Um controle de associações resistente a ataques Sybil para a disseminação segura de conteúdo da IoT*

Danilo Evangelista[1], Eduardo da Silva[1,2], Michele Nogueira[1], Aldri Santos[1]

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

[2]Departamento de Informática Instituto Federal Catarinense – Araquari, SC – Brazil

eduardo@araquari.ifc.edu.br, {dfrevangelista,michele,aldri}@inf.ufpr.br

Abstract. *The Internet of Things (IoT) comprises a diversity of heterogeneous objects that collect and disseminate data for Internet applications. The content dissemination on these networks is subject to various malicious actions, such as the identities impersonation made by Sybil attack. Although there are several Sybil attack detection techniques, such as LSD, they are costly, disregard heterogeneous devices and attackers with stolen identities. This work presents a association control mechanism for IoT, called SA^{2}CI, which prevents the access Sybil attackers on content dissemination service. The SA^{2}CI uses elliptic curve cryptography (ECC), physical unclonable functions (PUF), and identities receipts. The ECC technique provides key distribution and stablishes a secure channel with low cost. The physical unclonable function enables the verification of a device identity. Then, a receipt identity, calculated by the a device PUF, ensures its legitimacy. The effectiveness and efficiency of SA^{2}CI were evaluated in IoT network using Network Simulator 3 (NS3).*

Resumo. *A Internet das coisas (IoT) compreenderá uma diversidade de objetos heterogêneos integrados que coletam e disseminam conteúdo com diferentes propósitos de aplicações. Logo, uma disseminação segura na IoT é essencial, visto que ela está sujeita a diversas ações maliciosas, como a personificação de identidades por ataques Sybil que buscam violar a confidencialidade do conteúdo disseminado. Contudo, as técnicas existentes de detecção de ataques Sybil desconsideram o uso de identidades roubadas e de dispositivos heterogêneos, e em geral são custosas. Este trabalho apresenta um mecanismo de controle de associações para IoT, chamado SA^{2}CI, que previne o acesso de atacantes Sybil ao serviço de disseminação de conteúdo. O SA^{2}CI emprega criptografia de curvas elípticas (ECC) que prover uma distribuição de chaves e criação de um canal seguro com baixo custo, aplica funções não clonáveis (PUF) na comprovação da identidade dos dispositivos, e recibos de identidade para garantir a legitimidade dos dispositivos. Uma avaliação feita no NS3 mostra a eficácia do SA^{2}CI no controle de associações diante de ataques Sybil.*

1. Introdução

A crescente necessidade de serviços personalizados e autônomos tem possibilitado o desenvolvimento da Internet das coisas (IoT). Uma IoT permite que objetos (coisas) como

*Artigo parcialmente apoiado pelo CNPq projetos nº 488004/2013-6, 486393/2013-5 e 310609/2014-3

geladeiras, máquinas de lavar, aparelhos de ar-condicionado e dispositivos computacionais estejam conectados com as pessoas em qualquer momento e lugar. Um serviço fundamental nas IoTs é a disseminação de conteúdos, que possibilita a implementação eficaz de outros serviços como o monitoramento do consumo de água, da temperatura de um cômodo, e o acompanhamento dos dados vitais de uma pessoa, em tempo real. Isso promove um maior conforto e bem estar às pessoas, propiciando a implementação de ambientes inteligentes, como casa, hospitais e rodovias [Perera et al. 2014].

Uma vez que a disseminação de conteúdo é base ao provimento serviços da IoT, ela demanda garantia da sua segurança contra ações maliciosas. Dentre as ações maliciosas numa IoT destaca-se a personificação de identidades realizada pelo ataque Sybil. Em resumo, um atacante Sybil usa identidades forjadas visando o acesso à rede, incluindo o acesso à disseminação dos dados [Wallgren et al. 2013]. Logo, um atacante autenticado numa rede IoT busca alcançar vantagens como o uso de recursos não autorizados, a obtenção de informações vitais, infligindo a confidencialidade e a privacidade dos usuários da rede. Portanto, a qualidade dos serviços suportados pela disseminação de conteúdo é afetada, comprometendo a segurança dos dados trafegados na rede.

Diversas técnicas são encontradas na literatura para detectar ataques Sybil, que são classificadas neste trabalho em três grupos: baseadas nas características da rede [Vamsi and Kant 2014], em criptografia [Park et al. 2013], e no relacionamento entre vizinhos [Quercia and Hailes 2010]. A técnica baseada nas características das redes considera aspectos dos nós, como a força do sinal recebido (RSS) e a mobilidade, para identificar um ataque. Apesar de considerar a restrição de recursos dos dispositivos, ela não é eficaz contra ataques Sybil [Evangelista et al. 2015]. Já a técnica baseada em criptografia emprega chaves simétricas e assimétricas para garantir a irretratabilidade das identidades de uma rede. No entanto, ela necessita de constantes atualizações dos novos pares de chaves, sobrecarregando a rede. Por fim, a técnica baseada no relacionamento entre os vizinhos considera as opiniões sobre um nó emitidas por seus vizinhos. Contudo, um nó malicioso que simule um comportamento legítimo pode ludibriar o sistema. Logo, surge a necessidade de uma solução eficaz contra a associação de atacantes à rede e que considere as restrições de recursos dos dispositivos da IoT.

Este trabalho apresenta um mecanismo chamado SA^2CI (***S**ybil **A**ttack **A**ssociation **C**ontrol for **I**oT*) que previne associações de atacantes Sybil na disseminação de conteúdo da IoT. O SA^2CI atua entre as camadas de rede e aplicação sendo um *middleware* para apoiar a disseminação segura de conteúdo. Ele emprega criptografia de curvas elípticas (ECC) para a distribuição de chaves seguras a um baixo custo computacional e a criação de canais seguros entre dispositivos heterogêneos. Com um canal seguro, o SA^2CI aplica funções não clonáveis (PUF), extraídas do hardware dos dispositivos, para a comprovação da sua identidade, e associa aos recibos de identidade garantindo a legitimidade dos dispositivos. O SA^2CI foi avaliado por meio de simulações e os resultados comprovam a sua resistência a ataques Sybil, assegurando a disseminação segura de conteúdo.

