Avaliação das Técnicas de Detecção do Ataque Sybil na Disseminação de Conteúdo da Internet das Coisas

Danilo Evangelista, Michele Nogueira, Aldri Santos[1]

[1]Núcleo de Redes Sem-Fio e Redes Avançadas (NR2) – UFPR
Caixa Postal 19.081 – 81.531.980 – Curitiba – PR – Brasil

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

Abstract. *The Internet of Things (IoT) comprises a diversity of heterogeneous objects.They act in these networks collecting continuous and discrete data and disseminating this information to applications thus providing a welfare for people. The data dissemination service in the IoT uses the wireless medium that is unsafe. Thus, this service can be tampered by various types of attackers such as blackhole, sinkhole and the Sybil. Among these, the Sybil attack emerged as the most critical since it operates in the confidentiality of this data. Although the solutions found in the literature are effective against Sybil attack, they disregard the presence of heterogeneous devices or have complex solutions. This paper presents a study on the efficiency and effectiveness of attack detection techniques. Thus, this evaluation uses metrics of effectiveness and efficiency in order to assess the performance of an engine with characteristics closer the IoT.*

Resumo. *A Internet das coisas (IoT) compreende uma diversidade de objetos heterogêneos. Eles atuam nestas redes coletando dados contínuos e discretos e disseminando estas informações para aplicações provendo assim um maior bem estar para as pessoas. O serviço de disseminação de dados na IoT utiliza o meio sem fio que é inseguro. Assim, este serviço pode ser prejudicado por diversos tipos de atacantes como o blackhole, sinkhole e o Sybil. Dentre esses, o ataque Sybil desponta como o mais crítico visto que ele atua na confidencialidade destes dados. Embora as soluções encontradas na literatura sejam eficazes contra o ataque Sybil, elas desconsideram a presença de dispositivos heterogêneos ou apresentam soluções complexas. Desta forma, este trabalho apresenta um estudo sobre a efetividade e eficiência das técnicas de detecção do ataque Sybil. Desta forma, esta avaliação usa métricas de eficácia e eficiência a fim de aferir a performance de um mecanismo com características próximas da IoT.*

1. Introdução

O conceito de Internet das Coisas (IoT, do Inglês *Internet of Things*) consiste em uma rede híbrida, aberta e heterogênea que integra objetos desde lâmpadas, geladeiras, roupas até dispositivos computacionais [Li et al. 2014]. Esta rede proporciona a interação entre os objetos e os seres humanos em ambientes industriais, domiciliares, entre outros. Vários serviços podem ser oferecidos a partir da comunicação da IoT que ocorre através da disseminação de conteúdo. Ela demanda a cooperação entre os objetos da rede que colaboram encaminhando estes conteúdos para a sua adjacência provendo serviços como, a mensuração de temperatura, a localização de objetos e o monitoramento de funções vitais.

Assim, estes serviços podem ser oferecidos aos seres humanos em tempo real. Assim, um dos objetivos de uma rede IoT está em prover o conforto à população, recebendo a IoT em 2010 a denominação de internet do futuro [Gubbi et al. 2013].

A disseminação de conteúdo está sujeita a vulnerabilidades como a perda de enlaces, uso de escutas e a mobilidade do meio sem fio [Wallgren et al. 2013]. Na IoT, esta comunicação precisa lidar com a diversidade capacidade dos recursos, visto que os objetos e os dispositivos computacionais possuem diferentes capacidade de memória, processamento e bateria. A partir destas vulnerabilidades os atacantes podem explorá-las de modo a prejudicar a comunicação. Um atacante afeta a comunicação, descartando de pacotes, selecionando apenas os pacotes desejados, personificando a identidade dos participantes da rede. Desta forma, estas vulnerabilidades precisam ser consideradas para garantir o serviço de disseminação de conteúdo na rede IoT.

Dentre o conjunto de ações maliciosas cometidas por um atacante para prejudicar a disseminação destaca-se a personificação de identidades. Esta ação é realizada pelo ataque Sybil que age na manipulação de identidades dos dispositivos da rede [Agrawal and Vieira 2013]. Um atacante Sybil visa alcançar vantagens, como o uso de recurso não autorizado, a obtenção e a publicação de informações privadas de um ou mais usuários da rede. Na IoT, este ataque afeta a confidencialidade e a privacidade dos usuários, coletando informações pessoais, como o acesso à dados vitais, a chave de uma casa ou de um comércio. Logo, o ataque Sybil presente na disseminação de conteúdo interfere nos serviços oferecidos pela rede IoT ficam expostos a consequências danosas.

As técnicas de detecção do ataque Sybil baseiam-se nas características comuns as redes [Vamsi and Kant 2014], no relacionamento entre os dispositivos próximos [Yu et al. 2006] e na criptografia [Lin 2013]. A técnica baseada nas características comuns à rede considera o uso da força do sinal recebido (RSS, do inglês *Receive Signal Strength*) e do indicador da força do sinal recebido (RSSI, do inglês *Receive Signal Strength Indication*) a fim de identificar um atacante Sybil, contudo, a mobilidade dos dispositivos pode acarretar uma alta taxa de falsos positivos. As outras duas técnicas demandam uma alta sobrecarga na rede. Na criptografia, o custo para gerar chaves assimétricas seguras como o RSA requerem um alto processamento. As chaves simétricas precisam de um par uma chave para cada par de nós para garantir o não repúdio. Já o relacionamento entre os dispositivos requer uma atualização constante dos usuários legítimos e atacantes, e isto pode ocasionar uma sobrecarga na rede. Desta forma, a adoção destas técnicas implicam num *trade-off* entre eficácia e eficiência como limitações de recursos, sobrecarga na rede e escalabilidade.

