Mitigação de Ataques no Roteamento em IoT Densa e Móvel Baseada em Agrupamento e Confiabilidade dos Dispositivos

Christian Cervantes[1], **Michele Nogueira**[1], **Aldri Santos**[1]

[1]Núcleo de Redes Sem-Fio e Redes Avançadas (NR2)
Universidade Federal do Paraná (UFPR)
Caixa Postal 19.081 – 81.531-980 – Curitiba – PR – Brazil

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

Abstract. *One of the challenges to the deployment of Dense and mobile IoT consists of its vulnerability to various routing attacks due to a variable infrastructure, distinct computing resources, and being an open network with heterogeneous mobile objects. Sinkhole and selective forwarding stand out among the most destructive attacks for unstructured networks. Although current intrusion detection systems (IDS) are a good countermeasure for protecting networks and data dissemination systems against IOT attacks, they still have a number of cost and performance constraints. This paper proposes an intrusion detection system against sinkhole and selective forwarding attacks on routing in dense and mobile IoT. The system, called Thatachi, takes into account clustering to deal with the devices density and mobility, and combines watchdog, reputation and trust strategies for detecting attacker in order to ensure the device reliability. A Thatachi's evaluation using the Cooja simulator has showed its effectiveness in mitigating both attacks and its low resource consumption.*

Resumo. *Entre os desafios à implantação da IoT está sua vulnerabilidade a várias formas de ataques de roteamento por possuir uma infraestrutura variável, recursos computacionais distintos, e ser uma rede aberta e com objetos heterogêneos móveis. Os ataques sinkhole e selective forwarding destacam-se entre os mais destrutivos aos sistemas em redes não estruturadas. Embora os atuais sistemas de detecção de intrusão (IDS) sejam uma boa contramedida de proteção das redes e sistemas de disseminação de dados contra ataques na IoT, eles possuem diversas restrições de custos e desempenho. Este artigo propõe um sistema de detecção de intrusão contra ataques sinkhole e selective forwarding sobre o roteamento na IoT densa e móvel. O sistema, chamado Thatachi, utiliza agrupamento para lidar com a densidade e a mobilidade, e combina estratégias de watchdog, reputação e confiança na detecção de atacantes, a fim de garantir confiabilidade aos dispositivos. A avaliação do Thatachi no simulador Cooja mostrou sua eficácia na mitigação dos ataques e seu baixo consumo de recursos.*

1. Introdução

A Internet das coisas (*do inglês, Internet of Things*) tem conectado uma gama de objetos físicos heterogêneos a Internet, através de tecnologias como RFID, GPS e NFC, entre outras. Essas objetos ("coisas") possuem características como identidades, atributos físicos o virtuais, e muitos deles são móveis e usam interfaces inteligentes para estabelecer

uma comunicação [Bari et al. 2013]. A aplicação da IoT em larga escala possui potenciais benefícios nas áreas de logística, processos industriais, segurança publica, domótica, monitoramento ambiental, entre outras [Borgia 2014, Zarpelão et al. 2017].

Contudo, a intensa interação entre os dispositivos inteligentes e a sua mobilidade expõem a IoT ainda mais a diversas vulnerabilidades na comunicação. Em geral, os ambientes de IoT densos de dispositivos móveis e fixos possuem uma infraestrutura variável, e uma grande parte desses dispositivos apresentam recursos computacionais limitados, como baixa energia, limitada capacidade de processamento, armazenamento, conexão através de links com perdas, entre outros [Atzori et al. 2010]. Logo, a IoT densa torna-se suscetível a inúmeras formas de ataques nos serviços de disseminação de dados, como o roteamento, buscando prejudicar a disponibilidade e confidencialidade das informações.

Entre as ameaças ao serviço de roteamento na IoT, e assim prejudicando a disseminação de dados, destacam-se os ataques *sinkhole* e *selective forwarding*, considerados os ataques mais destrutivos à camada de rede [Sheikhan and Bostani 2017]. Um atacante *sinkhole* busca atrair para ele a maior quantidade de tráfego de uma certa área a fim de prejudicar um ponto de coleta de receber os dados enviados pelos dispositivos de modo completo e correto [Lima et al. 2009]. Já um atacante *selective forwarding* seleciona e restringe os dispositivos para alcançar seu propósito malicioso e, portanto, alguns dispositivos não podem encaminhar o pacote de dados [Airehrour et al. 2017].

Os sistemas de detecção de intrusão (IDS) existentes na literatura e que oferecem segurança da IoT incluem diferentes métodos, mecanismos e técnicas para fornecerem confidencialidade, autenticação de dados, controle de acesso, privacidade e confiança entre usuários e coisas [Sicari et al. 2015]. Os IDS baseados em agentes, aprendizagem estatística ou de máquinas são comumente aplicados em redes pequenas, fixas e não utilizam dispositivos heterogêneos. Eles não são adequados ao contexto da IoT densa e móvel por gerar elevados consumos de recursos, e ainda tornam as redes IoT vulneráveis a diversas formas de ataques que visam interromper a comunicação da rede. Logo, faz se necessário o desenvolvimento de IDSs para IoT densa que lidem com a interligação dinâmica entre os dispositivos heterogêneos, ofereçam confiabilidade, e que consigam isolar a presença de atacantes no serviço de roteamento, protegendo a disseminação de dados.

Este trabalho apresenta um sistema para mitigação de ataques *sinkhole* e *selective-forwarding* no serviço de roteamento de redes IoT densas e móveis. Este sistema, chamado Thatachi (*De**T**ection of Sink**H**ole **A**nd Selec**T**ive-Forw**A**rding for Supporting Se**C**ure routing for Internet of T**HI**ngs*), busca detectar e isolar da rede dispositivos atacantes com comportamento *sinkhole* ou *selective forwarding*. O sistema utiliza roteamento baseado em agrupamento hierárquico para lidar com a densidade e a mobilidade dos dispositivos, e a fim de garantir confiabilidade entre os dispositivos, ele combina o uso de *watchdog* multinível, reputação e confiança na detecção dos atacantes. Uma avaliação e comparação do Thatachi no simulador Cooja mostrou sua eficácia na mitigação dos ataques, uma baixa taxa de falso positivos e negativos, e um baixo consumo de recursos.

