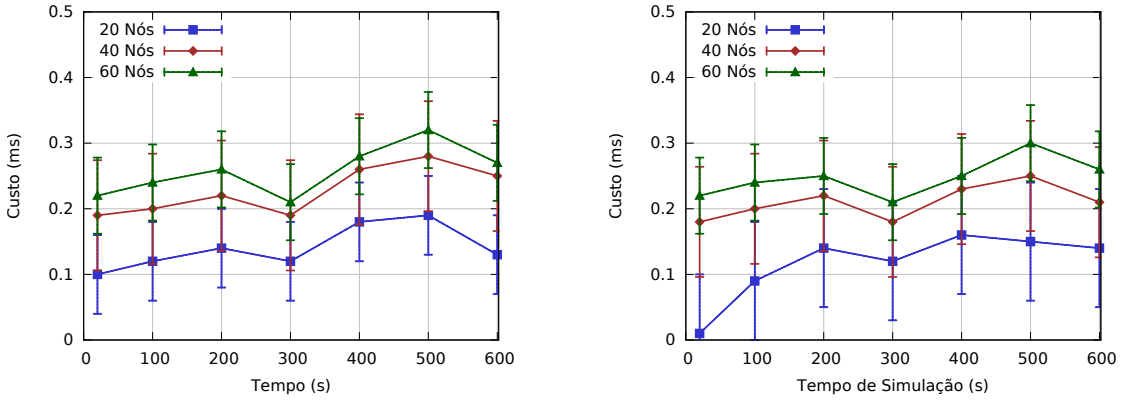
(a) Churn

(b) *Conluio*

(c) Churn

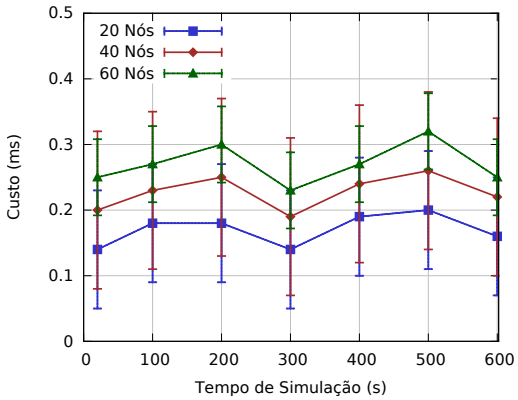
(d) *Conluio*

Figura 6.4: Quantidade de Ataques na Disseminação

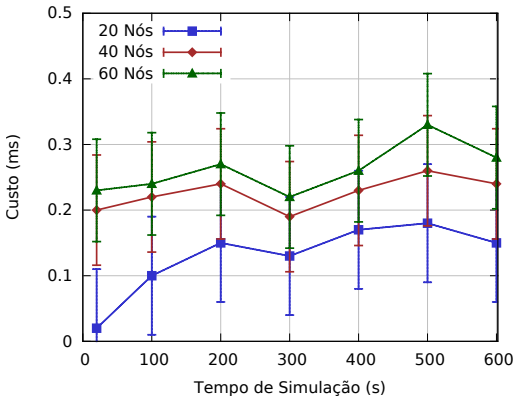


(a) Churn

(b) *Conluio*



(c) Churn



(d) *Conluio*

Figura 6.5: Custo para a disseminação de fluxos de dados