Este trabalho apresenta um estudo sobre a eficácia e a eficiência das técnicas de detecção do ataque Sybil. O estudo foi conduzido através de um mecanismo que usa a técnica baseada nas características das redes. Ele avalia este mecanismo mediante ao ataque Sybil num ambiente da IoT. Este mecanismo implementa apenas a manipulação de identidades a partir da fabricação. Assim, o roubo de identidades foi desenvolvido a fim de obter uma maior completude na análise dos resultados. Após análises extensivas os resultados foram classificados de acordo com as métricas de eficácia e de eficiência para o ataque Sybil com identidades fabricadas e roubadas.

O restante deste artigo está organizado da seguinte forma: a Seção 2 contém os

trabalhos relacionados. A Seção 3 apresenta as técnicas de detecção do ataque Sybil. A Seção 4 realiza uma avaliação um mecanismo de detecção do ataque Sybil na IoT.

2. Trabalhos Relacionados

Na literatura existem vários estudos que avaliam os serviços oferecidos pelas redes sem fio estruturadas e não estruturadas [Shivlal and Kumar 2012]. Dentre os serviços importantes estão a disseminação de conteúdo e a autenticação dos seus participantes para garantir uma comunicação segura. Contudo, esses serviços estão sujeitos a ataques de traffic ofuscation [Buttyan and Holczer 2012], sinkhole [Cervantes 2014], blackhole [Rani et al. 2015], e Sybil [Park et al. 2013]. Assim, a avaliação de técnicas de detecção de ataques nestes serviços permite aferir a eficácia e o comportamento destas técnicas sob a ação de um ataque. Os trabalhos a seguir avaliam o serviço de autenticação, a identificação do ataque Sybil, e o desempenho de mecanismos na IoT.

Os autores de [da Silva et al. 2008] propuseram uma avaliação do serviço de autenticação de um mecanismo chamado PGP-LIKE, baseado em criptografia para MANETS. Neste estudo, eles analisam a efetividade do PGP-LIKE submetido aos ataques Sybil e blackhole e empregam diversas métricas de desempenho para aferir o mecanismo proposto. Contudo, eles desconsideram métricas de segurança. Lin [Lin 2013] propôs um serviço de autenticação intitulado LSR que utiliza criptografia baseada em chaves simétricas para detectar o ataque Sybil em redes veiculares. O LSR detecta este ataque através da distribuição e da gerência de chaves realizada por autoridades certificadoras. No entanto, a criptografia acarreta uma sobrecarga na rede, e o uso de chaves simétricas detectam apenas o ataque Sybil com identidades fabricadas. Desta forma, a realização da avaliação possibilita observar a eficacia e a eficiência das técnicas de detecção de ataques, e assim melhorar a qualidade dos serviços oferecidos pela rede.

Abbas et al [Abbas et al. 2013] apresentaram no seu trabalho um framework para a identificação do ataque Sybil no serviço de disseminação de uma rede ad hoc móvel. A técnica adotada pelo framework considera as características das redes e dos dispositivos como RSS, RSSI e a mobilidade para detectar um atacante. Contudo, as características da rede são afetadas com interferências eletromagnéticas. Já os autores de [Vamsi and Kant 2014] propuseram um framework baseado em RSS e teste de hipóteses para identificar o ataque Sybil numa rede ad hoc. Este framework considera que os nos das redes sejam fixos para que as análises estatísticas sejam realizadas. Entretanto, esta forma de detecção pode gerar falsos positivos reduzindo a eficiência desta solução. Logo, os efeitos adversos como interferências eletromagnéticas contribuem com a redução de performance de um mecanismo baseado em características da redes, e por isso devem ser levadas em consideração para este tipo de avaliação.

Na IoT, os trabalhos destinam-se a analisar a eficiência de soluções em relação as características desta rede. Os autores em [Blazquez et al. 2015] apresentam uma avaliação de um protocolo de gestão de dados multimídia coletados na IoT. Nele os autores analisam a eficiência do protocolo OpenID e do Sensei nos ambientes desta rede. Este trabalho utiliza métricas de eficiência para aferir o desempenho deste protocolo, contudo a análise só é realizada para o protocolo OpenID desconsiderando o Sensei. Já os autores de [Wang et al. 2014] avaliam a eficiência de um esquema de chaves publicas baseado no atributo (ABE) para IoT. Para esse estudo, dois esquemas ABE foram avaliados o KP-

ABE e o CP-ABE. A avaliação deste trabalho considerou a presença de dispositivos com limitação de recursos, entretanto, foram utilizados apenas métricas de desempenho. Uma das maiores preocupações na IoT está relacionada a segurança dos dados trafegados nesta rede, tornando necessário a avaliação de técnicas de detecção de ataques, falhas e efeitos que prejudiquem a qualidade do serviço oferecido.

3. Técnicas de detecção do ataque Sybil

Esta seção descreve o funcionamento das técnicas de detecção do ataque Sybil existentes e discute a sua eficácia na IoT. Para apoiar o entendimento das técnicas, inicialmente são definidos um modelo de rede IoT, as suas entidades e interação, bem como o modelo de disseminação de dados adotado no trabalho. Em seguida, são explicados os tipos e comportamentos de ataques Sybil. Por fim, são evidenciadas as vantagens e desvantagens de cada técnica de detecção quando aplicadas na IoT.

