Controle de Acesso à IoT Baseado na Percepção de Comunidade e Confiança Social Contra Ataques Sybil

Gustavo H. C. de Oliveira[1], **Michele Nogueira**[1], **Aldri Santos**[1]

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

{ghcoliveira, michele, aldri}@inf.ufpr.br

Abstract. *The evolution of IoT has allowed more personal devices to be connected and influenced by habits and behavior of the owners. Hence, these environments demand security for access control against intruders, which may compromise privacy or disrupt of the network operation, such as Sybil attacks. The advent of the Social IoT paradigm allows access control systems to aggregate community context and sociability information of the devices. This work proposes a mechanism, called ELECTRON, for access control in IoT networks based on social trust between devices to protect the network from Sybil attacks. The social similarity between devices helps to define communities in the network and compose the calculation of social trust, strengthening the reliability between legitimate devices and their resilience against the interaction of Sybil attackers. Results in the NS-3 simulator show the ELECTRON effectiveness faces Sybil attacks on IoT that seek access to the network. It achieved detection rates around 90%, and variations according to the community in which social trust is built.*

Resumo. *A evolução da IoT tem permitido que mais dispositivos de uso pessoal estejam conectados, e sejam influenciados pelos hábitos e comportamento dos proprietários. Logo, esses ambientes demandam por segurança no controle do acesso quanto à presença de intrusos, que venham a comprometer a privacidade ou perturbar o funcionamento da rede, como ataques Sybil. O advento do paradigma Social IoT possibilita que sistemas para o controle de acesso possam agregar contexto de comunidade e informações de sociabilidade dos dispositivos. Este trabalho propõe o mecanismo ELECTRON para o controle de acesso em redes IoT baseado na confiança social entre os dispositivos para proteger a rede de ataques Sybil. A similaridade social entre os dispositivos ajuda a definir comunidades na rede e compõem o calculo da confiança social, fortalecendo a confiabilidade entre dispositivos legítimos e sua resiliência contra a interação de atacantes Sybil. Resultados obtidos no simulador NS-3 mostram a eficácia do ELECTRON em identificar ataques Sybil na IoT que buscam acesso à rede. Ele alcançou taxas de detecção por volta de 90%, tendo variações de acordo com a comunidade na qual a confiança social é construída.*

1. Introdução

A Internet das Coisas (IoT) tem ampliado a comunicação entre os dispositivos computacionais e os objetos do nosso cotidiano [Gartner 2017]. Com tantos dispositivos e serviços disponibilizados, as ameaças à segurança se magnificam na mesma proporção da expansão da rede [Sicari et al. 2015]. Entre os serviços potencialmente prejudicados

encontra-se a disseminação de dados, serviço essencial que possibilita o funcionamento de várias aplicações dentro do ecossistema da IoT, como sensoriamento de ambientes e acompanhamento de sinais corporais, entre outros [Evangelista et al. 2016].

A disseminação e o compartilhamento seguro de dados na IoT demandam por um serviço de controle de acesso (CA) eficaz, adaptativo a mudança de contexto e resiliente a ataques que buscam acesso não autorizado a rede. Contudo, os modelos de CAs existentes e oriundos das redes tradicionais não se ajustam completamente para operar em redes IoT [Alaba et al. 2017]. Uma variedade de questões inerentes à IoT como heterogeneidade, mobilidade, restrição de poder de processamento e energia limitam o uso desses modelos de CAs. Tais vulnerabilidades podem ser exploradas por ataques *Sybils*, que comprometem principalmente a privacidade e confiabilidade dos dados disseminados [Pongle and Chavan 2015]. O ataque *Sybil* consiste na personificação de identidades, no qual forjam-se várias identidades em um mesmo dispositivo computacional, na tentativa de se passar por um usuário legítimo. Ao conquistar o acesso, os dados pessoais dos usuários tornam-se disponíveis ao atacante, além do aumento expressivo de mensagens de controle devido ao seu mal comportamento [Medjek et al. 2017].

As técnicas de controle de acesso para redes tradicionais, como RBAC (*Role-Based Access Control*) [Ferraiolo et al. 1995] e ABAC (*Attribute-based Access Control*) [Yuan and Tong 2005, Kuhn et al. 2010], mostram serem inflexíveis (isto é, sem suporte para multiplataforma), difíceis de escalar, e produzem uma grande sobrecarga na rede [Gusmeroli et al. 2012], tornando-os efetivamente inviáveis às demandas das redes IoT. Já as abordagens baseadas em modelos de chave de capacidade, quantificação do risco e no gerenciamento confiança demonstram ser uma alternativa factível para tornar o CA na IoT mais resiliente e adaptativo [Ouaddah et al. 2017]. No modelo de chave de capacidade, uma autoridade certificadora distribui chaves aos dispositivos que solicitam acesso, a fim de determinar o conteúdo e serviços disseminados que o dispositivo pode ter acesso [Hernández-Ramos et al. 2016, Hussein et al. 2017]. Por outro lado, o modelo de quantificação do risco estima as vulnerabilidades e ameaças para cada requisição de acesso, com base em evidências e parâmetros de entrada [Alenezi et al. 2017]. Por fim, o modelo de gerenciamento da confiança estima a confiabilidade de um dispositivo com base em experiências (confiança direta) e recomendações dos vizinhos [Yan et al. 2014].

Embora essas soluções demonstrem avanços na segurança, elas ainda possuem desvantagens como escalabilidade, centralização e falta de especificação; além de se basearem apenas em características de hardware sem estabelecer uma inteligência social. Isso nem sempre reforça a verdadeira interação, isto é, as conexões entre indivíduos construídas no nosso dia-a-dia e, logo, da confiança entre os dispositivos; como ocorre com as relações humanas em suas comunidades, como família, trabalhos, amizades, entre outros. Tais relações possibilitam estabelecer níveis de confiança mais fortes e usá-los para restringir o acesso aos lugares e aos dados privados das pessoas e dispositivos [Abderrahim et al. 2017]. O uso de aspectos subjetivos em um modelo de segurança vai de encontro ao paradigma *Social Internet of Things* (SIoT) [Atzori et al. 2011], que consiste na evolução das associações dos dispositivos baseando-se nas relações humanas para disseminar conteúdo na rede.

