Um Sistema de Detecção de Ataques Sinkhole sobre 6LoWPAN para Internet das Coisas

Christian Cervantes, Diego Poplade, Michele Nogueira, Aldri Santos

[1]Núcleo de Redes Sem Fio e Redes Avançadas (NR2)
Universidade Federal do Paraná – Curitiba – Brasil

{cavcervantes,dap10,michele,aldri}@inf.ufpr.br

Abstract. *The networks of Internet of Things (IoT) are formed by heterogeneous objects and these objects have in general very limited resources. Thus, IoT networks are vulnerable to various attacks, being the attack sinkhole one of the most destructive. However, existing solutions to provide protection and security against attacks sinkhole on IoT have high consumption of resources and employ complex mechanisms to ensure good performance. This paper proposes a system, called INTI (intrusion detection of sinkhole attacks on 6LoWPAN for IoT), to identify the presence of sinkhole attacks on the routing service of IoT. INTI aims to prevent, detect and isolate sinkhole attacks on routing within the IoT, while mitigating adverse effects. The system combines the use of watchdog, reputation and trust for detection of attackers, by analyzing the behavior of devices. Simulation results show the INTI performance and efficiency in terms of attack detection rate, number of false positives and false negatives.*

Resumo. *As redes de Internet das coisas (IoT) são formadas por objetos heterogêneos e muito desses objetos possuem recursos limitados. Logo, as redes IoT são vulneráveis a vários tipos de ataques, sendo o ataque sinkhole um dos mais destrutivos. Contudo, as soluções existentes para a proteção e segurança contra os ataques sinkhole em IoT geram um elevado consumo de recursos e usam mecanismos complexos para garantir um bom desempenho. Este trabalho propõe um sistema para identificar ataques sinkhole no serviço de roteamento da IoT, chamado de INTI (Sistema de detecção de* ***I****ntrução de ataques Si****N****khole sobre 6LoWPAN para a Interne****T*** *das Co****I****sas). O INTI visa prevenir, detectar e isolar os ataques sinkhole no roteamento dentro da IoT, e ao mesmo tempo mitigar os efeitos adversos. O INTI combina o uso de watchdog, reputação e confiança para a detecção dos atacantes, por meio da análise do comportamento dos dispositivos. Resultados mostram o desempenho e a eficiência do INTI na detecção de ataques, número de falsos positivos e negativos.*

1. Introdução

Devido aos avanços das tecnologias e a redução dos dispositivos computacionais, estes se tornaram mais acessíveis e mais disponíveis ao público em geral. Baseado nesses avanços, surgiu o conceito da Internet das coisas (IoT). A IoT é uma rede híbrida, aberta e heterogênea que integra dispositivos inteligentes chamados de coisas (*things*), como eletrodomésticos, livros, canetas e carros, entre outros objetos que usualmente não pertencem à computação interatuando com computadores, sensores, celulares, PDAs e outros dispositivos. Estes dispositivos buscam compartilhar informações, dados e recursos, agindo e

reagindo diante de situações e mudanças no ambiente. O objetivo da IoT é possibilitar a integração e a unificação de todos os objetos e sistemas de comunicação que nos cercam.

Com o aumento dos dispositivos inteligentes e a mobilidade de alguns destes, a IoT está exposta a diversas vulnerabilidades na comunicação por apresentar uma infraestrutura variável e a maior parte dos dispositivos possuírem recursos computacionais limitados, como baixa energia, limitada capacidade de processamento, armazenamento, conexão através de links com perdas e outras características [Atzori et al. 2010]. Em razão das características, a IoT torna-se vulnerável a diversas formas de ataques de roteamento [Wallgren et al. 2013]. Dentre esses tipos de ataques na IoT, destaca-se o ataque *sinkhole*, sendo considerado um dos ataques de roteamento mais destrutivos para as redes sem fio [Jin Qi 2012, Bannack et al. 2008]. Um dispositivo atacante *sinkhole* tem o objetivo de atrair a maior quantidade de tráfego de uma certa área prejudicando um ponto de coleta de receber os dados enviados pelos nós.

Apesar de existirem vários trabalhos na literatura que quantificam o impacto do ataque *sinkhole* sobre redes como redes móveis Ad hoc (MANETs), redes de sensores sem fio (RSSFs) e redes veiculares Ad hoc (VANETs) [Sedjelmaci and Feham 2011, Sheela and Mahadevan. 2011, Shafiei et al. 2014, Lima et al. 2009], estas soluções geram outros problemas para a rede denominados de *efeitos adversos*, como elevadas taxas de falsos positivos e falsos negativos, elevado consumo de energia, baixo desempenho do sistema, entre outros. Além disso, poucas pesquisas têm sido desenvolvidas para a proteção e a segurança da IoT na transmissão de informação [Raza et al. 2013, Kasinathan et al. 2013], e estes trabalhos são inadequados para um funcionamento dinâmico porque não consideram a mobilidade dos dispositivos, sendo isso fundamental para seu uso por pessoas e objetos.

Os sistemas de detecção de intrusão (IDS) têm como objetivo melhorar a segurança diante de ataques e ameaças aos sistemas computacionais ou redes de computadores. Alguns trabalhos utilizam estratégias de *watchdog* para a detecção local de nós atacantes [Keally et al. 2010, Wahab et al. 2014], sendo capaz de escutar, analisar os pacotes transmitidos pelo próximo salto (*next-hop*) e dos nós vizinhos. Esta estratégia minimiza o número de falsos positivos e negativos aumentando a eficiência e evita o descarte de pacotes por nós vizinhos. Outros trabalhos usam mecanismos de reputação e confiança [Perez-Toro et al. 2010, Ganeriwal et al. 2008]. Entre as suas vantagens, estão que eles são dinâmicos, temporais e precisam ser atualizados de forma constante para que permitam identificar a origem da ameaça. Este mecanismo, além de ser eficaz, ajuda a reduzir o impacto de ataques na rede conseguindo um bom desempenho do sistema. Contudo, essas estratégias não têm sido aplicadas na IoT embora sejam adequadas.

Este trabalho propõe um sistema para identificar a presença de ataques *sinkhole* dentro do serviço de roteamento da IoT, chamado de INTI (*Sistema de detecção de **I**ntrução de ataques Si**N**khole sobre 6LoWPAN para a Interne**T** das Co**I**sas*). O INTI visa prevenir, detectar e isolar os efeitos do ataque *sinkhole* no serviço de roteamento, e ao mesmo tempo mitigar os *efeitos adversos*. O sistema combina o uso de *watchdog* com o uso reputação e confiança, para a detecção de ataques *sinkhole* na IoT, por meio da análise do comportamento de cada nó. Os resultados da simulação mostram que o INTI garante uma taxa de detecção de pelo menos 92% em um cenário com nós fixo e de 75% em um cenário com nós móveis.