3.1. Modelo da rede

O modelo da rede IoT consiste num conjunto de objetos (*things*), dispositivos computacionais, e seus respectivos ambientes. Estes ambientes correspondem, por exemplo, a uma residência, um hospital e até uma indústria automobilística. Dentro de um ambiente, os objetos interagem entre si e com os dispositivos computacionais, transmitindo seus dados coletados até uma determinada aplicação. Esta aplicação é manuseada pelos usuários finais através da Internet, como ilustrado na Figura 1. Os dispositivos e objetos são fixos ou móveis, e podem apresentar limitação de recursos. Além disso, a mobilidade torna a rede mais densa ou esparsa devido à associação e desassociação dos seus componentes. Logo, a adoção deste modelo de rede considera a integração entre os dispositivos computacionais, os objetos e seus ambientes de modo a oferecer serviços para seus usuários.

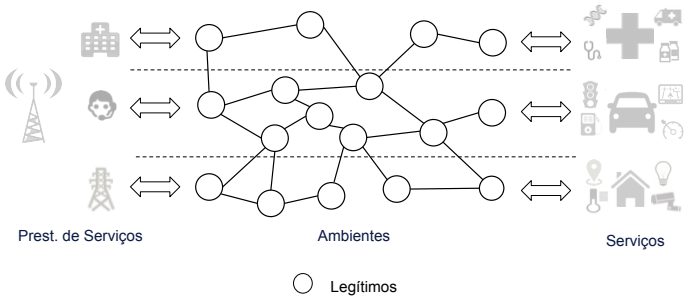


Figura 1. Modelo da rede

A Figura 1 ilustra o modelo da rede IoT, onde há a interação entre os prestadores de serviços, objetos e dispositivos de modo a disseminar um conteúdo do seu ambiente para uma aplicação. Estas aplicações recebem os conteúdos disseminados pelos componentes do ambiente e disponibilizam serviços para seus usuários. Uma companhia de energia, por exemplo, coleta informações de energia elétrica de uma residência. Assim, este serviço informa aos moradores de uma residência o consumo de energia em tempo real, permitindo um maior controle e economia do consumo energético. Este modelo de rede IoT beneficia as pessoas provendo conteúdo em tempo real para aplicações que oferecem serviços para seus usuários.

Os dispositivos computacionais e objetos presentes num ambiente de uma rede IoT formam o conjunto N = $\{n_1, n_2, n_3, ..., n_i\}$ dos nós legítimos. Cada elemento do conjunto N possui um identificador único dentro da rede que é denominado nó da rede. Estes nós atuam como origem, disseminador, e destino. O origem inicia uma disseminação, os disseminadores transmitem o conteúdo para as suas adjacências, e o destino recebe o conteúdo disseminado. Além disso, os nós da rede utilizam o meio sem fio para a transmissão dos dados. Eles realizam a comunicação a partir de um canal assíncrono sujeito à perda de pacotes devido a sua mobilidade. Este modelo define as entidades presentes na rede, as suas funções, e as características do meio de acordo com as necessidades de comunicação da IoT.

3.2. Modelo de Ataque Sybil

O ataque Sybil caracteriza-se pela manipulação de identidades fabricadas ou roubadas. Para realizar a manipulação de identidades, um atacante fabrica ou explora as vulnerabilidades das redes sem fio através da interceptação de pacotes, e do modo promíscuo a fim de adquirir um conjunto de identidades legítimas. Em seguida, este atacante escolhe uma ou mais identidades e solicita associação a partir destas identidades de modo a ludibriar a sua detecção. A Figura 2 ilustra o comportamento do ataque Sybil ao realizar a personificação de nós legítimo, onde as identidades contidas entre as chaves foram manipuladas. Desta maneira, este ataque prejudica o processo de identificação das identidades legítimas de uma rede, prejudicando a confidencialidade dos conteúdos disseminados.

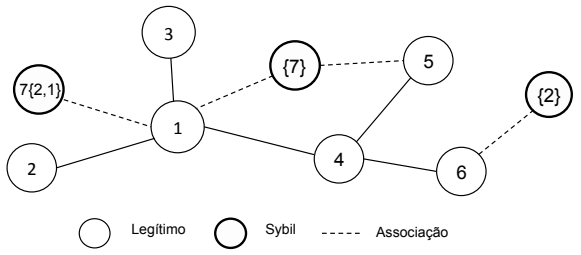


Figura 2. Ataque Sybil sob a rede IoT

Um atacante Sybil visa obter vantagens em uma rede a partir da manipulação de identidades. Estas vantagens consistem em burlar o resultado de sistemas de votações, obter recursos não autorizados, acessar e publicar informações não autorizadas. O ataque pode ser considerado sob dois pontos de vista da segurança de confidencialidade e de privacidade. Um atacante personifica uma identidade legítima infligindo a confidencialidade da rede. Em seguida, ele divulga as informações adquiridas de um nó legítimo, acarretando em perda de privacidade. Logo, o ataque Sybil pode causar danos de segurança aos nós da rede e nos serviços oferecidos para seus usuários numa rede IoT.