Este trabalho apresenta ELECTRON (*acc***E***ss contro***L** *driv***E***n on* **C***ommunity and social* **TR***ust* **O***f thi***N***gs*), um mecanismo para o controle de acesso em redes IoT contra

ataques *Sybil*. ELECTRON é baseado na confiança social entre os dispositivos, a partir da percepção de sociabilidade entre os dispositivos da rede, formam-se *comunidades inteligentes* onde os objetos se agrupam levando em conta suas propriedades sociais como interesses em comum, amizades e tipo de relação SIoT com seus vizinhos. A partir de uma forte similaridade de seus membros, o gerenciamento da confiança é potencializado para identificar dispositivos legítimos e ao mesmo tempo excluir aqueles com comportamento *Sybil*. ELECTRON foi avaliado no simulador NS-3 e os resultados mostram que a confiança dentro das relações possibilita taxas na detecção dos ataques *Sybil*, alcançando na comunidade *Escola* até 93,5% de identificação e exclusão, e 82,4% na comunidade *Residência*, onde a confiança evoluiu com maior facilidade.

O restante do artigo está organizado da seguinte forma: a Seção 2 discute os trabalhos relacionados. A Seção 3 detalha o mecanismo ELECTRON. A Seção 4 mostra a avaliação do ELECTRON e os resultados obtidos. A Seção 5 apresenta as conclusões.

2. Trabalhos Relacionados

O vasto ecossistema de dispositivos conectados da IoT promete entregar diversos serviços, mas sem adequada proteção, eles podem levar a quebra de privacidade e integridade dos dados [Greengard 2019]. O serviço de controle de acesso (CA) aumenta a segurança, e algumas soluções propostas baseiam-se em (i) capacidade (*Capability*) - CapBAC, (ii) risco (*Risk*) - RiskBAC e (iii) confiança (*Trust*) - TBAC. Tais abordagens se adéquam ao ambiente com restrição e heterogeneidade da IoT, principalmente pela sua dinamicidade e menor demanda de recurso. A abordagem CapBAC emprega uma chave que informa os privilégios de acesso do dispositivo dentro da rede, através de uma autoridade certificadora. Para adicionar escalabilidade e flexilidade na abordagem, [Anggorojati et al. 2012] incorporaram informação do contexto no CA, criando o CCAAC (*Capability based Context Aware Access Control*). Já [Hernández-Ramos et al. 2016] apresentaram DCapBAC (*Distributed Capability-based Access Control Approach*), que baseia-se na capacidade distribuída através da uma otimização da criptografia de curva elíptica (ECC), agregando vantagens como escalabilidade, interoperabilidade e segurança fim-a-fim. Entretanto, a falta de detalhes sobre o processo de inicialização do CA e na geração de chaves de acesso dificulta uma análise do real impacto da abordagem na rede. Além da necessidade de confiança entre os domínios e as entidades de autenticação e assinatura.

Uma estrutura baseada em comunidades foi incorporada no *framework* COCapBAC (*Community capability-based access control*) para definir a noção de direito de acesso em um ambiente distribuído [Hussein et al. 2017]. Neste trabalho, no entanto, o conceito de comunidade não está relacionado ao paradigma SIoT, e as comunidades surgem entre objetos inteligentes que compartilham as mesmas missões. Assim, as normas da comunidade embasam a concessão de direitos de acesso na rede, onde dispositivos com maior capacidade de recurso tomam a decisão de acesso em prol de dispositivos com restrição de recursos. Entretanto, num ambiente dinâmico, isto é, onde os dispositivos possuem alta mobilidade, áreas de atuação cada vez maiores e intensa relações sociais, o conceito de comunidade no COCapBAC possui desvantagens; tal como a falta de autonomia dos objetos em usar as características da comunidade como a similaridade para uma avaliação segura e individual do acesso. Além disso, não são descritos como os aspectos influenciam na criação de novas chaves de acesso.

As abordagens de CA baseadas em RiskBAC podem ser classificadas em modelos adaptativos e não adaptativos. Os modelos adaptativos atualizam em tempo real as informações dos aspectos para o cálculo do risco, já os não adaptativos calculam o risco apenas em sua inicialização. [Alenezi et al. 2017] propõem um modelo de CA adaptativo baseado na quantificação do risco para IoT, chamado AdRBAC (*Adaptive Risk-Based Access Control*). Nele, fatores como contexto (lugar e horário), sensibilidade aos recursos, gravidade da ação e histórico compõem a estimativa de risco de cada requisição. Embora não possua uma implementação e uma avaliação, AdRBAC considera esses fatores importantes para um ambiente heterogêneo e de alta mobilidade. Contudo, aspectos sociais dos dispositivos são desconsiderados, deixando AdRBAC em desvantagem em ambientes onde os nós se relacionam entre si.

A confiança é um conceito extensivamente discutido na IoT, principalmente por ser considerada um fator chave para alcançar mais segurança na rede [Gu et al. 2014, Chen et al. 2014, Nguyen et al. 2016, Sato et al. 2016, Khan and Herrmann 2017]. A abordagem TBAC começou a ser defendida em [Mahalle et al. 2013] com o *framework* FTBAC, onde valores de experiência (EX), conhecimento (KN) e recomendações (RC) são calculados e uma estrutura de decisão baseada em lógica Fuzzy controla o acesso. Mais tarde, [Bernal Bernabe et al. 2016] trouxe a sociabilidade ao TBAC com o modelo TACIoT. O modelo estabelece um controle de acesso à IoT multidimensional confiável com o objetivo de ser leve, flexível e adaptativo. O trabalho explora um ambiente onde os dispositivos se agrupam em bolhas (*bubbles*), formadas de acordo com os relacionamentos. A partir de quatro dimensões de avaliação: QoS (*Quality of Service*), segurança, reputação e relações sociais. As informações coletadas de cada dimensão estabelecem um valor final da confiança, e um verificador Fuzzy auxilia na tomada de decisão. Dentro do aspecto social, considera-se as propriedades como interesses em comum e amigos na avaliação. Contudo, o trabalho deixa vago como ocorre a construção dessas comunidades entre os objetos, e qual é relação do interesse em comum e amizade para a avaliação.

