CHRISTIAN ALONSO VEGA CERVANTES

UM SISTEMA DE DETECÇÃO DE ATAQUES SINKHOLE SOBRE 6LOWPAN PARA INTERNET DAS COISAS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.

Orientador: Prof. Aldri Luiz dos Santos
Coorientadora: Profa. Michele Nogueira Lima

CURITIBA

2014

CHRISTIAN ALONSO VEGA CERVANTES

UM SISTEMA DE DETECÇÃO DE ATAQUES SINKHOLE SOBRE 6LOWPAN PARA INTERNET DAS COISAS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.

Orientador: Prof. Aldri Luiz dos Santos
Coorientadora: Profa. Michele Nogueira Lima

CURITIBA

2014

C419s Cervantes, Christian Alonso Vega
Um sistema de detecção de ataques sinkhole sobre 6LoWPAN para Internet das Coisas/ Christian Alonso Vega Cervantes. – Curitiba, 2014.
94 f. : il. color. ; 30 cm.

Dissertação - Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-graduação em Informática, 2014.

Orientador: Aldri Luiz dos Santos – Co-orientador: Michele Nogueira Lima.
Bibliografia: p. 78-89.

1. Sistemas eletrônicos de segurança. 2. Redes de computadores. 3. Interconexão em rede (Telecomunicações). I. Universidade Federal do Paraná. II.Santos, Aldri Luiz dos . III. Lima, Michele Nogueira . IV. Título.

CDD: 003.72

DEDICATORIA

Este trabalho é dedicado a minha família, aos amigos do Perú, aos amigos do grupo de pesquisa NR2 e a comunidade acadêmica.

AGRADECIMENTOS

Gostaria de começar agradecendo a Deus por sempre me ajudar em tudo. Agradeço aos meus pais, José e Juana por sempre apoiar-me, de maneira direta e indireta, deram apoio em minhas atividades acadêmicas, só posso disser os quero muito. Agradeço aos meus irmãos José Luis e Marco Antonio, por ser minha inspiração de luta na vida. Valeu brothers!.

Agradeço ao professor, orientador de mestrado e de vida Aldri Luiz dos Santos pelos anos de trabalho, pelos muitos ensinamentos, pela confiança em min. Agradeço por sua serenidade, compreensão, por seus conselhos e pelo incrível poder de me deixar sempre calmo e mais confiante em mim mesmo. Agradeço à professora Michele Nogueira pelos muitos ensinamentos, pela amizade e entusiasmo.

Agradeço aos amigos e irmãos (brothers) do grupo NR2 e não membros. Ao meu brother Robson Gomes (Robinho) pela ajuda constante. O Ricardo Tombesi (bulbasaur), pelas dicas. O Júlio, pela ajuda e fazer que viva está experiência. O Danilo (Chico) e o Alisson (Beavis), pelas loucuras e o grande humor (ohh bichos doidos). O Claudio, o Jorge da floresta, pelo reggae. O Rodrigo, o filinho, pelos conselhos. O Adi, o micheline, pelas conversas em espanhol. O Benavid e o Thiago (salsicha), pelos conselhos e pelas conversas. O Metuzalen, o ursinho, pela amizade sincera. O Diego, pela ajuda na pesquisa. O Leonardo, pelos momentos de piadas no laboratório. O Fernando, o naufrago, pelas dicas para melhorar meus trabalhos. A Elisa pela ajuda e amabilidade em todo. O Douglas, pela seriedade em todo.

Por outro lado, não posso deixar de agradecer a meus brothers da baia. O Luciano e Juliano, pelas lições em japonês kampai brothers!. O Miguel, o cachorrão, pela conversação que me fizeram sentir como em casa. O Thiago, o Ivan drago e o Jeovan, o chassis, pelas saídas noturnas em lugares inesperados. Agradeço a todas as pessoas que conheci no Brasil e desculpem se esqueço de alguém. Também quero agradecer à CAPES pela bolsa que possibilitou meu estudo com dedicação integral, e ao PPGinf pela minha aceitação no curso de mestrado. Muito obrigado a todos por tudo.