O restante do artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados sobre detecção de ataques Sybil. A Seção 3 descreve mecanismo SA^2CI, suas fases de operação e seu funcionamento diante de ataques. Já a Seção 4 mostra uma avaliação do SA^2CI para suportar disseminação de conteúdo na IoT diante SA's e uma comparação com o mecanismo LSD. Por fim, a Seção 5 conclui o trabalho.

2. Trabalhos Relacionados

A necessidade de se garantir uma disseminação segura na Internet das coisas (IoT) torna-se providencial para o provimento dos serviços implementados por ela. As técnicas existentes de detecção de ataques Sybil encontradas na literatura geralmente são classificadas em **características das redes**, **criptografia**, e **relacionamento entre vizinhos**. Como a IoT requer soluções leves, dinâmicas, e eficientes, o uso destas técnicas no âmbito da IoT pode acarretar numa disseminação ineficaz. Isto acontece por que os trabalhos que empregam tais técnicas desconsideram estes requisitos.

Os trabalhos de detecção do ataque Sybil baseados nas características das redes em geral ressaltam a necessidade da solução ser leve e eficaz [Vamsi and Kant 2014]. Dentre os trabalhos encontrados na literatura, o mecanismo Lightweight Sybil Attack Detection (LSD) [Abbas et al. 2013], que emprega a técnica das características da rede, é uma solução leve e dinâmica. O LSD identifica o ataque Sybil através das características do RSS e da mobilidade dos dispositivos. Para realizar a detecção de um atacante, estas características são avaliadas por um conjunto de dispositivos da rede de modo à verificar o comportamento durante uma associação de um novo participante. Em seguida um dispositivo da rede armazena o RSS e a identidade numa tupla, e a identificação de um atacante ocorre quando esta identidade não condiz com o valor estimado pelos dispositivos através do seu RSS. Contudo, essa abordagem é vulnerável quando um atacante emprega identidades roubadas uma vez que ela ignora a irretratabilidades das identidades dos dispositivos da rede. Como o LSD adota a técnica de características das rede, ele requer de uma série de análises, e isto acarreta a uma alta taxa de falsos positivos.

Para uma solução garantir a disseminação segura diante de ataques Sybil na IoT é necessário que ela seja dinâmica, leve, escalar, confidencial e trate a irretratabilidade das identidades dos dispositivos. O estabelecimento de um canal seguro entre os componentes de uma rede propicia a disseminação de dados de forma confidencial, onde apenas os dispositivos em comum acordo de chaves tem acesso à informação. Dentre as técnicas existentes as quais asseguram um canal seguro, as cuvas elípticas [Mahalle et al. 2012, Chatzigiannakis et al. 2011] despontam como promissora para o uso na IoT, uma vez que ela demanda uma baixa quantidade energética para gerar pares de chaves, podendo ser empregada numa gama maior de dispositivos com ou sem restrições. Já a irretratabilidade dos dispositivos é alcançada por meio de técnicas de comprovação e garantia de identidades. Logo, o uso da função não clonável (PUF) [Choden Konigsmark et al. 2014, Zheng and Potkonjak 2014] associada com recibos de identidades [Wu et al. 2008] proporcionam a irretratabilidade das identidades dos dispositivos. O recibo de identidade permite identificar um dispositivo de forma única, sendo ele apenas necessário numa associação escalar a uma rede IoT. Assim, atendendo estes requisitos seria possível suportar uma disseminação segura diante de ataques Sybil.

3. Mecanismo contra Ataque Sybil

Para apoiar a disseminação de dados segura contra ataques Sybil é o proposto um mecanismo para controle de associações, chamado SA^2CI (*Sybil Attack Association Control for IoT*). O SA^2CI atua como um *middleware*, entra as camadas de rede e aplicação, e assegura que os dispositivos (nós) disseminem conteúdos de forma segura e resiliente à ataques Sybil. Ele 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. O SA^2CI assume nós com ou sem restrições de recursos.

3.1. Modelo da rede e do ataque

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 nó ($\mathcal{N}_S$) 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.

O nós que não possuem restrição de recursos são denotados por $\mathcal{N}_{KDC}$ enquanto $\mathcal{N}_{MOV}$ denota os nós com recursos limitados. 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} e os demais são denominados nós N_{MOV}. O relacionamento entre um N_{KDC} e um N_{MOV} ocorre a partir de uma função sobrejetora $F : \mathcal{N}_{KDC} \rightarrow \mathcal{N}_{MOV}$, em que 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 $\mathcal{N}_{KDC}$ não podem se associar aos $\mathcal{N}_{MOV}$ por conta da limitação de recurso destes.

O meio de transmissão 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, sendo que a estratégia de disseminação não impõe restrições na capacidade de detecção do SA^2CI. Sem a perda da generalidade, para evitar que os nós do conjunto $\mathcal{N}_{MOV}$ gastem seus recursos utilizando o *flooding*, neste trabalho é adotado um modelo de disseminação baseado nas capacidades dos dispositivos [Le et al. 2012]. 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.