3. Controle de Acesso Contra Ataques Sybil

Esta seção detalha o mecanismo ELECTRON para apoiar o serviço de CA à IoT, que é baseado na confiança entre os dispositivos dentro de uma rede SIoT. ELECTRON atua como um *middleware* no auxílio da segurança na disseminação e no compartilhamento de dados contra ataques de personificação, como os ataques *Sybil*. Inicialmente, são descritos o modelo da rede IoT e o comportamento dos ataques Sybil. Em seguida, são detalhados a arquitetura ELECTRON e modo de operação.

Assume-se uma topologia de rede composta por partes estruturadas e não estruturadas onde os dispositivos (nós) cooperam no encaminhamento dos dados. A rede possui nós heterogêneos e com mobilidade aleatória. O conjunto $N = \{n_1, n_2, ..., n_n\}$ representa todos os nós da rede num dado momento t, tal que eles pertencem à N_{man} ou N_{sub}, onde N_{man} e $N_{sub} \subseteq N$, $N_{man} \cup N_{sub} = N$. Os nós N_{man} formam uma rede lógica distribuída, que trocam informações sobre o gerenciamento da confiança e relações sociais. Esta organização fornece escalabilidade à rede, ao dividir o gerenciamento da confiança social entre os nós no conjunto N_{man}, além de aumentar a capacidade de gestão apenas ao incluir novos objetos na função de gerenciamento. Já os nós em N_{sub} caracterizam-se pelas restrições de recursos computacionais, como processamento, armazenamento e energia; e assim eles estão subordinados aos nós N_{man}.

O comportamento do ataque Sybil consiste no uso de identidades roubadas (Id_r) ou fabricadas (Id_f), pelo atacante externo a rede, a fim de conquistar o acesso à rede. As Id_r compreendem identidades roubadas de nós legítimos pelo nó atacante, já as Id_f são identidades fabricadas e, portanto, sem nenhuma associação com outros dispositivos da rede. Além disso, o comportamento dos nós Sybil pode variar de *churn* para múltiplas identidades (*MI*), como ilustra a Figura 1. No comportamento *churn* o nó possui apenas uma identidade, porém tenta várias associações com diferentes nós em um curto espaço de tempo. Já no comportamento *MI*, o nó possui várias identidades e uma movimentação menor, usando suas identidades para forçar a associação.

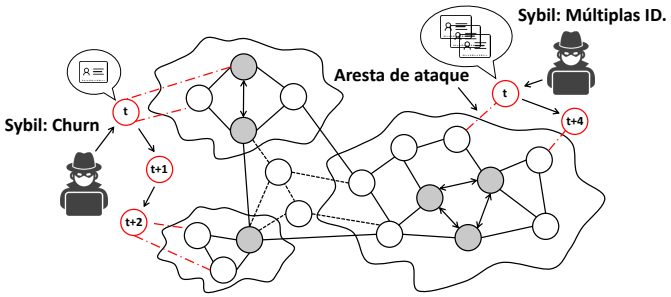

Figura 1. Comportamentos dos atacantes Sybil

3.1. Arquitetura do Sistema ELECTRON

O mecanismo ELECTRON divide-se em cinco partes chamadas de módulos: **social**, **confiança**, **contexto**, **experiência** e **autenticação**, como ilustrado na Figura 2. A maior parte dos módulos do mecanismo atua nos dispositivos pertencentes ao conjunto N_{man}, restando apenas certas funcionalidades dos módulos **social** e **confiança** aos nós N_{sub}, encaminhando as informações de suas relações sociais e experiências com os vizinhos para o nó N_{man} mais próximo. Desta forma, a heterogeneidade da rede pode ser satisfeita ao não atribuir tarefas complexas, como o cálculo da confiança e o gerenciamento das relações sociais, aos dispositivos do conjunto N_{sub} com restrição de recursos. Por fim, o nó N_{man} processa as informações e decide quanto ao acesso à rede, economizando recursos dos nós N_{sub}. A seguir, é descrita a operação de cada módulo.

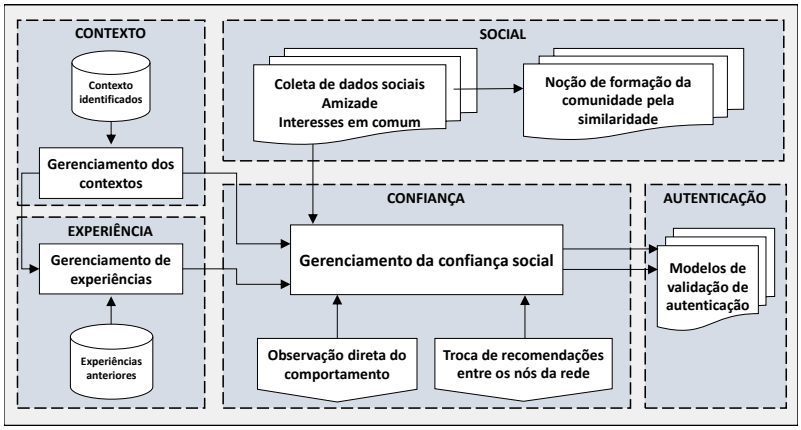

Figura 2. Arquitetura do ELECTRON

3.1.1. Módulo Social

O módulo social compreende todas as funções referentes aos relacionamentos dos nós até a noção de comunidade dentro do mecanismo, envolvendo a similaridade entre os dispositivos. O módulo armazena as relações de amizades e interesses em comum

construídas pelo nó N_{man}, como também as relações dos nós N_{sub} subordinados. Essas informações compõem o cálculo da confiança e contribuem no valor da similaridade entres os nós na comunidade. As comunidades "especiais" (denominadas comunidades inteligentes) têm um papel importante no comportamento social dos objetos porque elas refletem o contexto atual dos dispositivos. As comunidades são representadas através de um grafos de similaridade G, onde $V(G)$ representa o conjunto de vértices do grafo e $A(G)$ o conjunto de arestas indicando alta similaridade entre dois vértices, tal que $ij \in A(G) \Leftrightarrow S(i,j) > Similarity_{threshold}$. Denota-se a comunidade da seguinte forma:

$$\mathcal{C} = \forall i,j \in V(G) \mid S(i,j) > Similarity_{threshold} \tag{1}$$

$$S(i,j) = Sim^{A}(i,j) * \varphi_A + Sim^{CI}(i,j) * \varphi_{CI} \tag{2}$$

Onde $S(i,j)$ representa uma função para calcular a similaridade no conjunto de vértices que pertencem a comunidade $\mathcal{C}$, tal que sua similaridade seja maior que o limite $Similarity_{threshold}$. Isto indica que há uma forte similaridade entre tais vértices, e, assim, uma comunidade. A Figura 3 ilustra uma rede SIoT composta por nós N_{man} e N_{sub}, cinza e branco, respectivamente, onde há três comunidades sociais diferentes a partir da similaridade. Nelas alguns nós já possuem conexões estabelecidas - links direcionados para comunicação entre N_{man} e links não direcionados para demais comunicações, em outras estão estabelecendo as conexões - links tracejados.