RESUMO

A *Internet das coisas* (IoT) é fruto de uma revolução tecnológica que representa o futuro da computação e da comunicação, sendo identificada como uma das tecnologias emergentes que mudará nossa forma de vida. As redes IoT são formadas por objetos heterogêneos (nós) com alguma inteligência, isto é, com capacidade de processamento que lhes permitem, entre outras tarefas, enviar e receber informações através da rede. Entretanto, cada vez mais objetos estarão interligados com aparelhos digitais, veículos e demais, e a presença deles tende a crescer em nossas vidas trazendo mais comodidade e facilidade. A IoT ligará todos esses objetos, assim como ligará outros que não pertencem à computação podendo ser fixos ou móveis. Visto que os objetos que compõem a IoT possuem recursos limitados, estes se tornarão vulneráveis a vários tipos de ataques, sendo o ataque *sinkhole* um dos mais destrutivos nas redes. Contudo, as soluções existentes para a proteção e segurança contra os ataques *sinkhole* geram um elevado consumo de recursos e usam mecanismos complexos para garantir um bom desempenho. Desta forma, este trabalho propõe um sistema de detecção de intrusão, chamado de INTI (*Detecção **I**ntrução contra ataques Si**N**khole sobre 6LoWPAN para a Interne**T** das Co**I**sas*) para identificar a presença de ataques *sinkhole* no serviço de roteamento na IoT. Além disso, INTI visa mitigar os efeitos adversos encontrados em IDSs que perturbam o seu desempenho como falsos positivos e negativos, também como os elevados consumos de recursos. O INTI combina o uso dos mecanismos como o uso de *watchdog*, reputação e confiança. O mecanismo de *watchdog* possibilita o monitoramento das atividades dos outros nós durante o encaminhamento de pacotes. A reputação e a confiança colaboram para determinar os dispositivos considerados confiáveis e não confiáveis na rede IoT. Estes mecanismos são utilizados para a detecção de ataques *sinkhole*, analisando o comportamento dos dispositivos. O sistema INTI foi avaliado em dois cenários realísticos de IoT, e nesses cenários os resultados obtidos mostram a eficácia do INTI em termos de taxa de detecção de ataques, o número de falsos negativos e falsos positivos e da eficiência na taxa de entrega, na latência e no consumo de energia.

Palavras-chave: IDS, IoT, segurança, proteção, ataques sinkhole, watchdog, reputação.

ABSTRACT

The Internet of Things (IoT) is the result of a technological revolution that represents the future of computing and communication, being identified as one of the emerging technologies that will change our way of life. The IoT networks are formed by heterogeneous objects (nodes) with some intelligence, that is, with processing capabilities that enable them, among other tasks, send and receive information across the network. However, more and more objects are interconnected with digital devices, vehicles and other equipment, and their presence tends to grow in our lives bringing more convenience and ease. The IoT will connect all of these devices as well as bind other objects that do not belong to the digital world and that can be fixed or mobile. Since the objects that make up the IoT have limited resources, they become vulnerable to various attacks, and the sinkhole attack is one of the most destructive in the networks. However, existing solutions for the protection and security against sinkhole attacks generate a high consumption of resources and use complex mechanisms to ensure good performance. Thus, this dissertation proposes an intrusion detection system, called INTI (intrusion detection against sinkhole attacks on 6LoWPAN for IoT), to identify the presence of sinkhole attacks on the routing services in IoT. Moreover, INTI aims to mitigate adverse effects found in IDS that disturb its performance, suck as false positive and negative as well as the high resource cost. The INTI system combines the use of mechanisms such as watchdog, reputation and trust. The watchdog mechanism enables the monitoring the activities of other nodes for packet forwarding. The reputation and trust mechanisms collaborate to determine the devices considered reliable and unreliable in IoT network.These mechanisms are used for detection of attackers, by analyzing the behavior of devices. The INTI system was evaluated in two realistic scenarios of IoT, and these scenarios the results show the effectiveness of INTI in terms of attack detection rate, the number of false negatives and false positives and efficiency in the delivery rate, latency and energy consumption.