A manipulação de identidades realizada por um atacante ocorre através da fabricação e do roubo de identidades. Na técnica de fabricação de identidades, um nó atacante gera, isto é, ele fabrica suas identidades falsas. Esta técnica considera a fabricação de identidades através de listas aleatórias, vetores, e logs. A fabricação de identidades utilizando uma lista aleatória equivale ao conjunto F.Já no roubo de identidades, o atacante pode obter uma lista de identidades através do modo promíscuo. Esta lista consiste do conjunto de identidades R. Por motivos de simplicidade, as listas F e R serão representadas pela lista $S = F \cup R$, onde S representa a união dos conjuntos das identidades

fabricadas e roubadas. Logo após o processo de manipulação, o atacante seleciona as identidades legítimas obtidas e solicita associação para um nó da rede. A manipulação de identidades visa alcançar a personificação de um nó legítimo da rede para obter recursos e informações confidenciais dos membros da disseminação.

Um atacante Sybil pode utilizar o comportamento *churn* para solicitar associação à rede. A Figura 3 ilustra a conduta de um atacante com este comportamento. Nesta figura, num dado tempo t um nó atacante escolhe uma identidade da lista S. Em seguida, ele solicita associação à rede a partir dessa identidade. Caso não consiga o acesso, o atacante desassocia da rede e escolhe uma nova identidade para recomeçar o ataque. Nos instantes seguintes, $t+1$, $t+2$, o atacante realiza o mesmo procedimento de associação e desassociação. Este comportamento visa o acesso à rede e também causa o esgotamento dos recursos de uma rede devido às requisições de associações e desassociações seguidas.

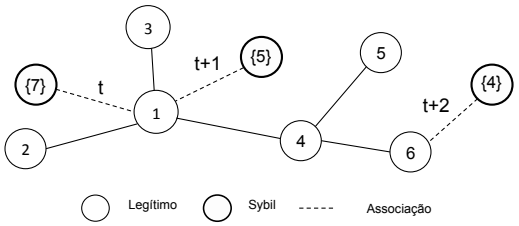


Figura 3. Atacante com o comportamento *Churn* para obter acesso à disseminação

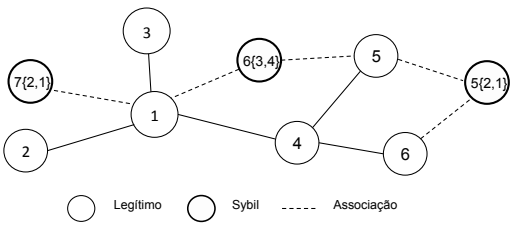


Figura 4. Atacante em conluio para obter acesso à disseminação

Um atacante Sybil também pode solicitar associação através de um conluio de identidades. Neste caso, a Figura 4 ilustra a conduta dos atacantes em conluio de identidades. Nesta figura, os atacantes solicitam associação à rede exibindo mais de uma identidade. Este comportamento tem como objetivo infligir a confidencialidade dos conteúdos disseminados. O resultado de uma votação, por exemplo, pode ser afetado por um atacante que age de forma maliciosa através das suas identidades, alterando, e obtendo informações deste serviço. O comportamento em conluio de identidades do ataque Sybil minimiza a efetividade da qualidade do serviço prestado numa rede.

3.3. Detecção Baseada nas Características das Redes

A técnica 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 à interferências eletromagnéticas e a identificação de um nó numa rede exige uma série de avaliações do seu RSS. A seguir esta técnica será descrita, evidenciando os seus pontos chaves e as suas desvantagens.

A Figura 5 ilustra a detecção do ataque Sybil a partir da técnica das características das redes. Nesta figura, um nó (n_i) detecta o ataque a partir da sua área de cobertura e do RSS do nó solicitante. O nó solicitante será monitorado a partir do momento que o nó atravessar a área de cobertura de n_i. Quando o nó solicitante realizar associação, ele deve enviar a sua identidade dentro da área pontilhada de n_i. Este nó concede acesso a rede e guarda o RSS e a identidade do nó solicitante numa lista composta pela tupla $< RSS, ID >$. A detecção ocorre quando o nó solicitante exibir mais de uma identidade na área pontilhada de n_i. As características das redes possibilitam a detecção do

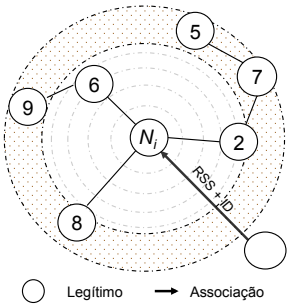


Figura 5. Detecção realizada pela técnica características das redes

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 [Abbas et al. 2013, Vamsi and Kant 2014]. 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.

3.4. Detecção Baseadas em Criptografia e no Relacionamento entre Vizinhos

As técnicas baseadas em criptografia de chaves assimétricas, simétricas, e relacionamento entre os vizinhos desconsideram a presença de dispositivos com restrição de recursos. Isto pode prejudicar tanto a eficácia quanto a eficiência de uma solução que use estas técnicas. Além disso, elas sobrecarregam a rede devido às constantes atualizações nas listas de identidades. Assim, elas podem ser classificadas e agrupadas. A seguir, estas técnicas serão descritas, evidenciando as suas vantagens e desvantagens quando aplicadas na IoT.

A Figura 6 ilustra o funcionamento da técnica baseada em criptografia para identificar o ataque Sybil. Nesta figura, o esquema de criptografia usa chaves simétricas e considera uma autoridade certificadora (AC) que concede e revoga as chaves. Cada nó da rede possui uma lista de identidades onde, ela dever ser atualizada de acordo com a associação de um novo integrante. A comunicação inicia assim que a AC distribuir as chaves para os nós e todas as listas de identidades estiverem atualizadas. Cada ação de um nó da rede é associada a um evento [Lin 2013]. A identificação de um ataque Sybil ocorre a partir da criação de eventos simultâneos realizada por um nó.