O restante deste artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados. A Seção 3 detalha o modelo da IoT. A Seção 4 descreve o sistema INTI. A Seção 5 apresenta a avaliação e os resultados obtidos pelo sistema diante de ataques. A Seção 6 finaliza o trabalho com as conclusões e os trabalhos futuros.

2. Trabalhos Relacionados

Diversas técnicas e mecanismos que tratam da segurança na comunicação têm sido utilizados para a detecção de ataques *sinkhole*. Os autores [Moon and Cho. 2009] propõem um IDS utilizando lógica *fuzzy* para a detecção da ataques *sinkhole* em uma RSSFs. Esta abordagem emprega nós mestres a fim de monitorar a comunicação. Os nós atacantes são detectados a partir dos dados coletados pelos nós mestres. Os autores [Sedjelmaci and Feham 2011] propuseram um IDS híbrido baseado em agrupamentos para uma RSSF. Este sistema usa uma combinação entre a detecção de anomalias baseado em máquina de vetor de suporte (SVM) e a detecção através de assinaturas. Ele possui dois módulos: a detecção híbrida (HIDM) e a detecção cooperativa (CDM) dos nós. No HIDM, ocorre o processo de treinamento, onde cada agente IDS treina o SVM localmente. Já o CDM executa um mecanismo de votação para a detecção de nós suspeitos.

O IDS proposto em [Sheela and Mahadevan. 2011] apresenta o uso de agentes móveis para a detecção de ataques *sinkhole*. Estes agentes utilizam dois algoritmos: o algoritmo de navegação e o algoritmo de roteamento. O algoritmo de navegação onde um agente móvel fornece informações da rede quando visita cada nó. O algoritmo de roteamento de dados descreve como um nó usa as informações da rede para rotear os pacotes de dados para não acreditar em caminhos falsos. Os autores [Shafiei et al. 2014] propõem duas abordagem para detectar ataques *sinkhole* em uma RSSF. A lógica utilizada é que os nós ao redor do *sinkhole* esgotam sua energia mais rápido. A primeira abordagem utiliza um método de geoestatística para avaliar a energia residual de cada região. A segunda abordagem possui um método de monitoramento distribuído para detectar regiões com o menor nível de energia residual a fim de detectar o atacante. Contudo, os sistemas abordados possuem a desvantagem de gerar elevadas taxas de falsos positivos e negativos, aumentado o consumo de memória e energia, entre outros. Além disso, essas abordagens não são apropriadas para a IoT por serem muito complexas. Desta forma, faz-se necessário a construção de IDS para IoT baseada em técnicas mais simples e eficazes.

O mecanismo RDAS [Perez-Toro et al. 2010] usa uma abordagem baseada na reputação para identificar e isolar nós maliciosos em uma RSSF. Ele considera a formação de agrupamentos dos nós, onde o líder analisa os dados coletados dos nós do agrupamento para determinar a localização de um evento malicioso, usando a redundância dos dados. Do mesmo modo, o modelo em [Wahab et al. 2014] propõe uma solução para detectar nós egoístas em (VANETs). O modelo consiste em duas fases: (i) motivar os nós para que atuem de maneira cooperativa utilizando incentivos; (ii) o uso de *watchdog* para detectar nós egoístas baseado em evidências cooperativas, aumentando a probabilidade de detecção. Contudo, estas estratégias além de ser eficazes e efetivas, devem ser usadas em conjunto para garantir um ambiente de comunicação segura para a IoT.

Existem na literatura poucas pesquisas desenvolvidas para a proteção e a segurança da IoT na transmissão de informação. O sistema SVELTE [Raza et al. 2013] considera consultas realizadas a partir de um roteador de borda, que percorre todos os

nós de uma rede IoT, a fim de detectar inconsistências. Essas inconsistências são obtidas através de comparações das informações das posições de cada nó. Já o sistema Ebbits [Kasinathan et al. 2013] emprega um componente que escuta o tráfego da rede a fim de realizar uma análise e detectar nós com mau comportamento em redes 6LoWPAN. Apesar destes IDSs atenderem a maioria das características da IoT, eles não consideram a mobilidade e são muitos restritos na análise do comportamento dos nós. Além disso, esses sistemas possuem elevadas taxas de consumo de recursos e baixo desempenho.

3. Modelo da IoT para o Sistema INTI

Esta seção descreve a rede física, o modelo de comunicação e o ataque. Esta rede considera dispositivos heterogêneos, sendo alguns deles móveis. Além disso, a rede possui duas hierarquias: a hierarquia principal e auxiliar. A **hierarquia principal** é a estrutura que permitirá a comunicação entre os diferentes agrupamentos, nesta hierarquia só intervém os nós líderes, os nós associados e a estação-base como alvo. A **hierarquia auxiliar** compreende a comunicação de cada agrupamento realizado pelo nó líder e seus nós membros. Portanto, a vantagem destas hierarquias é que elas permitem a comunicação de várias sub-redes, oferecendo um ganho expressivo na escalabilidade, estabilidade como mostra a Figura 1. A IoT no sistema INTI possui três características: o modelo físico da rede, o modelo de comunicação e o modelo do ataque, como apresentado na Figura 1.

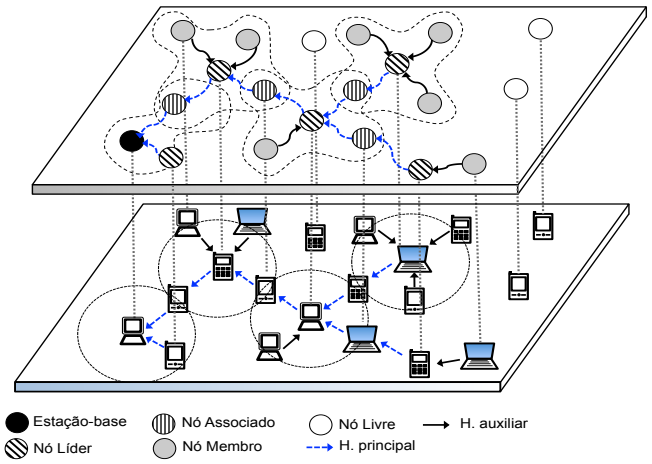

Figura 1. Modelo da IoT

Modelo físico da rede: O sistema INTI assume que a rede consiste em um conjunto T composto por n objetos (nós) identificados por $\{n_1, n_2, n_3, ..., n_i\}$, onde $n_i \in T$. Cada nó n_i possui um identificador (ID) único. A comunicação ocorre através do meio sem fio utilizando um canal de forma assíncrona, sujeita à perda de pacotes devido à mobilidade dos nós. O raio de transmissão empregado é igual para todos os nós da rede. Assume-se que inicialmente todos os dispositivos começam livres assumindo três papeis: nó membro, um nó associado ou um nó líder. Um nó livre é aquele que não pertence a um agrupamento, este movimenta-se dentro de uma determinada área de cobertura da rede. Um nó membro é aquele que pertence a um agrupamento, ele envia informações para seu líder em um intervalo de tempo. Os nós associados são os nós que fazem a conexão entre agrupamentos para o encaminhamento de dados. Os nós líderes tem a função de coletar as informações dos nós membros e encaminhar para o destino.