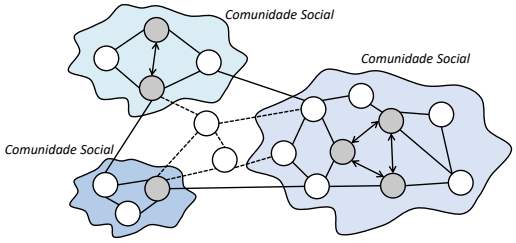

Figura 3. Estrutura das comunidades em uma rede SIoT

A tupla $<Sim^{A}, Sim^{CI}>$ representa a similaridade das informações sociais dos dispositivos, correspondendo respectivamente ao conjunto de amizades (A) e aos interesses em comum (CI). Denota-se φ o peso para cada conjunto, sendo que $\varphi_A + \varphi_{CI} = 1$. As métricas são obtidas a partir do coeficiente de similaridade de Jaccard [Abderrahim et al. 2017], onde **Conjunto de Amizades** (A): denota a relação social capaz de afetar recomendações e está ligada a intimidade entre as entidades, obtida pela Eq. 3a, onde A_i e A_j são as listas de amigos de i e j; **Conjunto de Interesse em Comum** (CI): denota usuários de uma comunidade que compartilham interesses similares. Logo, eles são mais prováveis a ter conhecimentos e padrões comuns a um serviço provido pelo mesmo dispositivo. Ela é obtida pela Eq. 3b, onde CI_i e CI_j são listas de interesses em comum dos dispositivos i e j.

$$Sim^{A}(i,j) = \frac{|A_i \cap A_j|}{|A_i \cup A_j|}, \tag{3a}$$

$$Sim^{CI}(i,j) = \frac{|CI_i \cap CI_j|}{|CI_i \cup CI_j|} \tag{3b}$$

As relações na SIoT são classificadas em cinco formas: ROP, ROPR, ROL, ROT, e RSO [Atzori et al. 2011]. A primeira é a **Relação de Objeto Parental** (ROP), criada

entre objetos similares produzidos no mesmo período e pelo mesmo fabricante, estabelecendo relações homogêneas. A **Relação de Objetos de Propriedade** (ROPR) envolve objetos pertencentes ao mesmo dono, essa relação se institui entre objetos heterogêneos, tais como celulares, computadores ou consoles de jogos. Os objetos também podem estabelecer **Relação de Objeto por Localização** (ROL) e **Relação de Objeto para Trabalho** (ROT). Na ROL, as relações possuem a característica de serem homogêneas ou heterogêneas e se estabelecem entre objetos presentes em uma mesma localização. Já na ROT, objetos formam uma relação a fim de cooperarem para uma aplicação em comum na IoT, como um serviço de emergência. Devido as suas características, as relações ROL e ROT podem ser criadas pelos mesmos dispositivos cooperando para uma aplicação IoT em uma localidade fixa. Por fim, a **Relação Social dos Objetos** (RSO) inicia entre objetos que entram em contato, seja esporadicamente ou continuamente, por razões unicamente ligadas aos relacionamentos entre seus donos [Atzori et al. 2012]. Assim como os humanos trocam contatos (telefone, e-mail, etc.), os objetos nesta relação trocam dados sobre seu perfil social. A ideia consiste que os objetos de características similares compartilhem boas práticas para resolver problemas comuns para seus "amigos". Essas informações contextualizam as relações sociais que são aplicadas no módulo confiança (Seção 3.1.3), ponderando as recomendações dos vizinhos.

3.1.2. Módulo Contexto e Experiência

O gerenciador de contexto identifica e retorna o contexto atual do dispositivo. Informações como posição atual e tipos de dispositivos próximos podem ser adquiridas por um nó da rede. Essas informações formam o que denomina-se de "contexto". Logo, um gerenciador que receba informações e identifique o contexto atual se faz necessário para uma maior acurácia na avaliação. Este módulo reflete uma lista detalhada sobre as localizações onde o dispositivo esteve, isto é, lugares e tipos de dispositivos envolvidos. Conforme o contexto atual do dispositivo a base para o cálculo da confiança pode alterar, propiciando uma melhor ou pior convergência da confiança conforme seu valor.

O gerenciador de experiências armazena as experiências ruins, em relação a serviços prestados por vizinhos. Portanto, o gerenciador de experiência mantém uma relação com o contexto, pois as más experiências serão relacionadas ao contexto atual. Nesse módulo, são feitas associações entre experiências ruins e o contexto nas quais estas ocorreram. Para que em futuras situações semelhantes, o valor da confiança seja menor.