A criptografia identifica as duas formas de manipulação de identidades realizada

pelo ataque Sybil. O uso de chaves assimétricas garante o não repúdio que é um requisito para a identificação do ataque Sybil com identidades roubadas. Ao usar um par de chaves um nó garante que assinou uma mensagem através de sua chave privada, garantindo assim o não repúdio. A criptografia com chaves simétrica é aplicada em [Lin 2013] realiza a detecção do ataque Sybil de forma escalar. Esta técnica não possui problemas de escalabilidade, sendo possível a sua aplicação em redes como a IoT. A criptografia realiza a detecção do ataque Sybil com identidades roubadas e fabricadas sem a necessidade de uma técnica adicional como um modelo estatístico.

A criptografia de chaves assimétricas reduz a eficiência de uma rede IoT devido ao alto custo para gerar chaves seguras. Elas também demandam sobrecarga na rede em virtude da atualização constante das chaves dos novos objetos da rede. Já as chaves simétricas requer um gerenciamento através de uma AC ou da criação de uma chave para cada par de nós para identificar o ataque Sybil com identidades roubadas. Contudo, esta abordagem diminui a escalabilidade na rede. Caso um nó atacante tenha o comportamento *churn* para solicitar associação, a detecção proposta por [Lin 2013] é comprometida, por que esta técnica usa apenas uma identidade por evento. Logo, a criptografia com chaves simétricas e assimétricas demandam uma sobrecarga na rede, afetando serviços que exigem tempo real como a mensuração de dados vitais de uma pessoa.

A detecção baseada no relacionamento entre vizinhos esta ilustrada na Figura 7. Nesta figura, os nós da rede possuem duas listas de identidades, dos nós legítimos e dos intrusos [Quercia and Hailes 2010]. Estas listas possuem as identidades dos nós de acordo com a sua reputação na rede num dado momento. A reputação dos nós deve ser atualizada de forma constante a partir das opiniões dos nós vizinhos. A identificação do atacante Sybil acontece quando a parte majoritária dos vizinhos de N_i julgam-o com baixa reputação.

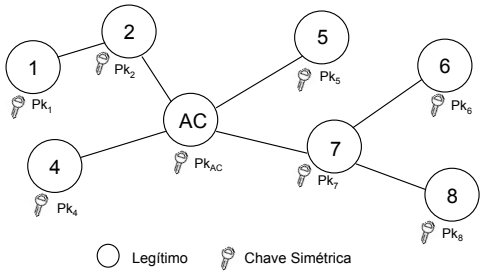


Figura 6. Detecção usando criptografia

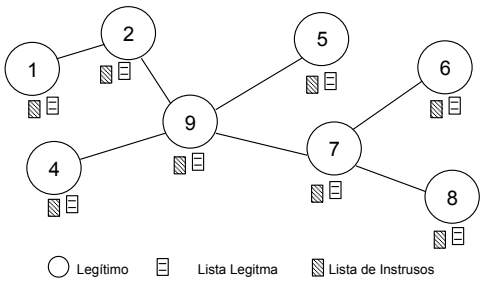


Figura 7. Detecção usando o relacionamento entre vizinhos

A detecção do ataque Sybil a partir do relacionamento entre vizinhos próximos considera o comportamento de um nó como parâmetro para detecção. Esta técnica é adaptável, e de fácil atualização, visto que ela usa como base a classificação dos nós a partir das opiniões de seus vizinhos. Com a aplicação desta técnica é alcançar uma alta acurácia. Este alto nível de acurácia pode ser atingido com um treinamento offline dos comportamentos maliciosos de modo a calibrar o mecanismo de detecção. A técnica baseada no relacionamento entre vizinhos detecta o ataque Sybil de forma dinâmica e com uma alta acurácia.

O relacionamento entre os vizinhos próximos proporciona uma classificação dos nós através das opiniões de vizinhos. Contudo, esta classificação demanda uma sobre-

carga na comunicação dos nós da rede, que reduz o tempo de bateria dos nós da rede. A detecção torna-se complexa quando um atacante solicita associação através de conluio de identidades, reduzindo a quantidade de vizinhos legítimos. Além disso, a alta acurácia pode ser afetada se aplicada em ambientes que requerem uma detecção em tempo real. Esta queda na detecção acontece por que na detecção em tempo real novos padrões de anomalias podem surgir, e os classificadores devem ser treinados a cada nova anomalia. Como boa parte dos serviços prestados pela IoT exigem uma detecção em tempo real, esta técnica torna-se difícil de ser aplicada em virtude da alta sobrecarga na rede e a dependência de uma fase de treino.

4. Avaliação

Esta seção descreve uma avaliação da eficácia e do desempenho do mecanismo proposto por [Abbas et al. 2013], 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.

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.