Modelo de comunicação: Para que os dispositivos da rede interajam é necessário de protocolos respeitem as limitações dos dispositivos que compõem a IoT. O protocolo 6LoWPAN permite o roteamento de pacotes IPv6 na rede 6LoWPAN (IPv6 com baixo consumo de energia para Rede sem fio de Área Pessoal) de uma forma comprimida. A compressão é necessária para permitir a ligação do 6LoWPAN e protocolo de camada física, IEEE 802.15.4. Com esta rede é possível conectar dispositivos com recursos limitados com a Internet convencional para formar a IoT. O RPL (Protocolo de roteamento IPv6 para redes de baixa potência e com perdas) [Gaddour and Koubâa 2012] é um protocolo de roteamento que respeita as limitações dos dispositivos da IoT. A desvantagem deste protocolo é que ele funciona só em ambientes estáticos [Korbi 2012]. O protocolo de comunicação utilizado pelo sistema INTI é uma variação do protocolo RPL, onde considera-se mobilidade e formação de agrupamentos. Além disso, a conexão orientada protocolos da Web, como HTTP não são viáveis e um novo protocolo, o protocolo de aplicação restrita (COAP), tem sido padronizada para a IoT.

Modelo do ataque na rede: Cada nó é responsável pelo envio e encaminhamento dos pacotes de dados. Um ataque tem como objetivo afetar o funcionamento normal e pôr em perigo a segurança da rede. Os nós afetados pelo ataque desempenham a função de nó líder, nó associado ou nó membro. O ataque *sinkhole* anuncia para seus vizinhos que possui o caminho ideal, o mais curto para o destino pretendido, a fim de atrair a maior quantidade de tráfego de uma certa área prejudicando um ponto de coleta de dados. Além disso, este ataque realiza outros tipos de ameaças, como o ataque *selective forwarding*.

4. Arquitetura do Sistema INTI

Esta seção apresenta a arquitetura INTI (*Sistema de detecção de **I**ntrução de ataques Si**N**khole sobre 6LoWPAN para a Interne**T** das Co**I**sas*) e detalha seus módulos. O INTI considera a mobilidade dos dispositivos (nós) que fazem parte da IoT, bem como a adaptabilidade dos nós adversários, sendo estes totalmente distribuídos e reativos. O INTI possui quatro módulos: o módulo de formação e restauração dos agrupamentos, o módulo de monitoramento, o módulo de detecção, e o módulo isolamento, ilustrado na Figura 2.

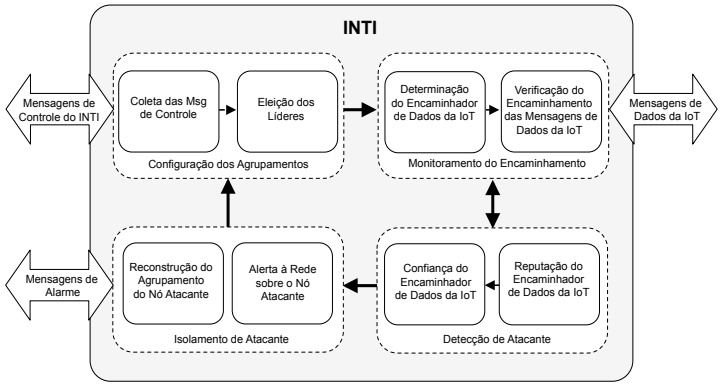

Figura 2. Arquitetura do INTI

O sistema INTI tem as propriedades de *auto-organização* e *auto-reparação*. A propriedade de auto-organização tem como objetivo a coordenação e cooperação dos dispositivos para a configuração da rede. Já a auto-reparação auxilia na detecção de um nó falho, reagrupando os nós afetados, a fim de manter a estabilidade da rede.

4.1. Formação e restauração dos agrupamentos

Este módulo gera uma hierarquia baseada em nós líderes para a formação de agrupamentos a fim de organizar, garantir a escalabilidade e estender a vida útil da rede. Os nós da rede são classificados como: *nós membros*, *nós associados* e *líderes*, conforme Figura 1. A classificação de cada nó mudará dependendo da função que desempenhe dentro da rede.

Inicialmente todos os nós da rede começam livres transmitindo e coletando dados de controle, como ilustrado na Figura 3. O nós enviam dados via *broadcasts* a fim de estabelecer troca de mensagens. Essas mensagem estimam a quantidade de nós vizinhos para eleger os líderes. Os nós livres são classificados como nós líderes quando estes possuem a maior quantidade de nós vizinhos em relação aos outros. Após da eleição dos líderes, são definido os agrupamentos. Nesta fase, os líderes aguardam a decisão dos nós livres (vizinhos), sendo estes nós responsáveis por selecionar um dos líderes para formar o agrupamento. Uma vez formado os agrupamentos, os líderes verificam se um dos nós de seu agrupamento (nós membros) recebeu mais mensagens de diferentes líderes. Caso exista um nó membro que recebeu diferentes mensagens, este nó será classificado como nó associado, sendo este capaz de interligar agrupamentos. No caso de haver dois nós membros dentro da mesma área, o nó membro é escolhido sendo aquele nó que possui a maior índice de energia (*IE*) que é determinado por: $IEi = \frac{TEr_i}{TEc_i}$, onde TEr_i é o total de energia restante do mesmo nó n_i e TEc_i representa o total de energia consumida pelo nó.