3.1.3. Módulo Confiança

A tomada de decisão por um controle de acesso demanda parâmetros de modo a permitir ou negar o acesso a um dado dispositivo. O ELECTRON baseia-se em um modelo de confiança que coleta informações a sua volta para a tomada de decisões. Embora o uso de confiança no contexto IoT não seja novo, neste trabalho, alia-se a confiança com um forte contexto social dos objetos. A finalidade é que a sociabilidade apoie na obtenção de valores mais precisos sobre o comportamento dos dispositivos. Adaptou-se, assim, a Lógica Subjetiva (LS) [Jøsang 2016], Eq 4a, onde os parâmetros da confiança são influenciados por fatores como similaridade e tipo de relacionamento.

$$T_{ij}^{\mathcal{C}} = \alpha D_{ij} + \beta S_{ij}^{\mathcal{C}} + \gamma R_{ij} \quad (4a) \qquad D_{ij} = b + d + u \quad (4b) \qquad R_{ij} = b + d + u \quad (4c)$$

Confiança Direta (D_{ij}), obtida pela Eq. 4b, trata das próprias experiências do dispositivo com os seus vizinhos e reflete o resultado das interações entre o nó i com o nó j. Representa o valor mais importante dentro da confiança, pois demonstra os resultados das escolhas do dispositivo. **Similaridade com a comunidade** ($S_{ij}^{\mathcal{C}}$) indica quanto um dispositivo j assemelha-se aos dispositivos pertencentes a comunidade $\mathcal{C}$. Através da similaridade computada pela Eq 2, essa propriedade influencia a confiança com fatores como interesse em comum e amizade, tal que esses fatores sociais melhorem a acurácia na construção da confiança. **Recomendação** (R_{ij}) trata da confiança de outros nós em relação ao nó j. Essa opinião é compartilhada entre os nós da comunidade, para então contribuir na construção da confiança geral de cada nó. Obtida pela Eq. 4c, a recomendação não sofre nenhuma alteração social para sua computação.

Todavia, as recomendações precisão ser medidas de acordo com a relação social estabelecida entre o recomendante e o requerente. Logo, estabeleceu-se valores para cada tipo de relação conforme a Tabela 1 [Abderrahim et al. 2017]. Tais valores constituem um *fator de relacionamento*, dentro da composição da confiança geral - denotada na Eq. 4a - onde somam-se a confiança direta (D_{ij}) e as recomendações (R_{ij}) dos vizinhos de i para obter-se a confiança geral ($T_{ij}^{\mathcal{C}}$) em relação ao nó j. Sendo que γ significa o fator de relacionamento ponderando as recomendações. Essa abordagem objetiva filtrar, por meio das relações sociais, as recomendações mais importantes à confiança.

Tabela 1. Fatores de relacionamentos

Relação dos objetos	ROPR	ROL	ROT	RSO	ROP
γ	0,3	0,2	0,2	0,1	0,1

O uso de Lógica Subjetiva (LS) tem sido visto em trabalhos focados na IoT [Son et al. 2017] [Khan and Herrmann 2017], gerenciando a confiança em forma de opiniões sobre outros dispositivos na rede. Nela, forma-se um triângulo de opiniões com três variáveis, crença (*b*), descrença (*d*) e incerteza (*u*), sendo $b + d + u = 1, \{b, d, u\} \in [0, 1]^3$ [Jøsang 2016] e os valores de (b, d, u) obtidos pela Eq. 5. A opinião na LS computa experiências positivas e negativas com o dispositivo em questão. O modelo da LS utilizado neste trabalho constitui de uma 4-tupla (b,d,u,a) onde $(b + d + u) = 1.0$ e $a = [0..1]$, com a confiança em uma opinião expressa pelo valor esperado $b + u * a$.

$$b = \frac{pos}{(pos + neg + 2.0)} \quad d = \frac{neg}{(pos + neg + 2.0)} \quad u = \frac{2.0}{(pos + neg + 2.0)} \tag{5}$$

Nas equações acima, o número de experiências positivas e negativas é expresso por pos e neg, respectivamente, enquanto a representa uma taxa base para a convergência da confiança. Neste trabalho a valor de a é definido pelo gerenciador de contexto, estipulando valores próximos de 1 para contextos mais seguros, como residências, e valores próximos de 0 para contexto menos seguros como o ambiente aberto de um parque.

3.1.4. Módulo Autenticação

O módulo para autenticação toma a decisão de acesso ou não do dispositivo dentro do ELECTRON. Para isso, recebe as informações do gerenciador da confiança e as emprega para tomar a decisão de acesso. A inteligência definida neste trabalho para a tomada de decisão baseia-se, inicialmente, no valor calculado para confiança. Sendo ele

acima de um *limite* (definido como 0,6) o acesso é concedido aos serviços e aplicações disponíveis na rede. Porém, a inteligência para tomada de decisão pode ser ainda melhorada, no qual outras técnicas com maior fundamentação para tomar decisões, como por exemplo a lógica Fuzzy, podem ser incorporadas nesse módulo.

4. Avaliação

Esta seção apresenta uma avaliação do mecanismo ELECTRON com o objetivo de mostrar a sua eficácia para detectar ataques Sybil atuando sobre ambientes IoT. O ELECTRON foi implementado no simulador NS-3 versão 3.27. Os ataques Sybil implementados empregam identidades fabricadas e roubadas, e possuem os comportamentos *churn* e de múltiplas identidades. O cenário avaliado leva em conta o conjunto de dados (*Dataset*) da rede social *Brightkite* baseada em localização. Nele, os usuários compartilham com amigos suas localizações através de *checking-in*, em áreas como a cidade de São Francisco (EUA). Os ambientes no *dataset* diferem-se entre residências, escritórios até locais de lazer e estão disponíveis em [Cho et al. 2011]. A rede de amizade consiste de 58,228 nós e 214,078 arestas com as informações coletadas entre abril de 2008 e outubro de 2010, sendo que cada aresta representa um laço de amizade. As informações de amizade foram implementadas nos dispositivos IoT dentro da simulação a fim de criar um cenário social mais realístico. Também estabeleceu-se cinco comunidades que representam ambientes como *casa*, *escola*, *escritório*, *academia* e *parque*. Para a tupla (b, d, u, a) correspondente a opinião do vizinho (Seção 3.1.3), definiu-se o valor de a segundo um nível empírico de segurança, iniciando com o valor 1 para os ambientes mais seguros, como o ambiente doméstico, e tendendo à 0 nos contextos menos seguros, tais como os ambientes abertos.