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 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 diver-

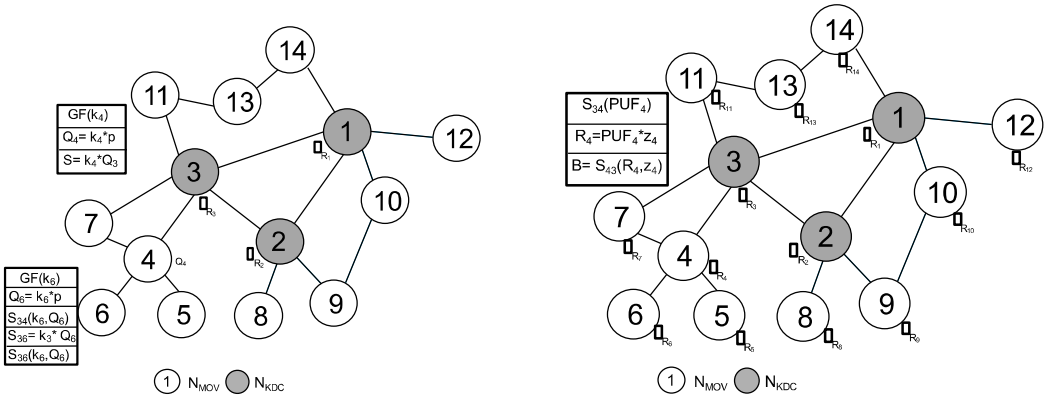
sas identidades, solicitando associação à rede. Um atacante com este comportamento se passa por mais de um nó legítimo apresentando identidades aos nós autenticadores com uma frequência baixa, e tentando reproduzir um dispositivo legítimo. Logo, ambos os comportamentos visam ludibriar um nó que executa a autenticação na rede.

3.2. Mecanismo de controle de associações para IoT - (SA^2CI)

Na 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 [Guicheng and Zhen 2013]. 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.

3.2.1. Inicialização

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 é necessário apenas nesta etapa. A curva elíptica é expressa pela equação de Weierstrass, $y^2 = x^3 + Ax + B$, em que A e B são constantes [Pinol et al. 2015]. 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.



(a) Inicialização - Distrib. dos Pares de Chave

(b) Configuração - Criação do recibo

Figura 1. Operações de Inicialização e configuração do mecanismo

É considerado um sistema de coordenadas projetivas jacobianas, que possibilita a representação dos pontos de uma curva E em um espaço projetivo P_k [Pinol et al. 2015], evitando assim multiplicações no grupo $E(GF)$. Isto permite gerar uma curva com menos recursos computacionais quando comparado 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 1(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. 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.

3.2.2. Configuração

A configuração da rede visa estabelecer os pares de chaves entre os nós $\mathcal{N}_{MOV}$ e os seus respectivos $\mathcal{N}_{KDC}$. Ambos os tipos de nós, ($\mathcal{N}_{MOV}$ e $\mathcal{N}_{KDC}$), participam dessa fase. Um nó pode ser configurado de forma direta ou indireta. Na primeira, um nó $\mathcal{N}_{KDC}$ realiza a configuração de um novo nó, enquanto que na segunda forma um $\mathcal{N}_{MOV}$ já associado na rede atua como intermediário entre um novo nó e o seu respectivo $\mathcal{N}_{KDC}$.

Após a criação e compartilhamento da curva elíptica E, os nós N_{KDC} geram 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 (Q_{N_x}) é computada por meio da sua chave privada multiplicada 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.

Então, cada nó N_{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 $S_x = Q_{N_x} \times K_{kdc}$. Após a criação do segredo compartilhado, cada nó $\mathcal{N}_{MOV}$ envia o seu código PUF$_x$ ao seu respectivo nó KDC, comprovando a sua identidade. A PUF do um dado nó é um código único extraído do hardware deste nó que permite a sua identificação. 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. Assim, cada nó $N_x \in \mathcal{N}_{MOV}$ envia sua PUF$_x$ cifrada com o segredo (S_x) ao seu respectivo nó KDC.

Ao receber a PUF do nó $N_x \in \mathcal{N}_{MOV}$, o nó N_{KDC} gera o recibo R_{N_x} para o nó N_x, a partir da PUF$_x$ e um ponto $z \in E$, obtendo $R_{N_x} =$ PUF$_x \times z$. Em seguida, o nó N_{KDC} cifra o recibo R_{N_x} com o segredo compartilhado S_x e o envia juntamente com o ponto z da curva ao nó N_x. Ao final deste processo, cada nó N_x recebe o seu R_{N_x}. Com esse recibo, um nó pode obter acesso à rede IoT e aos seus serviços. Por fim, os nós KDCs atualizam a sua lista de recibos gerados, de modo que todos os demais nós KDCs possuam os recibos dos legítimos, permitindo a sua verificação a partir de qualquer requisição.

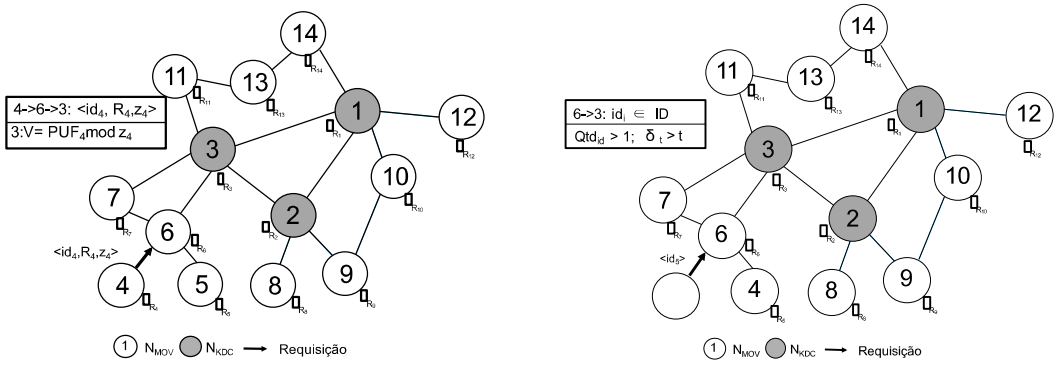
A Figura 1(b) ilustra o funcionamento da configuração dos nós $\mathcal{N}_{MOV}$ realizada pelos nós $\mathcal{N}_{KDC}$. No exemplo da Figura 1(a), N_3 gera um par de chaves privada K_4 e pública Q_4 para N_4. Com a chave pública de N_4, N_3 emite um segredo S_4 e compartilha

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 1(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, que pode utilizá-la para realizar uma requisição de acesso à rede, comprovando a legitimidade da sua identidade.