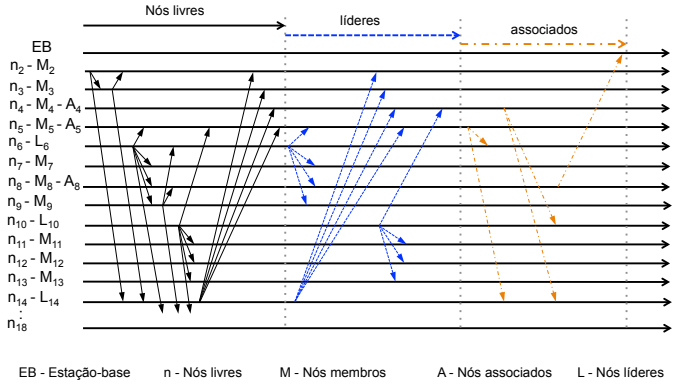

Figura 3. Formação dos agrupamentos no INTI

O uso da função densidade de probabilidade Beta denotada por $Beta(p|\alpha,\beta)$, representa o status de um nó dentro da IoT. Além disso, os parâmetros $Beta(\alpha,\beta)$ são constantemente atualizados determinando o comportamento de um nó. A Equação 1 define a função Beta, em que *p* é a probabilidade de ocorrência de α e $(1-p)$ é a probabilidade de ocorrência de β.

$$Beta(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} = \frac{p^{\alpha-1}(1-p)^{\beta-1}}{B(\alpha,\beta)} \quad (1)$$

$$Onde: 0 \leq p \leq 1 \quad e \quad \alpha,\beta > 0$$

A probabilidade de densidade e sua expectativa estatística fundamenta-se na função Beta. Ela é representada pela integral definida por: $B(\alpha,\beta) = \int_0^1 t^{\alpha-1}(1-p)^{\beta-1}dt$. A variável *status* (*St*) armazena o comportamento dos nós determinando como o

nó atua na transmissão de mensagens. $St = \frac{\alpha}{\alpha+\beta}$. Este valor tem como base a probabilidade de esperança futura *E(p)*, que é calculado a partir da função de densidade Beta.

A restauração do agrupamento acontece quando um dos nós falha, abandona o agrupamento ou quando ocorre um ataque *sinkhole*. Se um nó líder é afetado por alguns destes problemas, efetua-se uma nova eleição ou os nós membros afetados reagrupam-se em agrupamentos vizinhos. Se um nó associado é afetado existe a possibilidade de escolher outro nó associado, desde que este esteja dentro da área em comum. Caso contrario, se ambos líderes estão dentro do mesmo raio de transmissão, realiza-se uma fusão dos agrupamentos, considerando a maior quantidade de nós membros que cada agrupamento possui. Este método tem como finalidade minimizar o número de líderes.

4.2. Monitoramento do encaminhamento de dados

O módulo de monitoramento aplica os princípios de *watchdog* que monitora e contabiliza o número de transmissões de entrada e saída realizadas por um nó. Para isso, o nó monitor computa a quantidade de transmissões realizadas por um nó "superior" em relação a suas próprias mensagens. Um nó é chamado de nó superior quando este possui um (*rank*) menor. Feito isto, estima-se a quantidade de transmissões realizadas de entrada e saída. Se a quantidade de transmissões de entrada são iguais ao número de transmissões de saída o nó é considerado bom. Caso contrario, o componente assume que está acontecendo algum desvio do seu funcionamento normal.

4.3. Detecção de ataque Sinkhole

No módulo de detecção, o INTI identifica e revela a identidade do nó atacante *sinkhole*. Para isso, este módulo realiza avaliações da reputação e confiança dos nós para detectar nós atacantes. Tais avaliações ocorrem de forma constante mantendo a segurança e a integridade dos nós da IoT. A reputação é a opinião ou percepção que uma entidade cria através de iterações, ações ou informações. Sendo estas iterações de modo diretas ou indiretas com base a tarefas passadas. O uso da distribuição *Beta (α,β)* é essencial para representação da reputação e da confiança dos dispositivos (nós) da IoT. A vantagem de usar esta distribuição é que os parâmetros são continuamente atualizados.

O sistema INTI calcula três predições: incerteza (*i*), crença (*c*) e descrença (*d*) a partir da distribuição *Beta (α,β)* para representar a reputação. Os líderes, nós associados e algumas vezes pelos nós membros realizam esses cálculos. O cálculo destas predições $(i, c, d) \in (0, 1)^3 : i + c + d = 1$ respetivamente. A incerteza é a variância normalizada da distribuição Beta, sendo calculada de acordo com: $i = \frac{12*\alpha*\beta}{(\alpha+\beta)^2*(\alpha+\beta+1)}$, onde α e β obtidas da distribuição Beta. A certeza é computada por $(1 - i)$, que é dividida na crença (c) e na descrença (d) de acordo com sua proporção de iterações de prova. Sendo estas computadas através do valor esperado da distribuição Beta. Este cálculo é obtido por: $c = \frac{\alpha}{(\alpha+\beta)}(1 - i)$. Por ultimo, a descrença (d) é alcançado por: $d = (1 - i) - c = \frac{\beta}{(\alpha+\beta)}(1 - i)$.

Após obtidos os cálculos das predições (i, c, d) é possível calcular a reputação. A reputação de um nó é calculado a partir das próprias experiências baseadas nas predições computadas e do *status* enviado por um nó membro a seu líder. Desta forma, cada nó propagará seu *status* (*St*) sobre **seu comportamento na transmissão de mensagens** para o cálculo de sua reputação. Esses valores são dados de entrada para o uso da teoria de *Dempster-Shafer*, a fim de aumentar a probabilidade de detecção e reduzir os falsos

alarmes. A reputação é um valor continuo dentro dos limites R[0,1], se o valor de um nó é maior ou igual 0,5 considera-se um nó bom caso contrario, é considerado um nó atacante. Um nó $n_i : \Omega\{T, \overline{T}\}$, onde Ω tem três hipótese (*H*): $H = T$ representa que n_i é bom, $\overline{H} = \overline{T}$ mostra que n_i não é bom e $U = \Omega$ em que n_i representa que é bom ou não bom. Por exemplo, se o nó líder L_1 afirma que nó membro m_2 é bom, então a sua atribuição básica de probabilidade é representada na Equação 2.

$$\begin{aligned} m_2(H) = &\quad c \\ m_2(\overline{H}) = &\quad 0 \\ m_2(U) = &\quad 1 - c \end{aligned} \tag{2}$$

Se o nó líder L_1 afirma que nó membro m_2 não é bom, então a sua atribuição básica de probabilidade é representada na Equação 3.

$$\begin{aligned} m_2(H) = &\quad 0 \\ m_2(\overline{H}) = &\quad c \\ m_2(U) = &\quad 1 - c \end{aligned} \tag{3}$$