Tabela 2. Métricas de avaliação

Métrica	Fórmula
Taxa de detecção (R_d) contabiliza os ataques Sybil identificados corretamente pelo ELECTRON a partir da confiança social. O cálculo da R_d corresponde a razão entre o total de detecções, det_{ni}, e quantidade de ataques, T_{atq}. Esta métrica apresenta valores que variam entre 0% e 100%, onde quanto mais próximo dos 100% chegar a mensuração maior será a eficácia do mecanismo.	$R_d = \frac{\sum det_{ni}}{Tatq}$
Acurácia R_a, indica a precisão da detecção do ELECTRON. Esta métrica corresponde ao total de detecção do ataque Sybil, det_{ni}, a identificação correta dos nós legítimos da rede, det_{na}, dividido pelo total de requisições feitas à rede, T_{req}. A R_a também resulta em valores discretos entre 0 e 1, quando mais perto de 1 melhor a acurácia.	$R_a = \frac{\sum det_{ni} + \sum det_{na}}{Treq}$
Taxa de falsos positivos T_{fp} determina a quantidade de vezes que o ELECTRON identificou um ataque Sybil quando não existia o ataque. O seu cálculo acontece através da divisão entre o número de *Falsos Positivos* pela soma dos *Falsos Positivos* e *Verdadeiro Negativo* (nós legítimos classificados como legítimos).	$R_{fn} = \frac{FalseNeg}{FalseNeg + TruePos}$
Taxa de falsos negativos (R_{fn}) determina a quantidade de vezes que o ELECTRON classificou um nó atacante como legítimo. O seu calculo acontece através da divisão entre o número de *Falsos Negativos* pela soma dos *Falsos Negativos* e *Verdadeiros Positivos* (nós legítimos identificados corretamente).	$R_{fp} = \frac{FalsePos}{FalsePos + TrueNeg}$

O meio de transmissão baseia-se no padrão IEEE 802.15.4, utilizado por dispositivos dentro de uma rede 6LowPAN. Os dispositivos disseminam informações de uma origem para um destino com o propósito de simular uma aplicação em tempo real dentro de um ambiente IoT. Este fluxo de dados se caracteriza com mensagens de 127 *bytes*, isto é, *payload* e cabeçalhos que seguem o padrão 6LowPAN. Os atacantes requisitam acesso a rede através do uso de identidades roubadas ou fabricadas, com comportamento *churn* ou exibindo múltiplas identidades. Entre outros parâmetros de configuração estão a área total de $100m$x$100m$, no qual os nós se movem uma uma velocidade de $2m/s$ seguindo o modelo de mobilidade *Random Waypoint* do NS-3. Os nós utilizam o protocolo UDP para a comunicação e o total de nós nas simulações variou entre 100, 150 e 200. Os valores de a foram definidos como 1, 0,7, 0,5, 0,4 e 0,2 respectivamente para as comunidades residência, escritório, escola, academia e parque. Em cada simulação um total de 10% de atacantes busca acesso à rede, em um tempo total de $600s$ de simulação. As métricas aplicadas na simulação são descritas na Tabela 2. Por motivos de espaço, apenas os resultados da simulação com 150 nós são mostrados, onde houve uma maior variação na detecção, permitindo uma melhor análise de desempenho. Contudo, os resultados com 100 e 200 nós obtiveram comportamentos próximos e estão disponíveis no site[1].

4.1. Análise da Detecção dos Ataques

Na análise da eficácia do ELECTRON na presença de atacantes Sybil, as Figuras 4 e 5 mostram a taxa de detecção (R_d), a acurácia (R_a), a taxa de falsos negativos (R_{fn}) e a taxa de falsos positivos (R_{fp}). Na Figura 4 observa-se os gráficos das taxas de detecção (R_d) obtidos ao longo da simulação, onde arbitrariamente o atacante assumia um dos quatro comportamento Sybil, distribuídos dentro o total de 10% de atacantes. Assim, cada gráfico apresenta apenas a R_d de um comportamento. Inicialmente, as taxas de detecção estão muito próximas de 100%, mas no momento seguinte as taxas apresentam uma queda sendo elas mais bruscas em algumas comunidades. Isso acontece porque alguns atacantes foram implementados para terem um comportamento legítimo e tentar enganar o mecanismo. Considerando que o motor de detecção é baseado em confiança e sociabilidade, uma desvantagem para o mecanismo é o atacante alterar seu comportamento. Percebe-se uma maior alteração nas comunidades escritório e ainda mais brusca na residência, justamente onde a taxa base (a) para cálculo da confiança é maior. Indicando que uma taxa base maior não significa maior detecção, e que essas comunidades são mais sensíveis aos ataques, precisamente por convergir a confiança mais facilmente. Apesar de apresentar essa queda, o mecanismo se recupera e volta a apresentar taxas entre 79,6% e 90,6%. Outro ponto importante é a pequena diferença entre os ataques com identidades roubadas e fabricadas. Ao identificar uma identidade fabricada o mecanismo deduz a confiança do nó avaliado, porém sua avaliação se baseia na confiança conquistada, o que expressa-se na pequena diferença entre as abordagens.

Os gráficos da Figura 5 apresentam as taxas R_a, R_{fn} e R_{fp}, considerando todos os comportamentos dos atacantes juntos. O primeira gráfico mostra a R_a na qual segue a tendência da R_d, obtendo uma maior acurácia conforme a confiança social estabiliza. A seguir, o gráfico com os valores de taxa de falsos negativos (R_{fn}) obtidos na detecção do mecanismo ELECTRON, ou seja, o valor de atacantes classificados como nós legítimo da rede, e por isso não taxados como ameaça. Inicialmente, observa-se valores