O restante deste artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados. A Seção 3 detalha o modelo da rede IoT e o comportamento dos atacantes. A Seção 4 descreve o sistema Thatachi e detalha o funcionamento dos seus módulos e componentes. A Seção 5 apresenta a avaliação e os resultados obtidos pelo sistema na detecção de ataques. A Seção 6 apresenta as conclusões e os trabalhos futuros.

2. Trabalhos Relacionados

A importância da construção de IDSs cada vez mais sofisticados para atender as demandas de segurança na comunicação dos dados na IoT tem sido exaltada recentemente por diversos trabalhos na literatura [Cervantes et al. 2015, Sheikhan and Bostani 2017, Mathur et al. 2016, Thanigaivelan et al. 2016, Yang et al. 2017]. Em geral, o uso de IDS possibilita a identificação e a localização do atacante, bem como o seu comportamento [Sheikhan and Bostani 2017]. Particularmente, o serviço de roteamento tem sido o alvo mais comum dos atacantes na IoT devido à heterogeneidade dos dispositivos, onde se destacam os ataques *sinkhole* e *selective forwarding*.

Em [Le et al. 2016], os autores propuseram um IDS para a detecção de ataques *sinkhole* em uma rede baseada em RPL. Esta solução usa supernós distribuídos que geram uma máquina de estados finitos para o protocolo RPL. Os supernós monitoram os nós destinos através de solicitações decorrentes de regras aplicadas para verificação do monitoramento dos nós. Contudo, os resultados mostram altas taxas de verdadeiros positivos. Além disso, eles usam nós fixos e desconsideram o consumo de energia pelos supernós no sistema. Em [Sheikhan and Bostani 2017], os autores propuseram um IDS distribuído híbrido para a detecção em tempo real da ocorrência de ataques internos *sinkhole* e *selective forwarding* na 6LoWAPN. Este modelo baseia-se na abordagem MapReduce que usa um algoritmo OPF (*optimum-path forest*) supervisionado e um OPFC (*optimum-path forest clustering*) não supervisionado. Há também um mecanismo que detecta ataques cibernéticos (externos) à Internet. Este trabalho, no entanto, impõe uma alta taxa de falsos positivos e negativos. Em [Mathur et al. 2016], os autores propõem uma solução para a detecção dos ataques *blackhole* e *selective forwarding* numa WSN IoT médica, onde os sensores enviam amostra de dados para um ponto de acesso (AP). Esses APs são responsáveis por criptografar e encaminhar os dados através da Internet para armazenamento e processamento em servidores de modo a serem acessados pela equipe médica. Contudo, esta solução gera altas taxas de falsos positivos e negativos, e alto consumo de energia.

Um método tradicional aplicado no monitoramento dos componentes de um sistema é o uso de *watchdog* [Hasan and Mouftah 2017]. Os autores em [Yang et al. 2017] propõem um IDS baseado na detecção de anomalias usando *watchdog* para a detecção de ataques injeção de dados falsos. A ideia é aproveitar os dados coletados de vigilância ambiental da IoT para predizer eventos naturais urbanos. Assim, eles utilizam um modelo Hierárquico Bayesiano Espacial-Temporal (HBT) para descrever as características dos dados sensoriados. Em seguida, é empregada uma estratégia de decisão estatística baseada num teste de probabilidade sequencial para identificar um dispositivo atacante. Porém, o modelo HBT gera um alto consumo de energia e o teste probabilístico empregado assume uma margem de erro grande. Em [Sonar et al. 2016], os autores criaram um mecanismo de *watchdog* no hardware que monitora o vazamento do canal lateral do dispositivo e alerta ao usuário se um dado limiar é atingido, indicando que o hardware está vulnerável. Contudo, a solução é voltada para uma rede IoT com poucos dispositivos, e o uso de limiar também restringe a eficácia da detecção do ataque de canal lateral.

Em [Khan and Herrmann 2017], os autores propõem um IDS para a detecção de ataques *selective forwarding*, *sinkhole*, e de modificação do identificador das mensagens. Este IDS usa um mecanismo de gerenciamento de confiança que permite os dispositivos gerenciar informações de reputação sobre seus dispositivos vizinhos no contexto do do-

mínio da saúde. Porém, eles não mencionam os tipos de ataques que foram detectados e as taxas de falsos positivos e negativos são acima de 60%. Em [Cervantes et al. 2015], os autores propuseram um sistema para detecção e mitigação de ataques *sinkhole*. Neste sistema, os dispositivos estabelecem uma estrutura hierárquica para o encaminhamento dos dados e para o monitoramento da conduta dos dispositivos. Além disso, eles empregam mecanismos de reputação (distribuição Beta e teoria de Dempster-Shafer) e de confiança para identificação da honestidade entre os dispositivos. Logo, quando um nó detecta um ataque *sinkhole*, ele alerta os demais nós, isolando o atacante. Embora eficiente, a solução é voltada apenas aos ataques *sinkhole*, desconsiderando outros ataques no roteamento.

3. Modelo da Rede IoT e Comportamento dos Atacantes

Esta seção contextualiza a estrutura da rede IoT densa e móvel, o modelo de comunicação entre dispositivos (nós), e os ataques atuando no serviço de roteamento. Assume-se uma rede densa composta por nós heterogêneos, sendo alguns deles fixos e outros móveis. Além disso, o modelo de comunicação empregado assume uma comunicação intra-cluster e inter-clusters, estabelecida pelos agrupamentos dos nós, como ilustrado na Figura 1.