3.2.3. 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 ao serviço de disseminação de dados. Uma associação à rede consiste de uma requisição de acesso, em que o nó solicitante envia a sua identidade e o seu recibo, no caso de reassociação, ou apenas o pedido de nova associação se for um novo nó.

Quando um nó que não foi configurado deseja acesso à rede, ele realiza uma nova associação. Numa nova associação, este nó (N_x) tem o seu comportamento avaliado. Para isso, tanto um $\mathcal{N}_{MOV}$ quanto o $\mathcal{N}_{KDC}$ monitoram o comportamento de N_x durante a sua associação à rede, verificando se o seu comportamento é ou não malicioso através das assinaturas maliciosas conhecidas. Tais assinaturas consistem, por exemplo, em entrar e sair várias vezes da rede mudando de identidade ou exibir múltiplas identidades. Uma nova associação enviada por N_x compreende de apenas um campo, a identidade $< Id_x >$ de N_x. Assim, caso não seja detectado um comportamento malicioso de N_x, este nó tem o seu acesso concedido, recebendo um recibo correspondente à identidade apresentada.



(a) Reassociação (b) Nova Associação

Figura 2. Monitoramento das associações da rede

A Figura 2 mostra o funcionamento desta etapa, em que os nós da rede autenticam as reassociações e as novas associações. 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 verifica se a identidade apresentada na requisição equivale ao recibo R_{N_4}. Esta verificação acontece através de $V = PUF_{N_4} \mod z_{N_4}$, que confirma a veracidade do recibo. Se o recibo apresentado na requisição for verdadeiro, N_1 concede o acesso a este nó, caso contrário o acesso não é autorizado. 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. Ao avaliar a conduta de N_5 (Figura 2), o nó N_1 pode detectar um comportamento malicioso desassociando este nó ou, caso contrário, ele será configurado na rede.

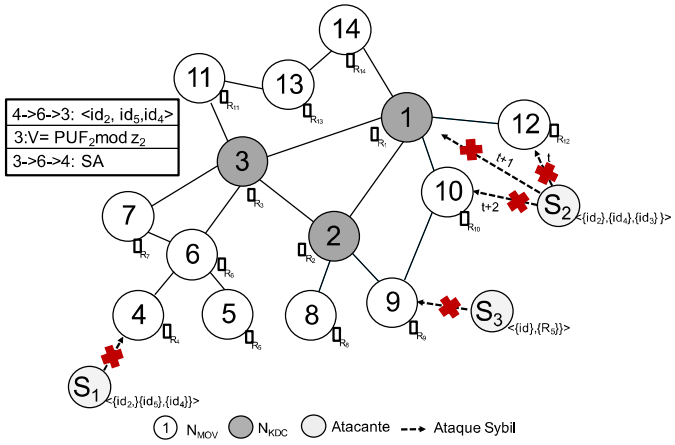


Figura 3. Detecção do SA

A detecção dos ataques Sybil, com comportamento de múltiplas identidades e *churn*, é ilustrada na Figura 3. Nela, o nó N_4 identifica um atacante com múltiplas identidades, S_1, no instante que ele exibe as identidades através da tripla $< id_2$,id_5,$id_4 >$ durante a associação à rede. Inicialmente, o nó N_4 averigua a conduta de S_1, verificando as assinaturas maliciosas conhecidas. Com a conduta legitima, o nó S_1 apresenta uma dada identidade falsa e inicia-se o processo de autenticação dessa identidade. O nó N_4 detecta a requisição maliciosa de S_1 neste momento, porque S_1 apresenta uma identidade que já possui um recibo associado e que não foi apresentado.

Um segundo atacante, S_2, apresenta o comportamento *churn* ao tentar o acesso à rede. Os nós N_{10} e N_{12} identificam a conduta de S_2 durante a avaliação da conduta, pois nos tempos t e $t+1$ o atacante S_2 realizou pedidos de associações num tempo menor do que a assinatura $\delta_{solicitacao} > t$. Caso S_2 apresente pedidos de associação num tempo maior do que assinatura $\delta_{solicitacao} \geq t$, a má conduta é identificada através da verificação da identidade e do seu respectivo recibo utilizando a função $Vreq$.

Um terceiro atacante, S_3, tenta o acesso ao serviço de disseminação por meio de uma identidade forjada id_5 associada com um recibo R_5 também forjado. O nó N_9 detecta o atacante de modo indireto. No pedido de acesso à rede, N_9 envia a tupla $< id_5, R_5 >$ ao nó KDC N_2 cifrada com o seu segredo $S_{9,2}$, para que ele verifique a veracidade de R_5. O nó N_2 executa a função $Vreq$, obtendo o resultado da legitimidade do recibo. Como esse recibo não condiz com a identidade forjada, o nó S_3 é desassociado da rede.

4. Avaliação

A eficácia do mecanismo SA^2CI sobre o controle de associações à disseminação de conteúdo da IoT diante de ataques Sybil foi avaliada e comparada com o mecanismo LSD (*Lightweight Sybil Attack Detection*) [Abbas et al. 2013]. Ambos os mecanismos foram implementados no simulador 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. Também foram implementados

os ataques Sybil com identidades fabricadas e roubadas, apresentando o comportamento churn e de múltiplas identidades.