As probabilidades prévias determinadas pelo líder para o nó m_2 levam em consideração o (*St*) do próprio nó. A construção das probabilidades do nó líder em relação ao nó m_2, conforme mostra a Equação 4, onde K representa a normalização das crenças, sendo representado por $K = \sum_{L \cap M = \emptyset} m_1(L)m_2(M)$, e onde a reputação é dado pelo valor de $m_1(H) \oplus m_2(H)$, sendo este um valor continuo entre $0 \leq m_2 \leq 1$. Este resultado considera $m_2 < 0,5$ como nó com má reputação e com valor de $0,5 \geq m_2$ representará um nó bom.

$$\begin{aligned} m_1(H) \oplus m_2(H) = &\quad \frac{1}{K}[m_1(H)m_2(H) + m_1(H)m_2(U) + m_1(U)m_2(H)] \\ m_1(\overline{H}) \oplus m_2(\overline{H}) = &\quad \frac{1}{K}[m_1(\overline{H})m_2(\overline{H}) + m_1(\overline{H})m_2(U) + m_1(U)m_2(\overline{H})] \\ m_1(U) \oplus m_2(U) = &\quad \frac{1}{K}[m_1(U)m_2(U)], \end{aligned} \tag{4}$$

$$\begin{aligned} Onde : K = &\quad m_1(H)m_2(H) + m_1(H)m_2(U) + m_1(U)m_2(H) + \\ &\quad m_1(\overline{H})m_2(\overline{H}) + m_1(\overline{H})m_2(U) + m_1(U)m_2(\overline{H}) + \\ &\quad m_1(U)m_2(U) \end{aligned}$$

Após obtida a reputação, calcula-se a confiança (*C*). Este cálculo considera dois valores (γ, δ), sendo realizada pela Equação 5, onde u é computado a partir do número de iterações realizadas entre dois nós n_i e n_j, dada por *m*: $u = 1 - \frac{1}{m}$, onde u possui valores entre $0 \leq u \leq 1$.

$$\gamma = u\gamma + r \quad ; \quad \delta = u\delta + (1 - r) \tag{5}$$

A Equação 6 obtém o valor da confiança que varia entre [0,1] com um valor médio de 0,5. Se o valor obtido é maior que 0,5 então o nó é considerado bom caso contrario, o nó é considerado atacante. A reputação, assim como a confiança precisam ser atualizadas de forma constante, para a detecção do *sinkhole*.

$$C = \mathbf{E}(Beta(\gamma + 1, \delta + 1)) = \frac{\gamma + 1}{\gamma + \delta + 2} \tag{6}$$

4.4. Isolamento do atacante

Uma vez detectado um nó *sinkhole*, o módulo de isolamento faz com que ele seja isolado da rede. Para isso, o nó que detectou o *sinkhole* gera e propaga uma mensagem de alarme em *broadcast* com o ID do nó atacante colocando o ID na *blacklist* da estação-base. Além disso, o nó que detectou o ataque promove o isolamento do atacante enviando uma mensagem de restauração para seus vizinhos. O *rank* é o dado que permitirá aos nós realizem a restaurem do agrupamento. Existem três formas de isolar um *sinkhole*: (i) quando um nó *sinkhole* é um nó membro: este será isolado pelo nó líder; (ii) quando o *sinkhole* assume a função de líder; neste caso os nós membros isolam o nó *sinkhole* ou caso exista um nó associado este isola o *sinkhole*; (iii) quando o nó *sinkhole* assume a função de nó associado, este será isolado pelo líder, com o maior *rank*, quebrando a comunicação com ele. É necessário verificar se existe dentro do agrupamento, que isolou o atacante, algum nó associado com o menor *rank*, a fim de encaminhar as mensagens do agrupamento para o destino. Caso contrario, o líder propagará uma mensagem de restauração para os nós do agrupamento para que se juntem em agrupamento vizinhos.

5. Avaliação do INTI

O sistema INTI foi implementado no simulador Cooja que faz parte do Contiki [Dunkels et al. 2004], sendo este um sistema operacional de código aberto para sistemas embarcados e redes de sensores sem fio. O IDS SVELTE usado para comparação também foi implementado neste simulador. Para avaliar a eficácia e a eficiência dos sistemas INTI e SVELTE, foi considerado um cenário com ataques *sinkhole*.

O cenário é composto por 50 nós, alguns fixos e outros moveis que representa a quantidade média de usuários podem transitar em uma estrada. Esses usuários utilizam equipamentos sem fio, como celulares, PDAs, notebooks, e movimentam-se em uma área delimitada. A área demográfica de IoT utilizada compreende um ambiente realística de caráter urbano como uma estrada [Bellavista et al. 2013], onde existe uma mistura de objetos e dispositivos. Esses usuários podem ser pedestres, pessoas correndo, ciclistas até automóveis que movimentam-se com velocidades entre 0 m/s até 6,94 m/s. A quantidade de nós *sinkhole* igual a 10 e 15 o que representa 20% e 30% dos nós pertencentes a ambos sistemas de detecção. Os nós usam o canal sem fio na comunicação, seguindo o modelo de propagação (*Unit Disk Graph Medium* (UDGM)) e o modelo de movimentação aleatória *RandomWaypoint* em uma região de $100x100m$. O protocolo de roteamento empregado no INTI é uma modificação do protocolo RPL, o raio de alcance dos nós varia de 10 a $40m$, e o tipo de pacote de transporte utilizado pelos nós é o UDP. O tempo de simulação é de 1500s. Os resultados apresentados são a média de 35 simulações e com um intervalo de confiança de 95%. As métricas utilizadas pelo sistema INTI são detalhadas a seguir:

Taxa de detecção do ataque sinkhole (T_{det}) contabiliza os ataques identificados corretamente pelo sistema INTI. O cálculo desta métrica é alcançada seguindo a Equação 7, em que *X* representa o total de iterações dos nós atacantes e os respectivos resultados obtidos pelo INTI, dado na forma de *X = (d, c)*, em que *d* é o valor da detecção realizada pelo sistema e *c* é a autêntica condição do nó $n_i \in R$.

$$T_{det} = \frac{\sum D_i}{|X|} \forall_i \in X \quad \text{onde} \quad D_i = \begin{cases} 1, & \text{se} \quad d_i = c_i, \\ 0, & \text{se} \quad d_i \neq c_i. \end{cases} \tag{7}$$

Taxa de falsos negativos (Tx_{Fn}) indica a quantidade de vezes em que os nós *sinkhole* foram considerados pelo sistema como nós confiáveis. Essa métrica é obtida pela Equação 8, em que *X* contabiliza o número total de iterações realizadas pelo INTI e T_{det} representa a taxa de detecção do *sinkhole*, que foi alcançada seguindo a Equação 7.