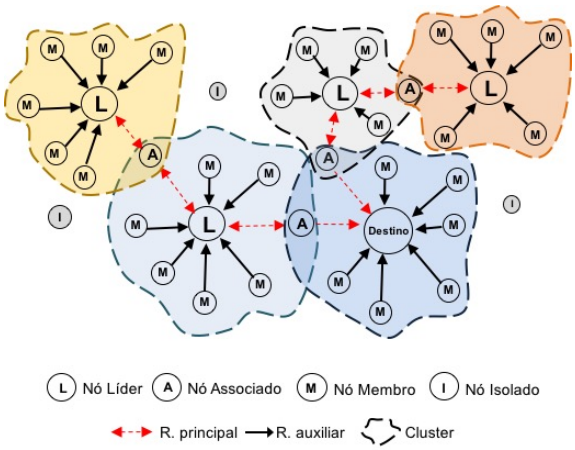


Figura 1. Configuração dos clusters

Modelo da rede: Corresponde a uma rede densa formada por um conjunto P de n dispositivos (nós) identificados por $\{n_1, n_2, n_3, ..., n_i\}$ onde $n_i \in P$. Cada nó n_i tem um endereço físico exclusivo que determina sua identificação (ID). A transmissão do nó ocorre através do meio sem fio mediante um canal assíncrono com perda de pacotes devido ao ruído e à mobilidade dos nós. Os nós são compostos de diferentes recursos, como tamanho da memória, armazenamento e bateria. Além disso, todos os nós atuam na mesma faixa de transmissão e formam parte do *cluster*. Todos os nós começam como nós isolados, e um nó pode ser isolado de duas maneiras: quando ele não consegue fazer parte de algum *clusters* ou quando ele é detectado como um nó atacante. Os nós na rede atuam na disseminação das informações como nós membros, associados e nós líderes. Os nós membros pertencem a um *cluster* e enviam suas informações aos nós líderes em intervalos de tempo. Os nós associados encaminham as informações e facilitam o roteamento de dados e a conexão entre diferentes *clusters*, atuando assim como uma "ponte" entre eles. Os nós líderes recebem informações dos nós membros e nós associados, que as enviam ao destino. A Figura 2 ilustra uma disseminação de dados na IoT.

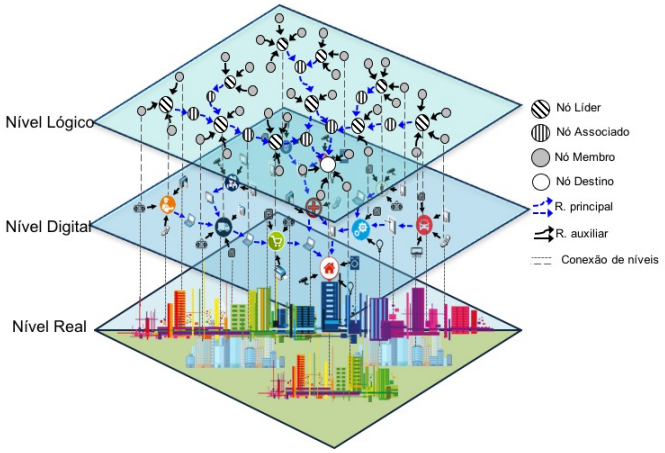


Figura 2. Modelo da IoT e disseminação da dados

Modelo de comunicação: Para a comunicação de dados, utiliza-se um protocolo de roteamento inspirado no RPL (*do inglês, IPv6 Routing Protocol for Low Power and Lossy Networks*) [Accettura et al. 2011], que considera tanto a densidade da rede e a mobilidade dos objetos (nós) quanto a formação de *cluster* provendo escalabilidade. Este protocolo de roteamento respeita as limitações dos objetos que compõem a IoT como energia, memória, processamento, entre outros. A rede possui dois tipos de roteamentos: o principal e o auxiliar. O roteamento principal (inter-cluster) estabelece a estrutura que permitirá a comunicação entre diferentes *clusters*, neste roteamento só intervém os nós líderes, associados e o nó destino alvo. O roteamento auxiliar (intra-cluster) compreende a comunicação de cada *cluster* feita pelo nó líder e seus membros. A vantagem desta estrutura simples de roteamento está numa comunicação organizada e efetiva sobre a rede densa, oferecendo um ganho de escalabilidade, estabilidade, e contribuindo assim para um melhor controle dos nós membros da rede.

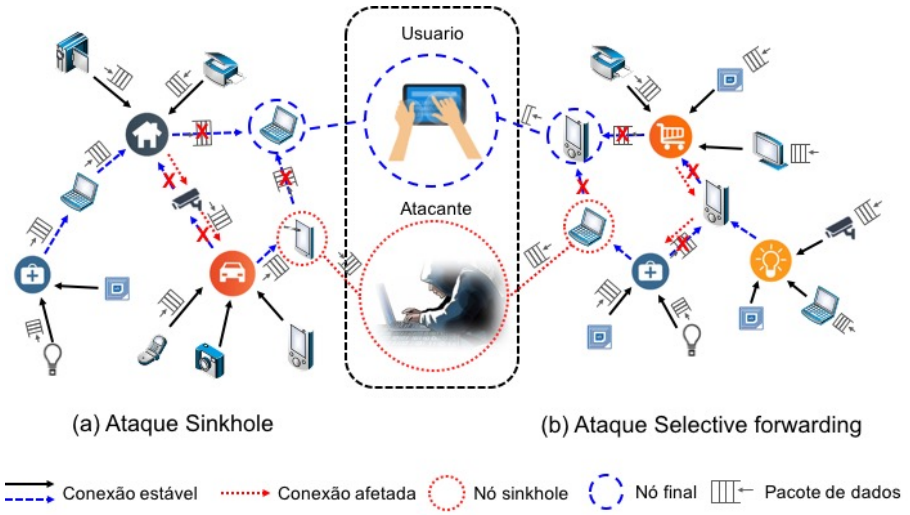


Figura 3. Ataque sinkhole e Ataque selective forwarding

Modelo dos ataques na rede: O *Ataque sinkhole* é um tipo de ataque de má-conduta que busca comprometer a confidencialidade e integridade na transmissão de dados. Este

ataque propaga aos dispositivos da rede que ele possui as melhores condições de recursos para auxiliar no encaminhamento dos dados. Assim, os pacotes de dados são naturalmente encaminhados ao dispositivo atacante *sinkhole*, tornando mais fácil, por exemplo, ao invasor acessar todo o conteúdo [Lima et al. 2009, Kamble et al. 2017], como ilustra a Figura 3(a). Já no *Ataque selective forwarding*, o dispositivo malicioso atua como um roteador primordial à transmissão dos dados. Neste ataque, o atacante pode optar por não repassar certos tipos de mensagem [Adat and Gupta 2017], como ilustra a Figura 3(b).

4. Thatachi

Esta seção descreve os detalhes do sistema de detecção de intrusão **Thatachi** (*DeTection of SinkHole And SelecTive-ForwArding for Supporting SeCure routing for Internet of THIngs*). A arquitetura do Thatachi compreende dois módulos principais, denominados **Agrupamentos** e **Confiabilidade**. O módulo Agrupamento configura a formação e a manutenção dos *clusters* e o módulo Confiabilidade cuida do monitoramento, detecção e isolamento de dispositivos atacantes atuando no roteamento dos dados. A Figura 4 ilustra a arquitetura do sistema.