Os mecanismos foram avaliados num cenário residencial como o descrito em [Le et al. 2012], 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. No 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 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. As Tabelas 1 e 2 resumem os parâmetros usados na configuração da rede IoT e no ataque Sybil. Nesta avaliação, os valores obtidos nas duas primeiras métricas, $MTBF$ e $MTTR$ definidas a seguir, consistem de apenas uma rodada de simulação com o objetivo de observar o funcionamento dos mecanismos. Já nas demais métricas foram consideradas trinta repetições da simulação com um intervalo de confiança de 95%.

Tabela 1. Parâmetros dos Nós

Parâmetro	Valores
Área	$25m$x$25m$
Qtd. de nós	20,40,60
Raio de alcance	$10m$ (KDC) e $100m$ (MOV)
Mod. de mobilidade	Random Waypoint
Vel. dos nós	0,2m/s a 2m/s
Tempo de simulação	600 s

Tabela 2. Parâmetros da Rede e do Ataque

Parâmetro	Valores
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

As métricas utilizadas na avaliação da eficácia do mecanismo SA^2CI são: ***Tempo médio entre falhas*** ($MTBF$), ***Tempo médio de reparo*** ($MTTR$), ***Taxa de Detecção*** (T_{det}), ***Acurácia*** (A_c), e ***Falsos Positivos*** (T_{fp}). Já ***Consumo Energético*** (CE) mede o custo da energia gasta pelo mecanismo. O $MTBF$ identifica o intervalo de tempo entre falhas do mecanismo na detecção de um ataque (Eq. 1). O $MTTR$ calcula o intervalo de tempo gasto para se recuperar uma falha causada por um atacante (Eq. 2). A T_{det} contabiliza os ataques Sybil identificados corretamente do total de ataques (Eq. 3). A métrica A_c indica a precisão da detecção, e corresponde ao total de detecção do ataque Sybil, det_{ni} mais o total de identificação correta dos nós legítimos da rede, det_{na}, dividido pela quantidade de requisições feitas à rede, T_{req}, (Eq. 4). A T_{fp} determina a quantidade de vezes que os mecanismos identificaram um ataque Sybil inexistente (Eq. 5).

$$MTBF = \frac{T}{d} \quad (1)\ MTTR = \frac{\sum_{i=1}^{d} T_i}{d} \quad (2) T_{det} = \frac{\sum det_{ni}}{Tatq} \quad (3)\ A_c = \frac{\sum det_{ni} + \sum det_{na}}{Treq} \quad (4) \quad T_{fp} = \frac{\sum det_{ni}}{Treq_l} \quad (5)$$

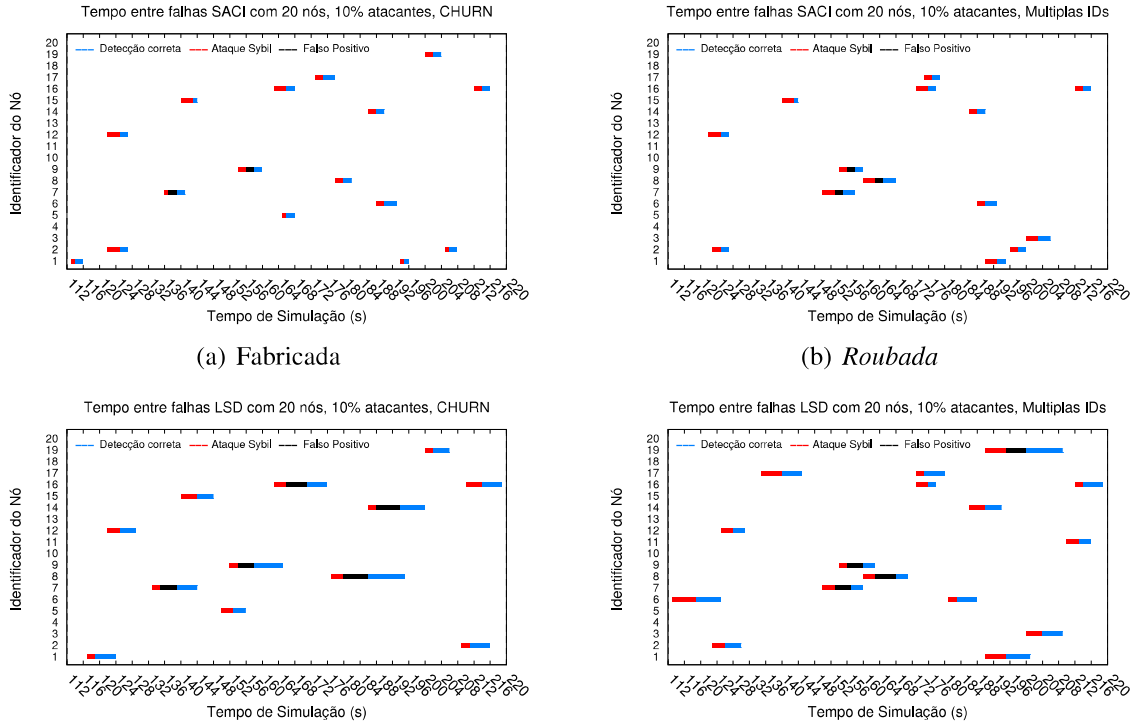
A métrica CE determina o consumo energético dos nós da rede com o mecanismo SA^2CI, sendo obtida através do somatório da energia inicial dos nós da rede, TE_i, subtraído do total restante de energia destes nós, TE_r, (Eq. 6).