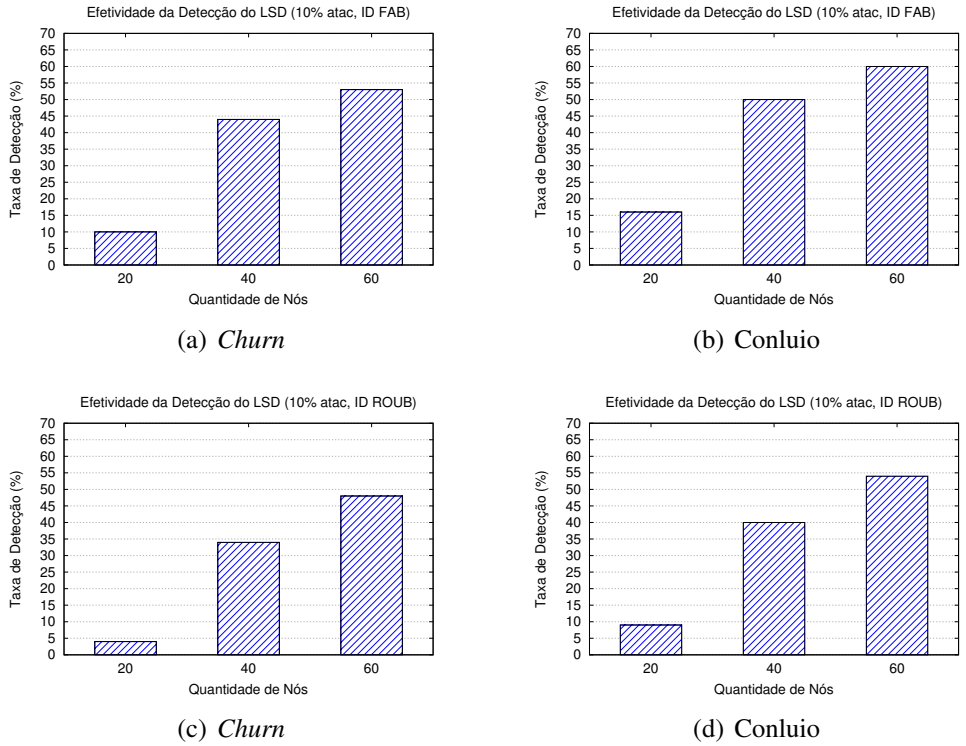
Os parâmetros de simulação usados na configuração da rede IoT consideram a quantidade de nós variando entre 20, 40, e 60. Estes nós podem ser móveis ou fixos, onde os fixos compreendem 25% do total de nós. Eles também emitem a força do sinal recebido (RSS) por até 100 segundos (s) e se deslocam na rede 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.

4.1. Resultados

Esta subseção descreve os resultados da eficácia e da eficiência do LSD. As Figuras 8(a) e 8(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 8(b) e 8(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.



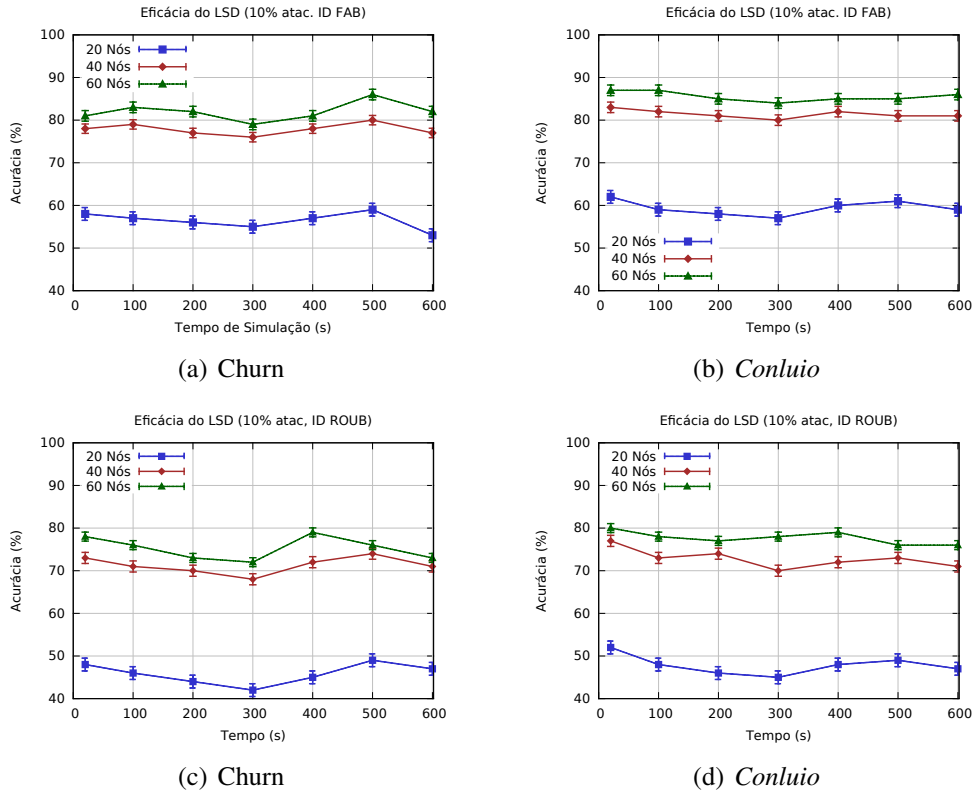
(a) *Churn* (b) Conluio

(c) *Churn* (d) Conluio

Figura 8. T_{det} diante do Ataque Sybil com identidades roubadas e fabricadas

As Figuras 9(a) e 9(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 9(c) e 9(d) mostram a acurácia do LSD sob o ataque Sybil com identidades roubadas. Nestas figuras, o comportamento da detecção é inferior à das Figuras 9(a) e 9(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.