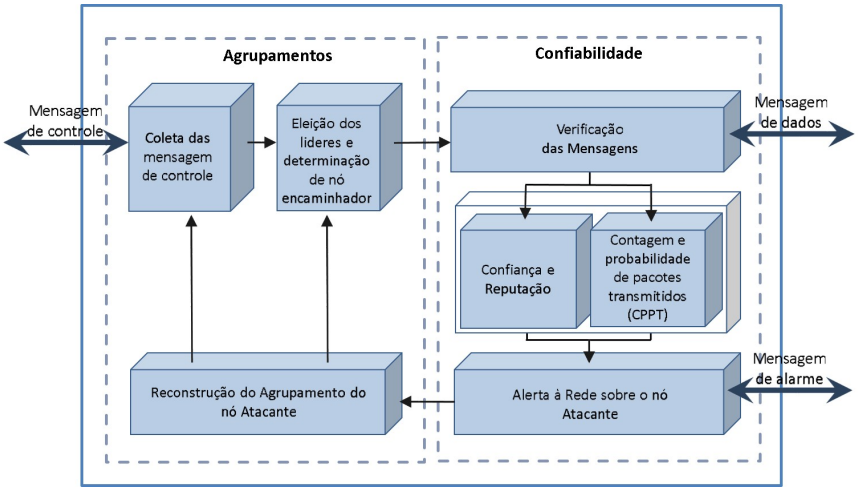


Figura 4. Arquitetura do IDS Thatachi

O **módulo agrupamentos**: é responsável pela configuração dos *clusters*. Ele consiste dos componentes *coleta de mensagens*, *eleição de lideres* e *associados*, e *reconstrução de clusters*. Ele atua na classificação dos nós como membros, associados e líderes, estabelecendo um caminho baseado em líderes e associados para oferecer escalabilidade e ampliar a vida útil da rede. A função atribuída ao nó é adaptável e muda ao longo do tempo com a reconfiguração da rede devido à mobilidade do nó ou um evento de ataque.

Inicialmente, os nós na rede começam como nós livres, coletando e transmitindo mensagem de controle em *broadcast*. Essas mensagens estimam a quantidade de nós vizinhos para a eleição dos líderes. Os nós livres são classificados como líderes quando eles têm a maior quantidade de nós vizinhos em relação aos outros. Após a eleição dos líderes, os outros nós livres classificados como nós membros formam os *clusters*. Em seguida, os líderes verificam se há nó membro que tenha recebido mensagens de outros lideres, e esse nó atuará como nó associado, visto que ele é capaz de interconectar diferentes *clusters*. Na existência de mais um nó membro na mesma área, assume-se como nó associado aquele

com o maior quantidade de energia (*QE*), determinado por: $QEi = \frac{TEr_i}{TEc_i}$, onde TEr_i é o total de energia restante do nó n_i e TEc_i o total de energia consumida pelo mesmo nó.

A reconstrução dos agrupamentos ocorre quando (i) um dos nós naturalmente falha; (ii) abandona o *cluster*; ou (iii) quando ocorre um ataque. Se um nó membro é afetado por alguns destes problemas, o nó líder remove o ID deste nó de sua lista, e os demais nós membros podem-se reagrupar em outros *clusters* vizinhos. Se um nó líder falha ou abandona o *cluster*, os nós membros e associados solicitam uma nova eleição de nó líder. Se um nó líder é o atacante, os nós membros e associados realizam uma nova configuração dos *clusters*. Quando um nó associado falha ou abandona o *cluster*, há a possibilidade do líder escolher outro nó como associado, desde que ele esteja dentro da área comum compartilhada por diferentes *clusters*. Sendo que o líder remove o ID deste nó de sua lista de vizinhos. Se o nó associado é um atacante, o nó líder propaga uma mensagem de reconstrução para que os nós afetados realizem uma nova configuração dos *clusters* e o nó líder superior coloca o identificador de nó atacante numa lista negra (*blacklist*). Caso contrario, se ambos os líderes estão dentro do mesmo raio de transmissão, ocorre uma fusão dos *clusters*. Assim, o *cluster* que possuir a maior quantidade de nós membros absorverá o outro. Este método tem como objetivo minimizar o número de líderes do roteamento principal e prover a escalabilidade da rede.

O **módulo confiabilidade**: garante a segurança e a confiabilidade entre os nós que formam a rede IoT. Ele consiste de três componentes responsáveis pelo monitoramento, detecção e isolamento dos dispositivos atacantes. O componente *Monitoramento* verifica o comportamento dos nós em relação ao encaminhamento dos dados recebidos. Ele emprega uma combinação de estratégias *watchdog* em dois níveis. Assim, o nó monitor calcula o número de transmissões encaminhadas por um nó "superior" em relação à sua própria mensagens. Um nó é dito superior se ele possui um classificação mais baixa. Assim, se a quantidade de transmissões recebidas for igual ao número de transmissões de saída, o nó é definido como um nó normal. Caso contrário, o nó monitor assume que está acontecendo algum desvio do comportamento normal, como ilustrado na Figura 5.

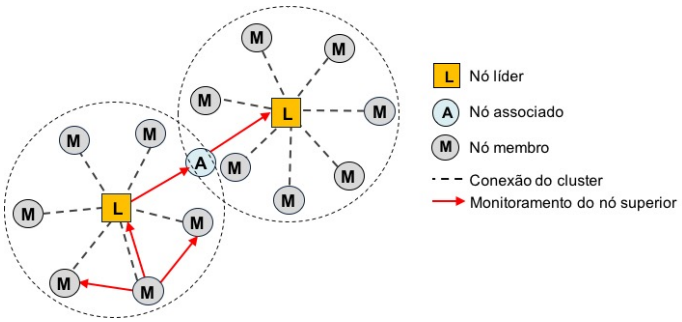


Figura 5. Monitoramento do roteamento

O componente *Detecção* emprega reputação e confiança para a detecção dos nós *sinkhole* ou *selective forwarding*. A reputação é a crença ou percepção que os nós estabelecem por iterações, ações ou troca de informações entre eles. Assim, três predições são calculadas: incerteza (*u*), crença (*b*) e descrença (*d*), usando a distribuição *Beta* (α,β) para representar a reputação do nó. Todos os nós executam esses cálculos. O cálculo dessas previsões $(u, b, d) \in (0, 1)^3 : u + b + d = 1$, respectivamente. O valor da incerteza (*u*) é a variância normalizada da distribuição *Beta*, que é calculada de acordo com:

$u = \frac{12*\alpha*\beta}{(\alpha+\beta)^2*(\alpha+\beta+1)}$. O valor da certeza é $(1-u)$, que pode ser dividido em *b* e *d* de acordo com sua quantidade de iterações. Já a transmissão de confiança de dois nós é definida por $\frac{\alpha}{(\alpha+\beta)}$. O cálculo de *b* é dado por: $b = \frac{\alpha}{(\alpha+\beta)}(1-u)$. Finalmente, o cálculo da descrença (d) é alcançado por: $d = (1-u) - b = \frac{\beta}{(\alpha+\beta)}(1-u)$.