$$CE = \sum(TE_i - TE_r) \quad (6)$$

4.1. Resultados

Os resultados inicialmente apresentados nesta seção mostram o funcionamento do SA^2CI e do LSD ao analisar seu desempenho em termos do tempo médio entre falhas e de recuperação diante de falhas num ambiente controlado onde foi realizada apenas uma rodada de simulação. As

falhas na detecção do ataque Sybil no SA^2CI e no LSD são mostradas nos gráficos da Figura 4. Estes gráficos descrevem um intervalo de tempo do funcionamento dos mecanismos em relação ao tempo total de simulação, onde os atacantes empregam identidades legitimas da rede. A faixa de tempo vermelha significa o período de tempo entre o inicio de um ataque e a sua percepção pelo mecanismo, já a preta representa o tempo de uma detecção errada até a percepção do diagnóstico equivocado, enquanto a azul equivale o intervalo de tempo entre uma detecção correta e a eliminação da falha. Nos gráficos, percebe-se que o SA^2CI detecta uma presença maliciosa, num curto espaço de tempo, em média 2 segundos. Já o LSD necessita de um tempo maior para identificar o ataque, uma vez que ele requer a mensuração do RSS pelos nós vizinhos durante a autenticação. Além disso, o LSD uma vez feita uma identificação errada, ele exige mais tempo para corrigir tal erro (faixa preta), para remover o ataque. Isto deve-se ao atraso na aferição dos valores de RSS e esses valores não serem precisos. No SA^2CI, os falsos positivos ocorreram em nós $\mathcal{N}_{MOV}$, que possuiam limitação de energia ou desconectaram-se devido à mobilidade.



(a) Fabricada (b) *Roubada*

(c) Fabricada (d) *Roubada*

Figura 4. Falhas do SA^2CI e LSD diante de ataques Sybil

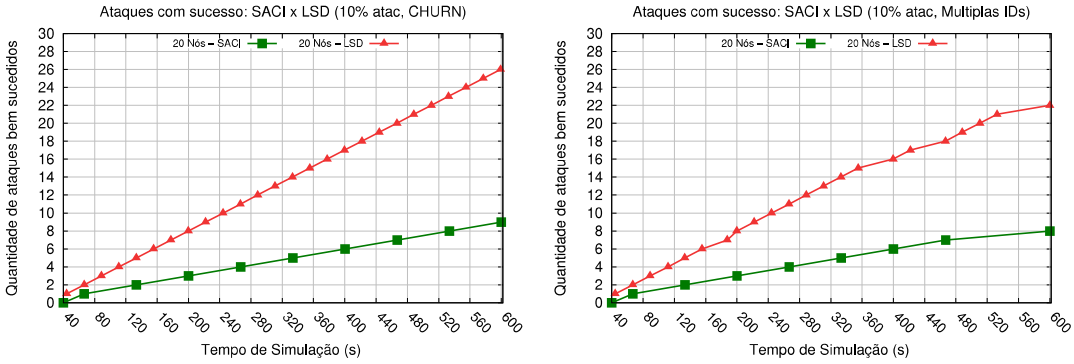
A Tabela 3 exibe o *MTBF* e o *MTTR* dos dois mecanismos na qual a frequência de falhas e o tempo de recuperação delas são menores no SA^2CI do que no LSD independente da quantidade de nós.

Tabela 3. 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

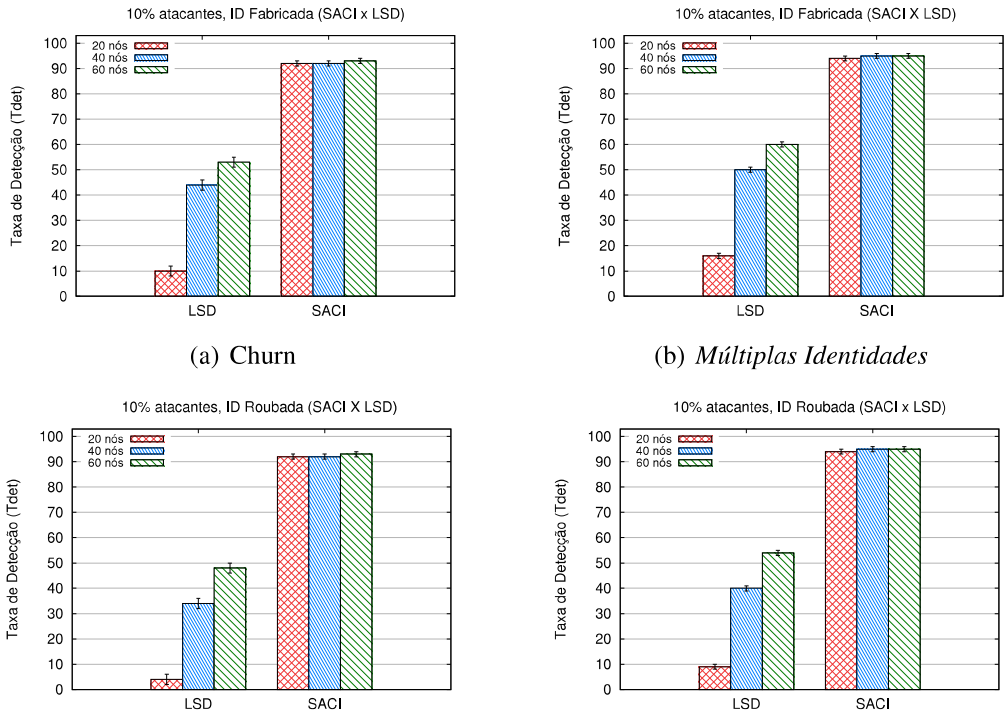
A resistência ao comportamento dos ataques Sybil é mostrada nos gráficos da Figura 5, onde a quantidade de ataques com sucesso é contabilizada ao longo do tempo. Percebe-se que

independente do comportamento, os ataques Sybil são mais difíceis de serem detectados pelo LSD. O gráfico 5(a) mostra que no SA^2CI apenas nove ataques obtiveram sucesso. Já no 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(b). 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. Efetividade do Ataque Sybil no SA^2CI e no LSD