$$Tx_{Fn} = |X| - T_{det} \tag{8}$$

Taxa de falsos positivos (Tx_{Fp}) determina a quantidade de vezes que o sistema detectou um ataque *sinkhole* sendo este negativo. A Tx_{Fp} é calculada pela Equação 9, em que *Z* é o conjunto das iterações dos nós normais, na forma *Z = (d, c)*, onde *d* representa o valor da detecção realizada pelo INTI e *c* é a condição real do nó $n_i \in R$, onde *c=1* representa um nó atacante e *c=0* representa um nó bom.

$$Tx_{Fp} = \frac{\sum Dp_i}{|Z|} \forall_i \in Z \quad \text{onde} \quad Dp_i = \begin{cases} 1, & \text{se} \quad d_i = 1, \\ 0, & \text{se} \quad d_i \neq 0. \end{cases} \tag{9}$$

Consumo de energia (E_{gc}) indica o total do consumo de energia dos nós da rede durante a simulação. Este cálculo é representado pela Equação 10, em que $\sum_{z=1}^{i} TE_i$ representa a somatória total de energia inicial de todos os nós da rede e $\sum_{z=1}^{i} TE_r$ é o somatório total da energia restante dos nós. Onde $\sum_{z=1}^{i} n_z = 1$ e $\forall$ *R* obtendo assim a energia total consumida quando é rodado o sistema.

$$E_{gc} = \sum_{z=1}^{i} (TE_i - TE_r) \tag{10}$$

Taxa de entrega de pacotes $(Tx_{Entrega})$ determina o total de pacotes de dados recebidos com sucesso. O cálculo da $Tx_{Entrega}$ é apresentada na Equação 11, onde esta é calculada dividendo o número de pacotes recebidos pelo destino através do número de pacotes originados pela origem.

$$Tx_{Entrega} = \frac{NpacotesRecibidos}{NpacotesEnviados} X100 \tag{11}$$

5.1. Eficácia

A avaliação da eficácia do INTI e SVELTE considera as métricas a T_{det}, Tx_{Fn} e Tx_{Fp}. No cenário fixo, o INTI e o SVELTE apresentam praticamente uma igualdade (92% e 90% respetivamente) na detecção de ataques *sinkhole*, como ilustra a Figura 4(a). Essa diferença de detecção entre o INTI e o SVELTE ocorre porque o SVELTE tem que percorrer todos os nós da rede, a fim de detectar as inconsistências. Em um cenário móvel, como ilustra a e Figura 4(b), a taxa de detecção do SVELTE diminuiu para 24% e a da INTI é superior a 70%. Esse aumento na taxa de detecção entre o INTI e o SVELTE se deve ao fato que o SVELTE não permite a mobilidade dos nós, sendo uns dos seus pontos fracos. Logo, o INTI supera ao SVELTE em um cenário fixo como móvel.

A taxa de falsos negativos obtidos pelo INTI em um cenário fixo é de 8%, Figura 5(a). Isso significa que poucos nós *sinkhole* não são detectados. A falha na detecção de um *sinkhole* pode acontecer devido à autonomia na detecção, que permite que os nós

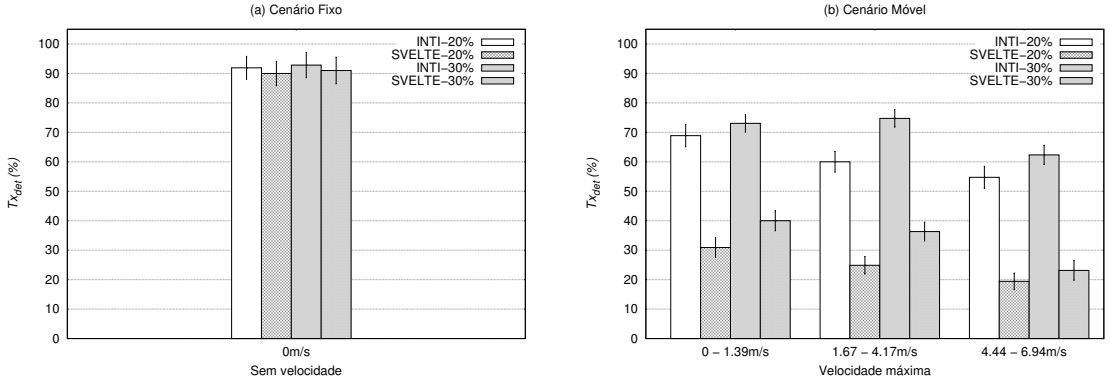

Figura 4. T_{det} do INTI e SVELTE diante de ataques sinkhole

contabilizem individualmente os pacotes transmitidos por outro nó, atuando como observador. Dessa forma, alguns nós podem demorar na identificação de nós *sinkhole*. Para um cenário com nós móveis, a quantidade de falsos negativos obtida pelo INTI é de 28% e pelo SVELTE é de 38%, conforme apresentado na Figura 5(b). Esse aumento de falsos negativos acontece pela dinamicidade dos nós da rede.

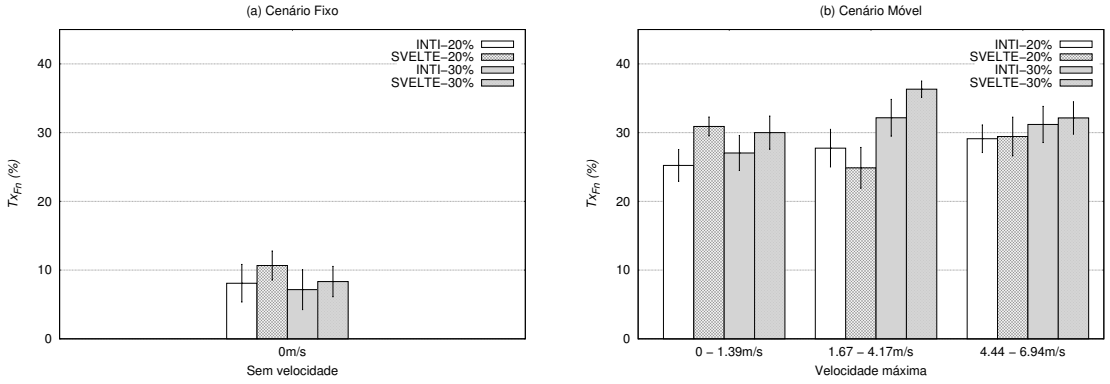

Figura 5. Tx_{Fn} do INTI e SVELTE diante de ataques sinkhole

Como mostra a Figura 6(a), a taxa de falsos positivos obtida pelo INTI na detecção de ataques *sinkhole* em um cenário com nós fixos é inferior a 3%. Enquanto, o SVELTE alcançou uma taxa em média de 4%. No cenário com nós móveis, Figura 6(b), a taxa de falsos positivos obtida pelo INTI é inferior a 30%, sendo que no SVELTE é de aproximadamente 39%. As detecções erradas podem acontecer quando alguns nós que reencaminham os pacotes de outros nós atrasam-se. Assim, momentaneamente eles são considerados *sinkhole*, porém conforme acontece a movimentação e a interação entre os nós, eles são identificados como nos bons.