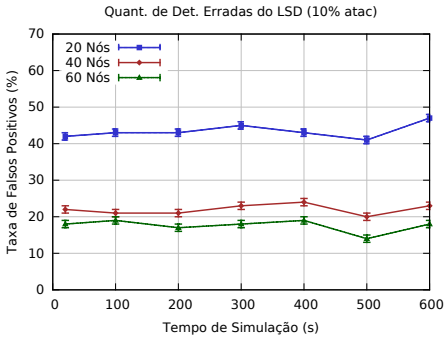
(a) Churn (b) *Conluio*

(c) Churn (d) *Conluio*

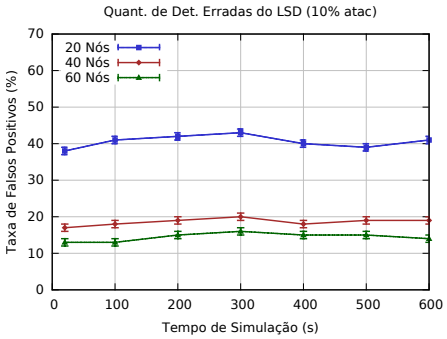
Figura 9. A_c diante do Ataque Sybil com identidades roubadas e fabricadas

As Figuras 10(a) e 10(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 10(b) e 10(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.

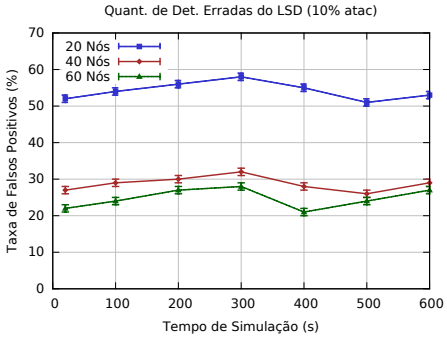
As Figuras 11(a) e 11(b) mostram a efetividade do ataque Sybil com identidades fabricadas numa rede com o LSD. Nesta figura, a efetividade do ataque num cenário esparso é superior aos dos cenários mais densos, ou seja com 40 e 60 nós. Isto ocorre por que a quantidade de nós que realizam a detecção de 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 9(a) instante 300. A efetividade do ataque Sybil com identidades roubadas, Figuras 11(c) 11(d), é ainda maior quando comparado aos resultados das Figuras 11(a) e 11(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.



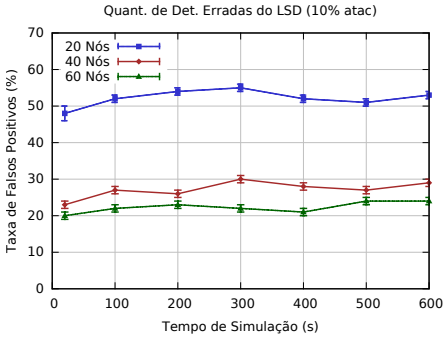
(a) Churn



(b) *Conluio*

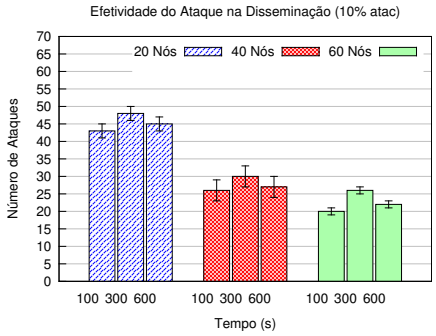


(c) Churn

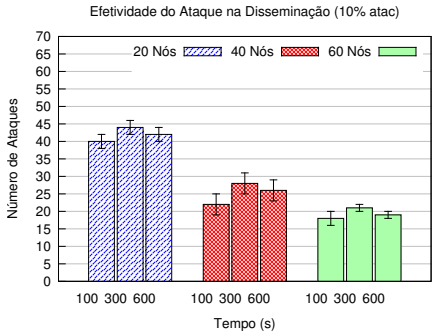


(d) *Conluio*

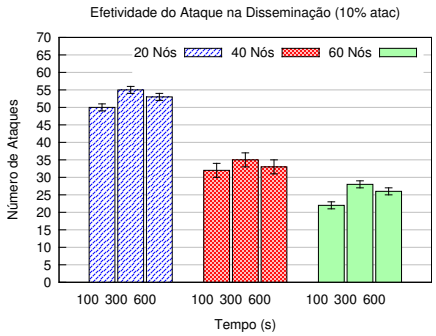
Figura 10. T_{fp} diante do Ataque Sybil com identidades roubadas e fabricadas