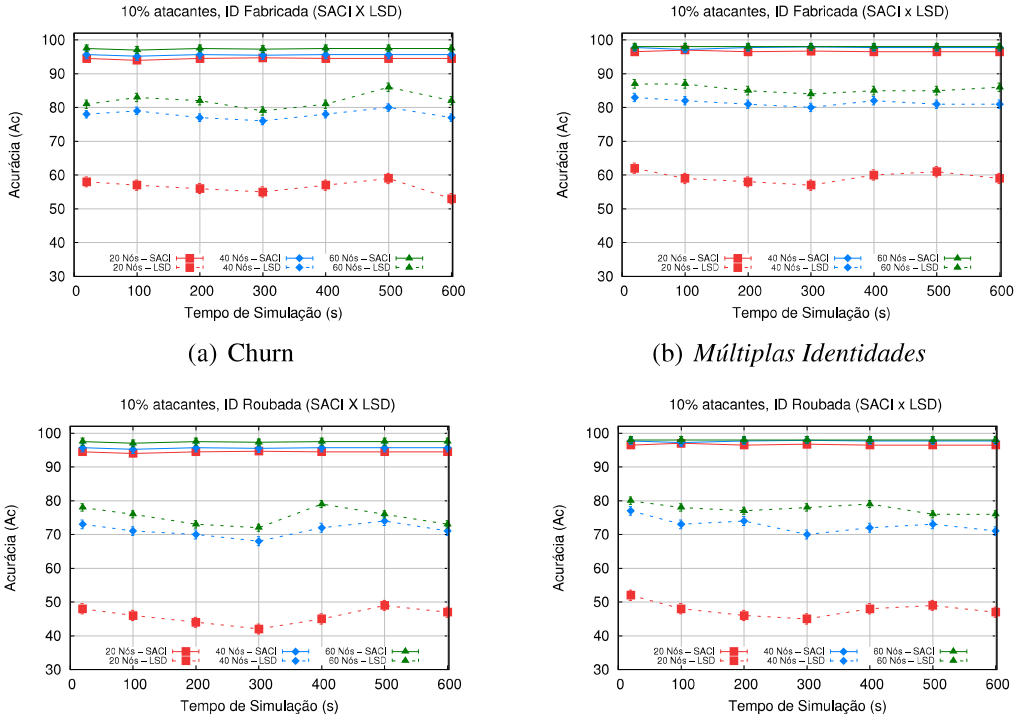
(a) Churn (b) *Múltiplas Identidades*

(c) Churn (d) *Múltiplas Identidades*

Figura 6. Comparativo entre taxa de detecção

Este bloco de resultados tem como objetivo a discursão dos resultados relacionados a métricas de segurança, isto é, T_{det}, A_c, e T_{fp}, aonde são considerados trinta repetições de simulação para cada métrica. Os gráficos da Figura 6 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 do RSS do 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, 5% com 20 nós e identidades roubadas, possuindo uma baixa T_{det} pois ele desconsidera a irretratabilidade das identidade 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.



(a) Churn (b) *Múltiplas Identidades*

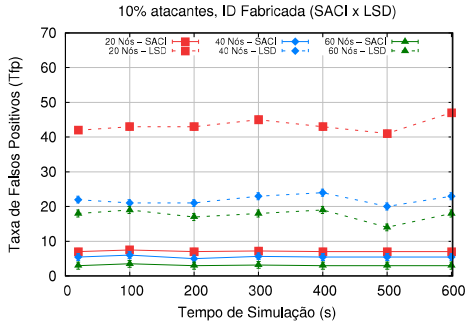
(c) Churn (d) *Múltiplas Identidades*

Figura 7. Comparativo entre as acurácias

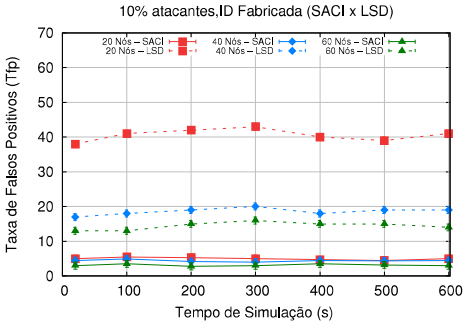
Os gráficos da Figura 7 mostram a A_c de ambos os mecanismos. O comportamento constante do SA^2CI ocorre em razão da técnica empregada necessitar apenas do recibo de identidades para realizar a detecção. Esta forma de detecção é diferente da técnica usada pelo LSD, que requer uma constante mensuração do RSS dos nós. Além disso, o comportamento de uma atacante durante uma associação interfere muito pouco na acurácia do SA^2CI, onde ela reduz 3% em cenários mais esparsos quando os ataques empregam o churn no lugar de múltiplas identidades. 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 8 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. Por outro lado, os ataques Sybil com o comportamento churn aumentam a taxa da falsos positivos de

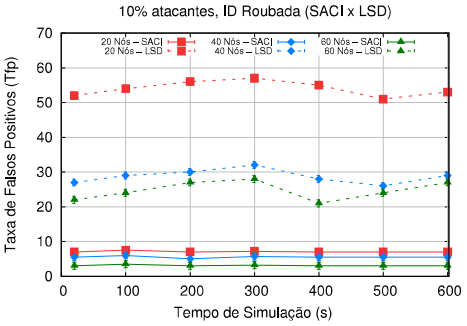
ambos os mecanismos em relação ao ataques de multiplas identidades.