[1] http://www.nr2.ufpr.br/~oliveira/electron-results.html

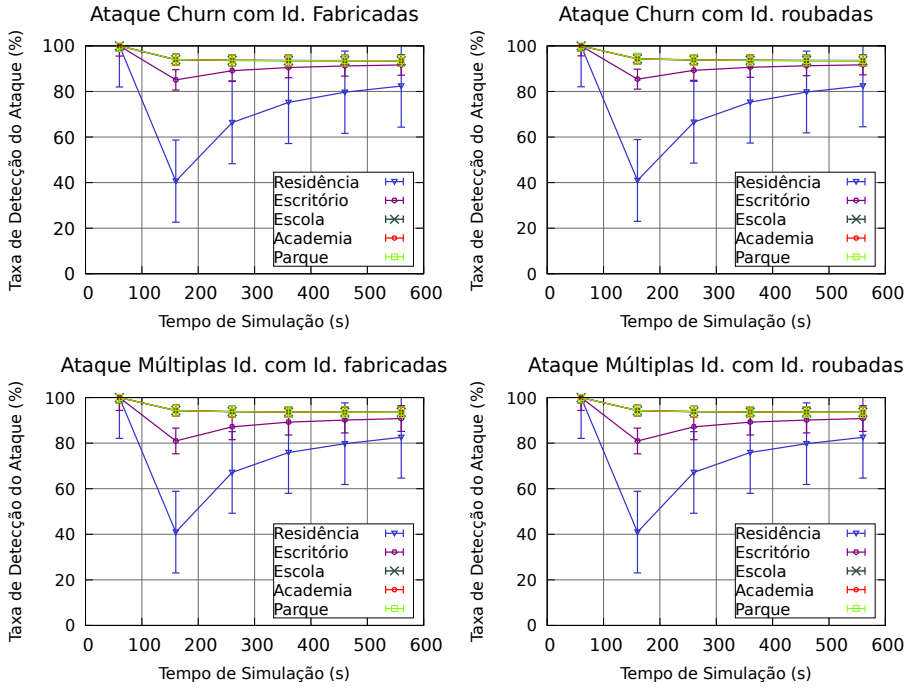

Figura 4. Taxa de detecção por comportamento dos atacantes

altos, principalmente na comunidade residência, mostrando que houve problemas para identificar os atacantes no início da simulação. A medida que o valor da confiança social foi se ajustando aos dispositivos, houve uma melhora na identificação dos atacantes. Encaminhando-se no fim para taxas menores que 20% para residência e menores que 10% para as demais comunidades.

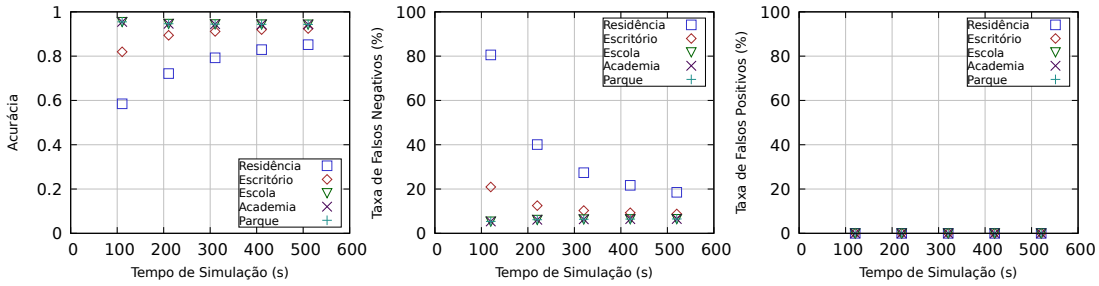

Figura 5. Acurácia, Taxa de Falsos Negativos, e Taxa de Falsos Positivos

A Figura 5 também apresenta o gráfico da taxa de falsos positivos (R_{fp}), ou seja, os nós legítimos classificados como atacantes. Nota-se que não houve a ocorrência de falsos positivos junto ao mecanismo. Isso demonstra que o mecanismo consegue manter níveis estáveis de identificação de nós legítimos. Porém, será feito um estudo com outras tecnologias de transmissão e controle de canal, onde maiores taxas de colisão e perda de pacotes se aplicam, a fim de verificar como eles impactam na precisão da R_{fp}.

4.2. Análise das Relações Sociais na Confiança das Comunidades

Nós avaliamos como a confiança social estabelecida entre os dispositivos evolui ao longo da simulação. Os valores da confiança foram separados por tipo de relação para

uma melhor análise da sua evolução, ao considerar que o tipo de relação influencia diretamente nas recomendações fornecidas pelos vizinhos. Os gráficos na Figura 6 mostram também como a confiança social converge diferentemente em cada comunidade, representando contextos diferentes. Eles contêm o valor da confiança social em uma função de distribuição acumulativa (CDF). Para cada tipo comunidade há dois gráficos, onde o gráfico superior mostra a evolução da confiança entre os nós internos à rede e o gráfico inferior a confiança dos nós internos em relação aos nós externos, que fazem a requisição de acesso. Os resultados mostram que a confiança obtida na relação parental (com menos importância nas recomendações) tem pior desempenho entre os nós internos. Isto deve-se ao peso atribuído na Tabela 1, o que já era esperado. No entanto, seu comportamento vária entre os nós externos, alcançando valores mais altos na comunidade residência e valores mais baixos na comunidade academia. Esse comportamento acontece pela influência dos atacantes estabelecendo diferentes relações com os nós internos, onde observa-se que em cada comunidade diferentes relações obtiveram melhores resultados.