Após o cálculo das previsões, considera-se as iterações e previsões de comunicação computadas com base no *status* que é enviado pelo nó membro ao seu líder. Cada nó propaga seu estado (*Es*) em seu **comportamento na transmissão de mensagens** para o cálculo de reputação. Esses valores são dados de entrada para aplicar a *theory Dempster-Shafer* [Tang 2015] e aumentar a probabilidade de detecção e reduzir falsos alarmes. A reputação é um valor contínuo dentro dos limites P[0,1], se o valor da reputação for maior ou igual a 0.5, o nó é "*bom*", e caso contrário, ele é um "*invasor*". O valor da reputação é dado por $m_1(H) \oplus m_2(H)$ variando um valor contínuo entre $0 \leq m_2 \leq 1$. Este resultado considera $m_2 < 0,5$ como uma má reputação, e do contrário, m_2 tem uma boa reputação.

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

O próximo passo estabelece o cálculo da Confiança (*C*), que consiste na relação de honestidade que uma entidade tem com outra. A Equação 2 obtém o valor de confiança de um nó, que varia entre [0,1]. Se este valor for superior a 0.5, assume-se o nó como "*bom*"; Caso contrário, ele é um "*invasor*".

$$
C = \frac{u\gamma + R + 1}{u\gamma + R + u\delta + (1-R) + 2} \tag{2}
$$

Já na detecção do ataque *selective forwarding* determina-se o limite de detecção d_{thresh} baseado no CPPT (Contagem e Probabilidade de Pacotes Transmitidos), que consiste no número esperado de transmissões de dados necessárias para entregar com sucesso um pacote de um remetente ao receptor, incluindo as retransmissões. O CPPT de um link baseia-se nas relações de entrega direta e reversa do link. A relação de entrega direta, d_f, é a probabilidade medida de que um pacote de dados seja entregue com sucesso no receptor, e a relação de entrega reversa, d_r, é a probabilidade do pacote de confirmação ser recebido com sucesso pelo remetente. Assim, o CPPT de um link é calculado como: $CPPT = \frac{1}{(d_f \times d_r)}$. O inverso do CPPT corresponde ao índice de entrega do link. O limite de detecção d_{thresh} de uma rota é calculado como o inverso da soma de CPPT de todos os links *i* ao longo do caminho *p*. $d_{thresh} = \frac{1}{\sum_{linki \in p} CPPT_i}$ e $AR = N \times d_{thresh}$ onde, *AR* é a taxa de aceitação e *N* é o número de pacotes transmitidos pelo nó de origem.

Um nó atacante *sinkhole* ou *selective forwarding* pode atuar na rede como nó líder, nó associado ou nó membro. O Algoritmo 1 detalha a detecção dos atacantes dentro

da rede diante da presença de uma suspeita. Neste algoritmo, *DetecRepConf (l.1)*, recebe os valores do <ID, Es> do nó encaminhador detectado como nó suspeito para determinar se ele é um nó bom (normal) ou um nó atacante. Estes valores são baseados em seu comportamento na transmissão de mensagens. Assim, o nó que detectou o nó suspeito utiliza suas próprias observações (valores) definidas em *(l.2-4)* no cálculo da reputação. Além disso, são utilizadas as observações próprias do nó definida por *c* e o valor da qualificação do nó suspeito (Es) *(l.5)*. Em seguida, calcula-se a confiança do nó suspeito *(l.9)*. O sistema assume o nó como atacante se ele possui uma reputação e confiança abaixo de [0.5]; logo ele não encaminhará as informações enviadas pelos demais nós *(l.10)*.

Algoritmo 1 Detecção de nós atacantes

1: **procedimento** DETECREPCONF(id,Es)
2: $i \Leftarrow uncertainty \leftarrow \{af, bta\}$ ▷ cálculo das predições do nó observador
3: $c \Leftarrow belief \leftarrow \{af, bta\}$
4: $d \Leftarrow disbelief \leftarrow \{af, bta\}$
5: $DetecRep \Leftarrow m \leftarrow \{c, Es\}$ ▷ calcula a reputação considerando a crença(c) e o estado (Es) do encaminhador
6: $u \Leftarrow 1 - (1/IteRations[Root]$
7: $Gma \Leftarrow (u * Gma) + DetecRep$
8: $Dlta \Leftarrow (u * Dlta) + (1 - DetecRep)$
9: $Trust \Leftarrow (Gma + 1)/(Gma + Dlta + 2)$ ▷ calcula a confiança do nó suspeito
10: **se** $(DetecRep > 0.5) \wedge (Trust > 0.5)$ **então** ▷ verificação do nó suspeito
11: $InKlin \Leftarrow$ "*good*"
12: **senão**
13: $InKlin \Leftarrow$ "$sinkhole$"
14: **fim se**
15: **retorna** $InKlin$ ▷ retorna o valor da suspeita
16: **fim procedimento**
17: **procedimento** DETECSELECFORREPCONF(df,dr)
18: $CPPT \Leftarrow 1/(df * dr)$
19: $D \Leftarrow 1/(CPPT_a + CPPT_b)$
20: $AR \Leftarrow N * D$
21: **se** $(AR > C_{pkt})$ **então** ▷ verificação do nó suspeito
22: $InKlin1 \Leftarrow$ "$selectiveforwarding$"
23: **senão**
24: $InKlin1 \Leftarrow$ "*good*"
25: **fim se**
26: **retorna** $InKlin1$ ▷ retorna o valor da suspeita
27: **fim procedimento**