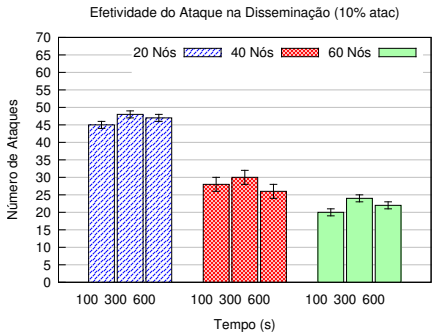
(a) Churn



(b) *Conluio*

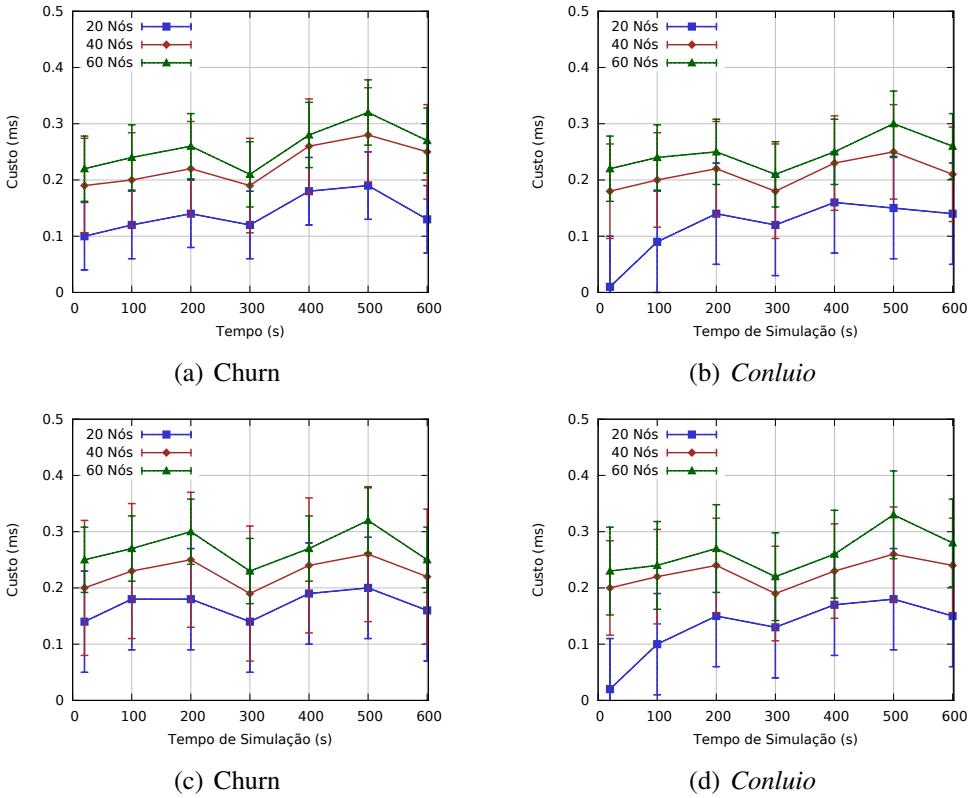


(c) Churn



(d) *Conluio*

Figura 11. Quantidade de Ataques na Disseminação



(a) Churn (b) *Conluio*

(c) Churn (d) *Conluio*

Figura 12. Custo para a disseminação de fluxos de dados

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 12(c), um dado nó numa rede de 20 nós disseminou um fluxo de dados até um nó destino gastando 0.18 ms. Na Figura 12(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 desassociações 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.

5. Conclusão

Este trabalho apresentou um estudo da eficácia e da eficiência sobre as técnicas de detecção do ataque Sybil no serviço de disseminação de conteúdo da IoT. As técnicas de detecção foram classificadas nas características das redes, em criptografia, e no relacionamento entre vizinhos. A eficácia do *Lightweight Sybil Attack Detection Framework* (LSD) foi avaliada sob o ataque Sybil com identidades fabricadas e roubadas, e comportamentos *churn* e de conluio. Este mecanismo apresentou uma baixa eficácia nos cenários mais esparsos, principalmente quando o atacante usa identidades roubadas. A disseminação de conteúdo foi prejudicada quando um atacante utiliza o comportamento *churn*. Portanto, é necessário o desenvolvimento de técnicas eficazes de detecção do ataque Sybil que suportem a qualidade do serviço de disseminação de conteúdo na IoT.

Referências

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

Agrawal, S. and Vieira, D. (2013). A survey on internet of things-doi 10.5752/p. 2316-9451.2013 v1n2p78. *Abakós*, 1(2):78–95.

Blazquez, A., Tsiatsis, V., and Vandikas, K. (2015). Performance evaluation of openid connect for an iot information marketplace. In *Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st*, pages 1–6. IEEE.

Buttyan, L. and Holczer, T. (2012). Traffic analysis attacks and countermeasures in wireless body area sensor networks. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*, pages 1–6. IEEE.

Cervantes, C. A. V. (2014). Um sistema de detecção de ataques sinkhole sobre 6lowpan para internet das coisas.

da Silva, E., Santos, A. L., Albini, L. C. P., and Lima, M. N. (2008). Quantifying misbehavior attacks against the self-organized public key management on MANETs. In *Proceedings of International Conference on Security and Cryptography (SECRYPT '08)*, pages 128–135, Porto, Portugal. INSTCC Press.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013). Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645–1660.

Li, S., Da Xu, L., and Zhao, S. (2014). The internet of things: a survey. *Information Systems Frontiers*, pages 1–17.

Lin, X. (2013). 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.

Park, S., Aslam, B., Turgut, D., and Zou, C. C. (2013). 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.

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

Rani, R., Dolly, M. P., and Kumar, M. D. (2015). Black hole prevention & detection under average energy consumption in wsn.

Shivlal, M. and Kumar, S. U. (2012). Performance analysis of secure wireless mesh networks. *Research Journal of Recent Sciences ISSN*, 2277:2502.

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

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

Wang, X., Zhang, J., Schooler, E. M., and Ion, M. (2014). Performance evaluation of attribute-based encryption: Toward data privacy in the iot. In *Communications (ICC), 2014 IEEE International Conference on*, pages 725–730. IEEE.

Yu, H., Kaminsky, M., Gibbons, P. B., and Flaxman, A. (2006). Sybilguard: defending against sybil attacks via social networks. In *ACM SIGCOMM Computer Communication Review*, volume 36, pages 267–278. ACM.