5.2. Eficiência

As métricas da eficiência verificam o desempenho obtido pelo INTI, essas métricas são: E_{gc}, $Tx_{Entrega}$ e as funções assumidas pelos nós dentro da rede como: número de agrupamentos, número de líderes, número de associados, número de nós por líder e o número de nós solitários, a fim de determinar o desempenho do INTI para se adaptar às variações do ambiente. A métrica empregada para a avaliação do desempenho é o consumo de energia E_{gc}, como mostram os gráficos na Figura 7. No cenário fixo, o INTI apresenta um consumo de energia de 25000(mj), sendo menor ao consumo do SVELTE de 67000(mj),

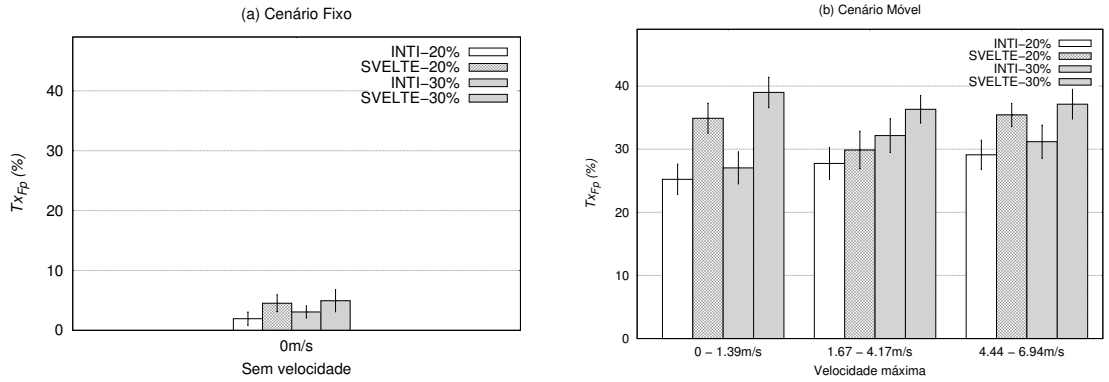

Figura 6. Tx_{Fp} do INTI e SVELTE diante de ataques sinkhole

como ilustrada na Figura 7(a). Em um cenário móvel, o INTI obtém quase o mesmo consumo que em um cenário fixo. Isto se deve à técnica usada pelo INTI permitindo a formação de agrupamentos para diminuir o consumo de energia e a escolha do nó associado como o maior índice de energia (*IE*). É interessante observar que o consumo de energia do SVELTE em um cenário móvel aumento para 75000(mj). Este aumento é devido à formação da topologia da rede no SVELTE, conforme o mostrado na Figura 7(b).

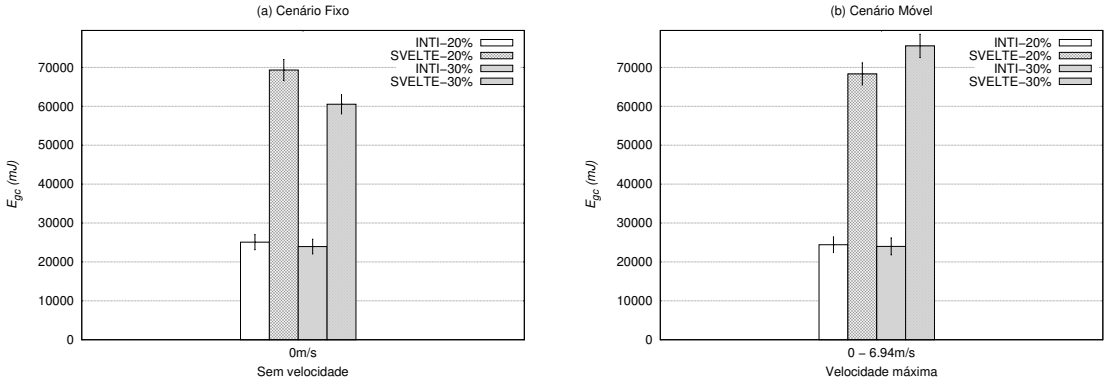

Figura 7. E_{gc} do INTI e SVELTE diante de ataques sinkhole

No cenário fixo, o SVELTE apresenta uma maior taxa de entrega $Tx_{Entrega}$ alcançando o 99% na entrega de dados da IoT, superando aos 95% alcançado pelo sistema INTI, como ilustrado no gráfico da Figura 8 (a). É possível também observar que o sistema INTI começa com uma taxa de entrega de 79% conseguindo aumentar 95%, essa variação é devido à pouca quantidade de nós dentro da área estabelecida. Desta forma, com o aumento da quantidade de nós a taxa de entrega aumenta. O gráfico da Figura 8 (b) apresenta só a avaliação do sistema INTI, já que o sistema SVELTE não permite a mobilidade dos nós. Este gráfico considera diferentes velocidades definidos anteriormente. Como pode-se apreciar o INTI no começo possui uma taxa de entrega superior a 55% mais conforme aumenta a quantidade de nós e a velocidade o INTI aumenta conseguindo alcançar uma taxa de entrega superior a 75%.

Outra métrica considerada é: **o número de agrupamentos, o número de líderes, o número de associados, o número de nós por líder e o número de nós solitários** A Figura 9 (a) ilustra a quantidade de agrupamentos, número de líderes, número de associados, número de nós por líder e o número de nós solitários calculados em um cenário fixo