O componente *Isolamento do Atacante* atua nas ações para isolar o nó atacante e refazer os *clusters*. Assim, um nó que detecta um ataque *sinkhole* ou *selective forwarding* gera e propaga uma mensagem de alarme a fim de alertar os nós vizinhos. Em seguida, ele também promove o isolamento do atacante ao enviar uma mensagem de restauração aos seus vizinhos. Os dados principais propagados na mensagem de restauração consiste na classificação do *cluster*, de modo que nós do mesmo grupo comecem um reagrupamento. Há três maneiras de isolar os atacantes *sinkhole* ou *selective forwarding*: (i) se o atacante é um nó membro, o próprio líder isolará esse nó; (ii) se o nó atacante atua como líder, os nós membros isolam o nó atacante ou se houver um nó associado, este isolará o ataque; (iii) caso o nó atacante atua como nó associado, ele será isolado pelo nó líder com a maior classificação, rompendo assim a comunicação com o atacante. É importante verificar se há dentro do *cluster*, outros nós associados com a classificação mais baixa, tal que eles possam encaminhar mensagens ao nó de destino. Caso contrário, o líder propagará uma mensagem de restauração aos seus membros tal que eles busquem os *clusters* vizinhos.

5. Avaliação

Esta seção apresenta uma avaliação do sistema Thatachi para analisar sua eficácia e eficiência na mitigação de ataques *sinkhole* e *selective forwarding* sobre o roteamento de IoT Densa. O Thatachi foi comparado ao sistema INTI, desenvolvido para mitigar principalmente ataques *sinkhole* [Cervantes et al. 2015]. Ambos os sistemas foram implementados no simulador Contiki-Cooja, um sistema operacional de código aberto [Dunkels et al. 2004]. O funcionamento de ambos os sistemas foram aferidos num cenário simulado de 50 nós, sendo eles nós fixos e móveis, e que foram distribuídos aleatoriamente numa área de 200x200 m. Embora o cenário seja simplificado, ele é efetivo para representar uma área de IoT densa, à medida que espera-se que os dispositivos estabeleçam agrupamentos interligados onde as informações são encaminhadas a um ponto de acesso conectado a uma rede estruturada. Os resultados mostrados são a média de 35 simulações e intervalo de confiança de 95%. A Tabela 1 apresenta os parâmetros aplicados nas simulações. Já as métricas usadas para medir a eficácia e eficiência de ambos os sistemas são: Taxa de detecção de ataque (T_{dt}), Taxa de falsos positivos (Tx_{fp}), Taxa de falsos negativos (Tx_{fn}), Taxa de entrega de pacotes (Tx_{Ep}), e consumo de energia (E_{gc}).

Tabela 1. Configurações da simulação

Parâmetros	Valores
Número de nós	50
Tempo de simulação	1500s
Velocidades	5 km/h, 15 km/h e 25 km/h
Tempo de pausa do nó	60s, 90s e 120s
Área	200x200 metros
Tipo de pacote utilizado	UDP
Tempo para gera pacote de dados	10s
Padrão	IEEE 802.15.4
Canal sem fio	Unit disk graph Medium (UDGM)
Radio de transmissão	20s, 30s e 40s
Número de nós atacantes	20% e 30%
Taxa de dados	10^2 kbps

Taxa de detecção do ataque: (T_{dt}) contabiliza os ataques identificados corretamente pelo sistema. Ela é obtida pela Eq. 3, onde *X* é o total de iterações, i.e. encaminhamento de dados dos nós atacantes, dado na forma de *X = (d, c)*, em que *d* é o número de detecções feitas pelo sistema e *c* é a autêntica condição do nó $n_i \in R$.

$$T_{dt} = \frac{\sum D_i}{|X|} \forall_i \in X \quad \text{onde} \quad D_i = \begin{cases} 1, & \text{se} \quad d_i = c_i, \\ 0, & \text{se} \quad d_i \neq c_i. \end{cases} \tag{3}$$

Taxa de Falsos negativos: (Tx_{fn}) calcula o percentual nós intrusos falsamente identificados como não intrusos. Ela é obtida pela Eq. 4, onde *X* é o total de iterações, i.e. encaminhamento de dados no sistema, e T_{det} a taxa de detecção do ataque.

$$Tx_{fn} = |X| - T_{dt} \tag{4}$$

Taxa de Falsos positivos: (Tx_{fp}) indica o número de nós não intrusos que foram falsamente identificados como intrusos. A Tx_{fp} é calculada pela Eq. 5, em que *Z* é o conjunto das iterações dos nós normais, na forma *Z = (d, c)*, onde *d* representa o valor da detecção feita pelo sistema 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.

$$Tx_{fp} = \frac{\sum Dp_i}{|Z|} \forall_i \in Z \quad \text{onde} \quad Dp_i = \begin{cases} 1, & \text{se} \quad d_i = 1, \\ 0, & \text{se} \quad d_i \neq 0. \end{cases} \tag{5}$$

Taxa de entrega de pacotes: (Tx_{Ep}) indica o total de pacotes de dados recebidos com sucesso, i.e. o nº de pacotes recebido no destino dividido pelo nº de pacotes emitidos na origem, Eq. 6.

$$Tx_{Ep} = \frac{NpacotesRecibidos}{NpacotesEnviados} X100 \tag{6}$$

Consumo de energia: (E_{gc}) calcula o total do consumo de energia dos nós da rede gasto na simulação. Este cálculo é obtido pela Eq. 7, onde $\sum_{z=1}^{i} TE_i$ é o somatório total da 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 o consumo energético pelo sistema.

$$E_{gc} = \sum_{z=1}^{i} (TE_i - TE_r) \tag{7}$$

5.1. Resultados

A Figura 6 mostra a capacidade de detecção e mitigação obtida pelos sistemas Thatachi e INTI. O Thatachi obteve uma taxa de detecção (T_{dt}) de 96%, inclusive alcançando algumas vezes uma taxa de 100% para ambos os ataques. Esta efetividade alcançada pelo Thatachi deve-se as estratégias de confiabilidade implementadas de *watchdog*, reputação e confiança entre os dispositivos. Embora o sistema INTI tenha obtido uma boa taxa de detecção, 95% para o cenário com ataques *sinkhole*, ele não obteve uma boa taxa na detecção do ataque *selective forwarding*, chegando a ter uma taxa inferior aos 35%.