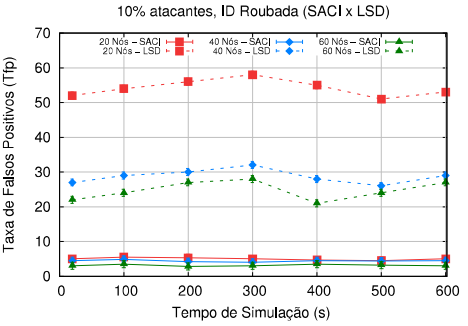
(a) Churn



(b) *Múltiplas Identidades*



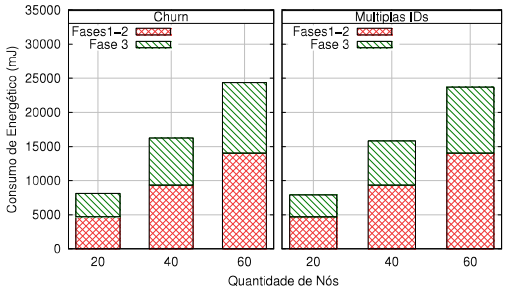
(c) Churn



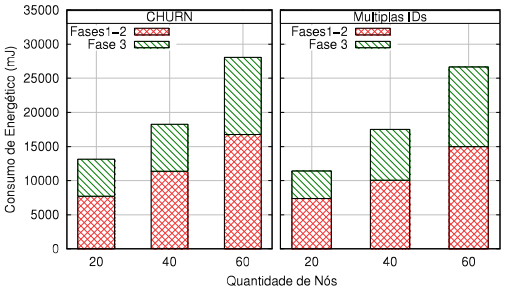
(d) *Múltiplas Identidades*

Figura 8. Comparativo entre os falsos positivos

Os gráficos da Figura 9 mostram o CE do SA^2CI na detecção de ataques Sybil, e compreende o custo da sua inicialização e configuração (fases 1 e 2), e a gerência das associações (fase 3). Percebe-se que os nós com comportamento churn demandam um gasto energético maior, pois o SA^2CI lida com as constantes associações e desassociações de um atacante. Em ambos os tipos de identidades empregadas pelo atacante Sybil, o SA^2CI obteve o mesmo consumo, e isto deve-se porque ele precisa apenas do recibo de identidade para determinar uma associação maliciosa.



(a) Fabricada



(b) *Roubada*

Figura 9. Consumo energético do SA^2CI diante de ataques Sybil

5. Conclusão

Este trabalho apresentou um mecanismo SA^2CI para o controle de associações resistente à ataques Sybil para a disseminação de conteúdo em redes IoT. Ele detecta ataques Sybil de forma escalar, distribuída e adaptativa. Além disso, O SA^2CI leva em conta a heterogeneidade computacional e a irretratabilidade das identidades dos dispositivos. O SA^2CI foi avaliado em um ambiente

doméstico e a sua eficácia foi comparada ao do LSD. As simulações demonstraram que ele previne associações de atacantes com comportamentos maliciosos e de identidades manipuladas em razão das técnicas empregadas. Futuros trabalhos consiste em avaliá-lo em domínios maiores.

Referências

Abbas, S., Merabti, M., Llewellyn-Jones, D., and Kifayat, K. Lightweight sybil attack detection in manets. *Systems Journal, 2013*, páginas:236–248.

Chatzigiannakis, I., Pyrgelis, A., Spirakis, P. G., and Stamatiou, Y. C. Elliptic curve based zero knowledge proofs and their applicability on resource constrained devices. In *8th International Conference on Mobile Adhoc and Sensor Systems (MASS), 2011*, páginas 715–720.

Choden Konigsmark, S., Hwang, L. K., Chen, D., and Wong, M. D. System-of-pufs: Multilevel security for embedded systems. In *Hardware/Software Codesign and System Synthesis (CODES+ ISSS), 2014*, páginas 1–10.

Evangelista, D., dos Santos, A., and Nogueira, M. 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*.

Guicheng, S. and Zhen, Y.. Application of elliptic curve cryptography in node authentication of internet of things. In *Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013*.

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

Mahalle, P. N., Anggorojati, B., Prasad, N. R., and Prasad, R. . Identity establishment and capability based access control (IECAC) scheme for internet of things. In *15th International Symposium on Wireless Personal Multimedia Communications (WPMC), 2012*, páginas 187–191.

Park, S., Aslam, B., Turgut, D., and Zou, C. C. Defense against sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support. *Security and Communication Networks, 2013*, páginas 523–538.

Perera, C., Zaslavsky, A., Christen, P., and Georgakopoulos, D. Sensing as a service model for smart cities supported by internet of things. *Transactions on Emerging Telecommunications Technologies*, páginas 81–93.

Pinol, O. P., Raza, S., Eriksson, J., and Voigt, T. Bsd-based elliptic curve cryptography for the open internet of things. In *7th International Conference New Technologies, Mobility and Security (NTMS), 2015*, páginas 1-5.

Quercia, D. and Hailes, S. Sybil attacks against mobile users: friends and foes to the rescue. In *INFOCOM, 2010*, páginas 1–5.

Vamsi, P. R. and Kant, K. A lightweight sybil attack detection framework for wireless sensor networks. In *Seventh International Conference on Contemporary Computing (IC3), 2014* páginas 387–393.

Wallgren, L., Raza, S., and Voigt, T. Routing attacks and countermeasures in the RPL-based Internet of things. *International Journal of Distributed Sensor Networks, 2013*.

Wu, C.-C., Chang, C.-C., and Lin, I.-C. . New sealed-bid electronic auction with fairness, security and efficiency. *Journal of Computer Science and Technology, 2008*, páginas 253–264.

Zheng, J. X. and Potkonjak, M. 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*, páginas 255–256.