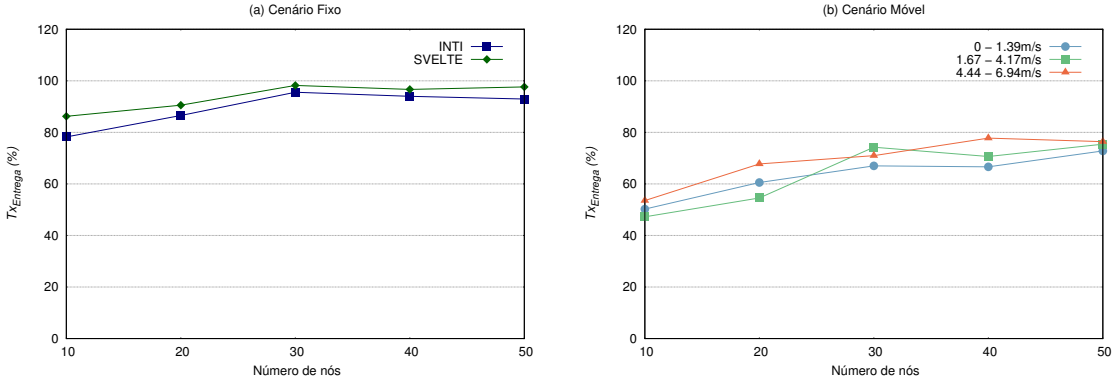

Figura 8. $Tx_{Entrega}$ do INTI e SVELTE

durante a simulação. No cenário móvel, o INTI apresenta uma redução na quantidade de nós que desempenham alguma função no encaminhamento de dados. Além disso, o número de nós solitários aumenta, como mostrado no gráfico da Figura 9 (b), isto é a causada da mobilidade dos nós. Sendo que estes nós movimentam-se dentro de uma área determinada, entrando e saindo dos agrupamentos formados.

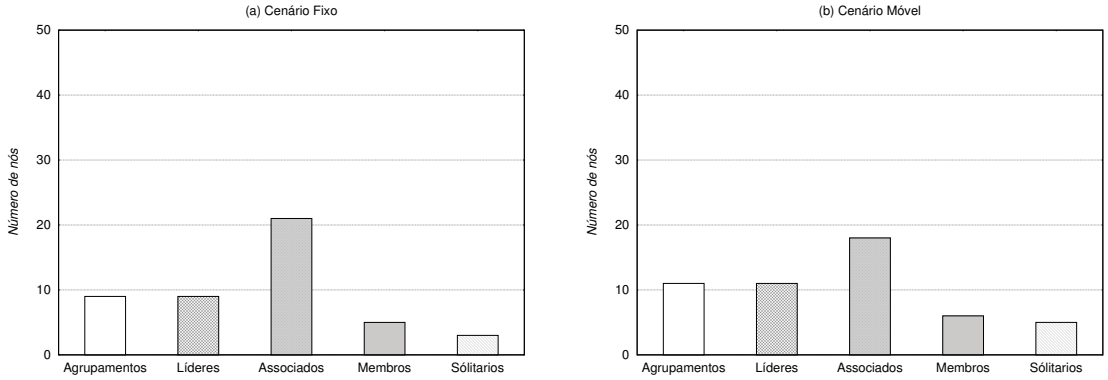

Figura 9. Funções assumidas pelos nós na IoT

6. Conclusão

Este artigo propôs o sistema INTI para a detecção e isolamento de ataques *sinkhole* na IoT. O INTI usa uma abordagem baseada no comportamento dos nós durante a transmissão das mensagens. Este comportamento é definido pela reputação e confiança de cada nó. O INTI foi avaliado em um cenário realístico para o uso da IoT, e os resultados obtidos mostram que ele alcançou uma taxa de detecção de ataques *sinkhole* de até 92% em um cenário com nós fixos e de 75% em um cenário com nós móveis. Além disso, o INTI apresentou um baixo consumo de energia e uma baixa taxa de falsos positivos e negativos em relação ao SVELTE. Como trabalhos futuros, avaliaremos a eficácia do INTI na detecção de outros tipos de ataques que acontecem na IoT.

Referências

Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. volume 54, páginas 2787–2805, Catania, Itália. Elservier Science Publishers B. V.

Bannack, A., da Silva, E., Lima, M. N., dos Santos, A. L., and Albini, L. C. P. (2008). Segurança em redes ad hoc. *Anais do XXVI Simpósio Brasileiro de Telecomunicaçoes (SBRT)*, páginas 19–20.

Bellavista, P., Cardone, G., Corradi, A., and Foschini, L. (2013). Convergence of MANET and WSN in IoT urban scenarios. volume 13, páginas 3558–3567. IEEE.

Dunkels, A., Gronvall, B., and Voigt, T. (2004). Contiki-a lightweight and flexible operating system for tiny networked sensors. páginas 455–462. IEEE.

Gaddour, O. and Koubâa, A. (2012). RPL in a nutshell: A survey. páginas 3163–3178. Elsevier.

Ganeriwal, S., Balzano, L. K., and Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 4(3):15.

Jin Qi, Tang Hong, K. X. L. Q. (2012). Detection and defence of sinkhole attack in wireless sensor network. In *ICCT-2012*, páginas 809–813, Chengdu, China. IEEE Security.

Kasinathan, P., Pastrone, C., Spirito, M. A., and Vinkovits, M. (2013). Denial-of-service detection in 6lowpan based internet of things. In *WiMob-2013*, páginas 600–607. IEEE.

Keally, M., Zhou, G., and Xing, G. (2010). Watchdog: Confident event detection in heterogeneous sensor networks. In *RTAS-2010 16th IEEE*, páginas 279–288. IEEE.

Korbi, I.E. Ben Brahim, M. A. C. S. L. (2012). Mobility enhanced RPL for wireless sensor networks. In *NOF-2012*, páginas 21–23. IEEE.

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

Moon, S. Y. and Cho., T. H. (2009). Intrusion detection scheme against sinkhole attacks in directed diffusion based sensor networks. In *IJCSNS*, páginas 118–122, Coreia. IEEE Computer Society.

Perez-Toro, C. R., Panta, R. K., and Bagchi, S. (2010). Rdas: reputation-based resilient data aggregation in sensor network. In *IEEE SECON-2010*, páginas 1–9. IEEE.

Raza, S., Wallgren, L., and Voigt., T. (2013). Svelte: Real-time intrusion detection in the internet of things. páginas 2661 – 2674, USA. Elservier.

Sedjelmaci, H. and Feham, M. (2011). Novel hybrid intrusion detection system for clustered wireless sensor network. In *International Journal of Network Security & Its Applications*.

Shafiei, H., Khonsari, A., Derakhshi, H., and Mousavi, P. (2014). Detection and mitigation of sinkhole attacks in wireless sensor networks. volume 80, páginas 644–653. Elservier.

Sheela, D., K. C. N. and Mahadevan., G. (2011). A non cryptographic method of sinkhole attack detection in wireless sensor networks. In *ICRTIT-2011*, páginas 527–532, Tamil Nadu, Chennai. IEEE Security.

Wahab, O. A., Otrok, H., and Mourad, A. (2014). A cooperative watchdog model based on dempster–shafer for detecting misbehaving vehicles. *Computer Communications*, 41:43–54.

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.