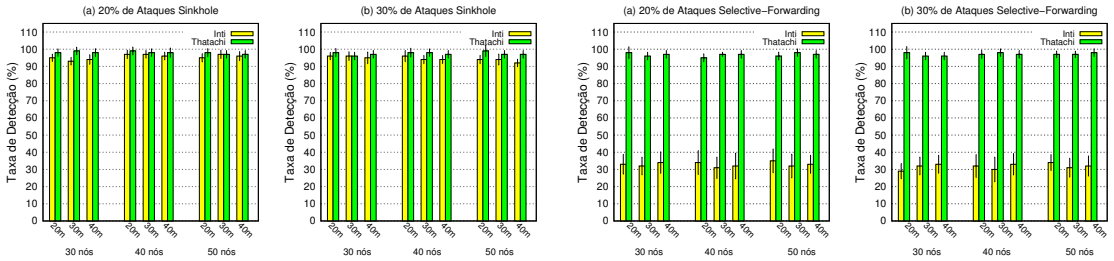
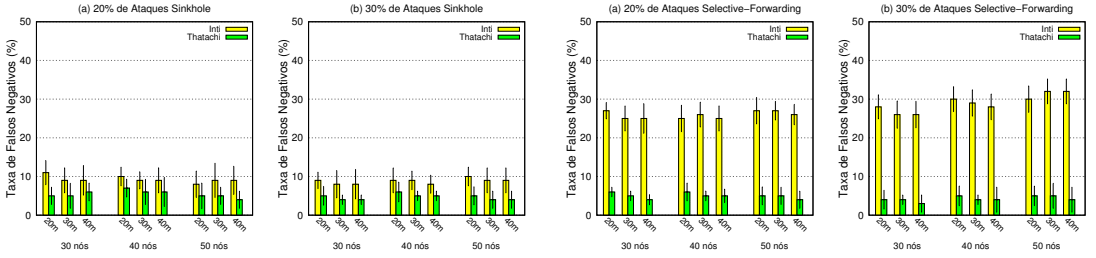


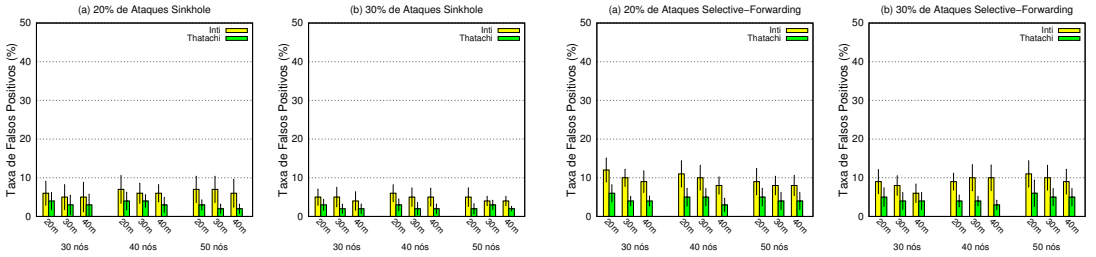
Figura 6. Taxa de detecção (T_{det}) para os ataques sinkhole e selective forwarding

A Figura 7 mostra o desempenho de ambos os sistemas quanto as taxas de falsos negativos (Tx_{fn}) e positivos (Tx_{fp}) na presença de ambos os ataques. O Tathachi obteve uma taxa de falsos negativos menor que 5% para ambos ataques. Isso significa que poucos nós atacantes não são detectados. A falha na detecção de um atacante pode acontecer quando há um erro no calculo feito pelo nó inferior quanto a quantidade de pacotes transmitidos pelo nó superior. Dessa forma, alguns nós demoram na identificação dos atacantes. Por outro lado, o INTI obteve uma taxa de falsos negativos superior a 8% no *sinkhole* chegando até alcançar uns 20% no *selective forwarding*, como ilustrado nas Figuras 7(a) e 7(b). Isto deve-se porque o INTI não consegue observar quando um atacante descarta todos os pacotes. Em relação as taxas de falsos positivos, Figuras 7(c)

e 7(d), o Thatachi obteve uma taxa inferior a 3% para ambos ataques e o INTI obteve uma taxa que vai de 5% até 12%. As detecções erradas do Thatachi ocorrem quando os nós encaminhadores demoram a reencaminhar os pacotes. Assim, momentaneamente eles são considerados como atacantes, porém à medida que ocorre a movimentação e o encaminhamentos de pacotes, eles são identificados como nos bons.



(a) FN sinkhole (b) FN selective forwarding



(c) FP sinkhole (d) FP selective forwarding

Figura 7. Taxa de falsos negativos e positivos para os ataques sinkhole e selective forwarding

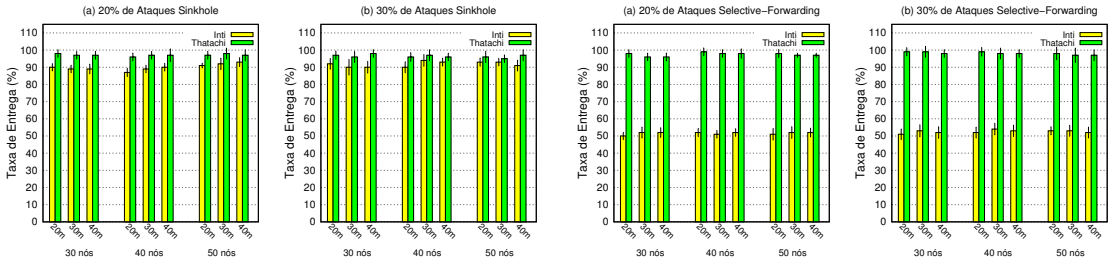


Figura 8. Taxa de entrega (Tx_{Ep}) com ataques sinkhole e com selective forwarding

O Thatachi obteve uma taxa alta de entrega (Tx_{Ep}) de quase 99% na presença de ambos os ataques, superando os 95% alcançados pelo INTI nos ataques *sinkhole* e os 54% nos ataques *selective forwarding*, como ilustrado nos gráficos da Figura 8. O ganho com o Thatachi deve-se as técnicas aplicadas a fim de aumentar a confiabilidade e o tempo de vida dos dispositivos. O custo energético E_{gc} de ambos os sistemas é apresentado nos gráficos na Figura 9. Observa-se que o INTI consome maior quantidade de energia na presença de ambos os ataques, obtendo um consumo superior a 29000(mJ) com os ataques *sinkhole* e um consumo superior a 33000(mJ) com ataques *selective forwarding*. Já o consumo energético do Thatachi foi inferior aos 20500(mJ) tanto na presença de ataques *sinkhole* quanto de ataques *selective forwarding*. Isto deve-se a técnica usada pelo Thatachi permitindo a formação de agrupamentos para diminuir o consumo de energia.