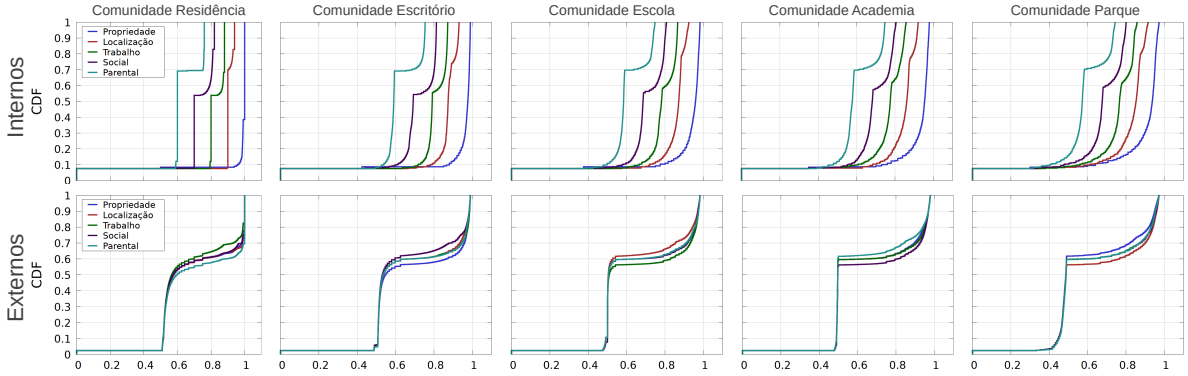

Figura 6. Evolução da confiança social em diferentes comunidades e relações

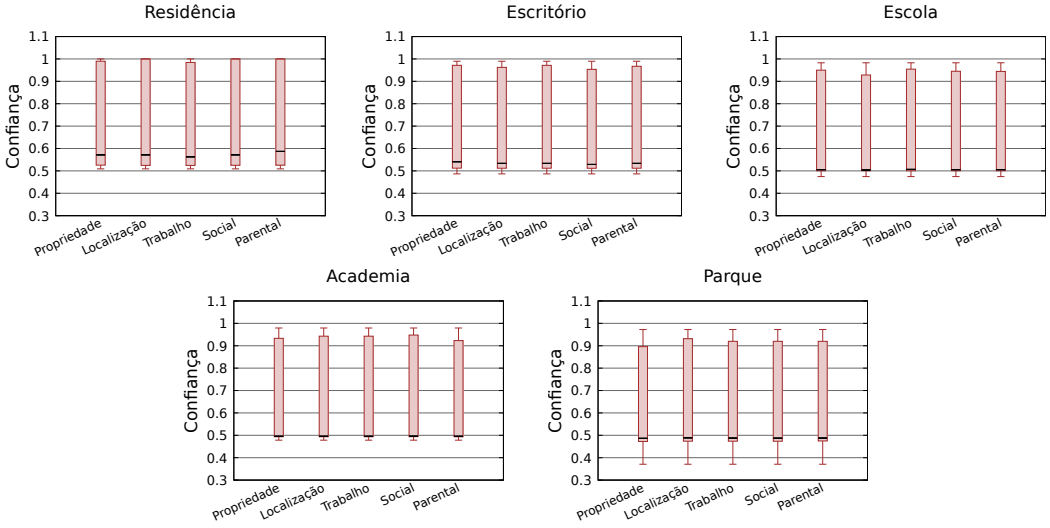

Figura 7. Dispersão da confiança social dos nós externos

Os gráficos da Figura 7 apresentam as informações da confiança social no formato *boxplot*. Os valores correspondem apenas as medições do comportamento do ELECTRON nos nós internos referentes aos nós que requisitam acesso à rede. Percebe-se em

todos gráficos que os valores da confiança entre as comunidades não possuem expressivas diferenças, mostrando que o valor de a para cada comunidade não representa grande peso no valor final da confiança. Contudo, o valor de a tem maior influência na curvatura da CDF do que na dispersão final dos dados. Além disso, nos gráficos a mediana da confiança em todas as comunidades concentra-se abaixo de 0,6, variando entre 0,5 e 0,6. Isso deve-se a distribuição dos nós na simulação, como internos, candidatos legítimos ao acesso, e atacantes; sendo o número de atacantes maior do que o de nós candidatos legítimos.

5. Conclusões

Este trabalho apresentou o mecanismo ELECTRON para o controle de acesso em rede IoT contra ataques Sybil. Ele leva em conta a sociabilização dos dispositivos ao longo do tempo e propõem uma percepção de comunidade conforme a similaridade entre os dispositivos ao analisar aspectos sociais como amizades e interesses, a fim de impedir que atacantes obtenham acesso aos dados. Ao unir o gerenciamento da confiança, através da lógica subjetiva, e as relações sociais criadas pela SIoT, buscou-se reforçar a precisão da confiança na tomada de decisão sobre os atacantes. As simulações mostraram a eficácia do ELECTRON em diversos ambientes, onde acalçou-se taxas entre 90%, entre as comunidades *Escola*, *Academia* e *Parque*, a 80% para as comunidades *Escritório* e *Residência*, com ganhos de 0,82 a 0,96 na acurácia ao barrar atacantes. Como trabalhos futuros estão o emprego do ELECTRON em um cenário com maiores colisões e perda de pacotes, aplicar técnicas, como lógica Fuzzy, para melhorar a tomada de decisão no módulo Autenticação, assim como associar ELECTRON com técnicas de *hardware*.

Referências

Abderrahim, O. B., Elhedhili, M. H., and Saidane, L. (2017). Ctms-siot: A context-based trust management system for the social internet of things. In *3th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 1903–1908.

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

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

Anggorojati, B., Mahalle, P. N., Prasad, N. R., and Prasad, R. (2012). Capability-based access control delegation model on the federated iot network. In *The 15th International Symposium on Wireless Personal Multimedia Communications*, pages 604–608.

Atzori, L., Iera, A., and Morabito, G. (2011). Siot: Giving a social structure to the internet of things. *IEEE Communications Letters*, 15(11):1193–1195.

Atzori, L., Iera, A., Morabito, G., and Nitti, M. (2012). The social internet of things (SIoT) - When social networks meet the internet of things: Concept, architecture and network characterization. *Computer Networks*, 56(16):3594–3608.

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

Chen, I. R., Guo, J., and Bao, F. (2014). Trust management for service composition in soa-based iot systems. In *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 3444–3449.

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

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

Ferraiolo, D. F., Cugini, J. a., and Kuhn, D. R. (1995). Role-Based Access Control: Features and Motivations. *Proceedings of the 11th Annual Computer Security Applications Conference*, (JANUARY 1995):241–248.

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

Greengard, S. (2019). Deep insecurities: The internet of things shifts technology risk. *Commun. ACM*, 62(5):20–22.

Gu, L., Wang, J., and Sun, B. (2014). Trust management mechanism for internet of things. *China Communications*, 11(2):148–156.

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

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

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

Jøsang, A. (2016). *Subjective logic*, pages XXI, 337. Springer International Publishing.

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

Kuhn, D. R., Coyne, E. J., and Weil, T. R. (2010). Adding attributes to role-based access control. *Computer*, 43(6):79–81.

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

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

Nguyen, T., Hoang, D., and Seneviratne, A. (2016). Challenge-response trust assessment model for personal space iot. In *IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pages 1–6.

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

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

Sato, H., Kanai, A., Tanimoto, S., and Kobayashi, T. (2016). Establishing trust in the emerging era of iot. In *IEEE Symposium on Service-Oriented System Engineering (SOSE)*, pages 398–406.

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

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

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

Yuan, E. and Tong, J. (2005). Attributed based access control (abac) for web services. In *IEEE International Conference on Web Services (ICWS'05)*, page 569.