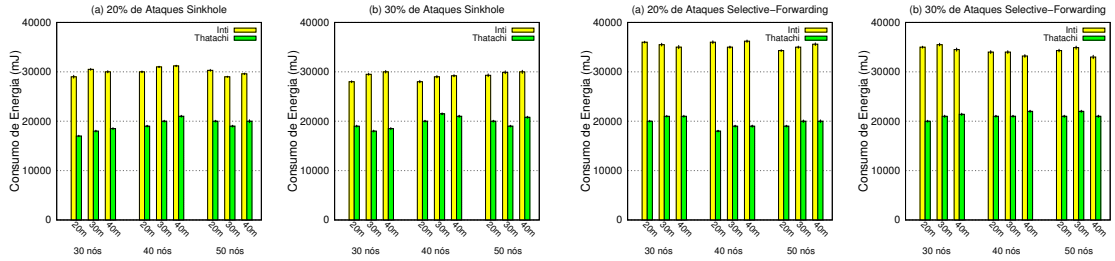


Figura 9. Consumo de energia (E_{gc}) para os ataques sinkhole e selective forwarding

6. Conclusões

Este trabalho propôs o sistema Thatachi para mitigação de ataques no roteamento de dispositivos de redes IoT densa e móvel. O Thatachi consegue lidar com a densidade e mobilidade da rede por empregar uma estrutura de agrupamento no encaminhamento dos dados. Além disso, ele monitora o comportamento dos nós no encaminhamento dos dados, tal que aqueles não confiáveis possam ser analisados sobre a sua confiabilidade, e isolados do serviço de roteamento da rede em caso de má conduta. Resultados obtidos por simulação mostraram a eficácia do Tathachi na detecção de nós atacantes sinkhole e selective forwarding e na garantia da transmissão dos dados; além de uma baixa taxa de falso positivos e negativos, e uma baixo consumo energéticos pelos dispositivos. Como trabalhos futuros pretende-se analisar os ataques de personificação no serviço de roteamento na IoT, bem como propor uma solução para mitigá-los.

Referências

[Accettura et al. 2011] Accettura, N., Grieco, L. A., Boggia, G., and Camarda, P. (2011). Performance analysis of the rpl routing protocol. In *Mechatronics (ICM), 2011 IEEE International Conference on*, pages 767–772. IEEE.

[Adat and Gupta 2017] Adat, V. and Gupta, B. (2017). Security in internet of things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, pages 1–19.

[Airehrour et al. 2017] Airehrour, D., Gutierrez, J., Ray, S. K., et al. (2017). A trust-aware rpl routing protocol to detect blackhole and selective forwarding attacks. *Australian Journal of Telecommunications and the Digital Economy*, 5(1):50.

[Atzori et al. 2010] Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15):2787–2805.

[Bari et al. 2013] Bari, N., Mani, G., and Berkovich, S. (2013). Internet of things as a methodological concept. In *Fourth International Conference on Computing for Geospatial Research and Application (COM. Geo), 2013*, pages 48–55. IEEE.

[Borgia 2014] Borgia, E. (2014). The internet of things vision: key features, applications and open issues. *Computer Networks*, 54:1–31.

[Cervantes et al. 2015] Cervantes, C., Poplade, D., Nogueira, M., and Santos, A. (2015). Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things. In *IFIP/IEEE International Symposium on Integrated Network Management (IM) 2015*, pages 606–611. IEEE.

[Dunkels et al. 2004] Dunkels, A., Gronvall, B., and Voigt, T. (2004). Contiki-a lightweight and flexible operating system for tiny networked sensors. In *29th Annual IEEE International Conference on Local Computer Networks, 2004*, pages 455–462. IEEE.

[Hasan and Mouftah 2017] Hasan, M. M. and Mouftah, H. T. (2017). Optimization of watchdog selection in wireless sensor networks. *IEEE Wireless Communications Letters*, 6(1):94–97.

[Kamble et al. 2017] Kamble, A., Malemath, V. S., and Patil, D. (2017). Security attacks and secure routing protocols in rpl-based internet of things: Survey. In *International Conference on Emerging Trends & Innovation in ICT (ICEI), 2017*, pages 33–39. IEEE.

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

[Le et al. 2016] Le, A., Loo, J., Chai, K. K., and Aiash, M. (2016). A specification-based ids for detecting attacks on rpl-based network topology. *Information*, 7(2):25.

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

[Mathur et al. 2016] Mathur, A., Newe, T., and Rao, M. (2016). Defence against black hole and selective forwarding attacks for medical wsns in the iot. *Sensors*, 16(1):118.

[Sheikhan and Bostani 2017] Sheikhan, M. and Bostani, H. (2017). A security mechanism for detecting intrusions in internet of things using selected features based on mi-bgsa. *Int. Journal of Information & Communication Technology Research*, 9(2):53–62.

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

[Sonar et al. 2016] Sonar, S., Roy, D. B., Chakraborty, R. S., and Mukhopadhyay, D. (2016). Side-channel watchdog: Run-time evaluation of side-channel vulnerability in fpga-based crypto-systems. *IACR Cryptology EPrint Archive*, 2016:182.

[Tang 2015] Tang, H. (2015). A novel fuzzy soft set approach in decision making based on grey relational analysis and dempster–shafer theory of evidence. *Applied Soft Computing*, 31:317–325.

[Thanigaivelan et al. 2016] Thanigaivelan, N. K., Nigussie, E., Kanth, R. K., Virtanen, S., and Isoaho, J. (2016). Distributed internal anomaly detection system for internet-of-things. In *13th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2016*, pages 319–320. IEEE.

[Yang et al. 2017] Yang, L., Ding, C., Wu, M., and Wang, K. (2017). Robust detection of false data injection attacks for the data aggregation in internet of things based environmental surveillance. *Computer Networks*.

[Zarpelão et al. 2017] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., and de Alvarenga, S. C. (2017). A survey of intrusion detection in internet of things. *Journal of Network and Computer Applications*.