Keywords: IDS, IoT, security, safety, sinkhole attacks, watchdog, reputation.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

IoT	Internet of Things
IDS	Intrusion Detection System
MIT	Massachusetts Institute of Technology
EPC	Eletronic Product Code
ITU	International Telecommunication Union
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
IP	Internet Protocol
3G	Third Generation of Mobile Telecommunications Technology
M2M	Machine-to-machine
GPS	Global Positioning System
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
RSSF	Wireless Sensor Networks
RFID	Radio Frequency Identification
NFC	Near Field Communication
UDP	User Datagram Protocol
RPL	IPv6 Routing Protocol for Low Power and Lossy Network

NOTAÇÃO

P	Conjunto de nós
n_i	Identificação de um nó na rede
IE	Índice de energia
TEr	Total de energia restante
TE	Total de energia
TEc	Total de energia consumida
St	Comportamento de nó na transmissão de mensagens
$Beta(\alpha, \beta)$	Distribuição Beta
$Beta(p\|\alpha, \beta)$	Função densidade de probabilidade
(α, β)	Iterações de um nó
R	Reputação
(i, c, d)	Predições incerteza, crença e descrença
$n_i : \Omega\{T, \overline{T}\}$	Possibilidades de suspeita do nó
$H = T$	Hipóteses do nó ser bom
$\overline{H} = \overline{T}$	Hipóteses do nó ser atacante
K	Normalização das crenças
C	Confiança do nó
γ, δ	Atualização das iterações
u	Fator de confiança
m	Número de iterações do nó

CAPÍTULO 1

INTRODUÇÃO

Hoje em dia, vivemos em um mundo em que a Internet é adotada não só por pessoas, mas também por dispositivos com alguma inteligência, isto é, com uma capacidade computacional que lhes permitem, entre outras tarefas, enviar e receber informações através da rede. Com os avanços das tecnologias e a redução das dimensões dos dispositivos computacionais, estes se tornaram mais acessíveis e mais disponíveis ao público em geral. Baseado nesses avanços, surgiu a ideia da **Internet das coisas** (IoT, do inglês, *Internet of the Things*) [1], considerada um dos pilares da Internet do Futuro [2].

A Internet das coisas (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 [3, 4, 5]. Entretanto, essas coisas **objetos** possuem características como mobilidade, identidades, atributos físicos e usam interfaces inteligentes para estabelecer uma comunicação [6]. Desta forma, o objetivo da IoT é possibilitar a integração e a unificação de todos os objetos e sistemas de comunicação que nos cercam.

Existem vários ambientes onde a IoT é aplicada, como em construções e escritórios inteligentes, no transporte, na saúde, na segurança e na indústria. Estes ambientes são classificados de acordo com o tipo de rede disponível, a cobertura de alcance, a escalabilidade, a heterogeneidade e a participação do usuário [7]. Países como os Estados Unidos, onde a polícia de Nova Iorque conta com uma sala de situação com o objetivo de monitorar a segurança da cidade; o Brasil, com o centro de operações do Rio de Janeiro; a Suécia, com o projeto de redução do congestionamento em Estocolmo [8].

No futuro, cada vez mais objetos conversarão sem a interação do ser humano, e deixando de ser apenas provedores de informação [9]. Para isso, a IoT demanda o uso da tecnologia 6LoWPAN, que tem como base o protocolo IPv6 [10], no aumento do **espaço de endereçamento**, suportando um número maior de dispositivos endereçáveis e permitindo a autoconfiguração. A tecnologia 6LoWPAN possibilita o uso da internet em dispositivos inteligentes, visto que ela possibilita o transporte dos pacotes IPv6 sobre redes sem fio de baixo consumo de energia, mais especificamente sobre redes IEEE 802.15.4 [11]. Além disso, esta tecnologia permite ter um melhor controle da grande quantidade de dispositivos da rede.

Dentre os desafios existentes na IoT destaca-se a necessidade de oferecer **mecanismos**

de **proteção** e de **segurança** confiáveis para a rede [12]. Com o aumento dos dispositivos inteligentes e a **mobilidade** de alguns destes, a IoT é 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 [3]. Em razão das características, a IoT trona-se vulnerável a diversas formas de ataques de roteamento [13]. Dentre esses tipos de ataques na IoT, destaca-se o ataque *sinkhole* [14], que é um ataque ativo sendo considerado uns dos ataques de roteamento mais destrutivos para as redes sem fio. O objetivo de um atacante ativo é interromper o funcionamento da rede, comprometendo assim a **confiabilidade** e a **integridade** das informações [4]. Além disso, a IoT herda as mesmas vulnerabilidades que a internet, como a necessidade de garantir a robustez, a confiabilidade, a confidencialidade, a integridade e a escalabilidade.

Particularmente, a **mobilidade** dos nós os tornam mais vulneráveis a ataques de roteamento, por não apresentar alguma infraestrutura fixa. Além disso, os dispositivos que compõem a IoT podem possuir limitações de recursos de computação e de capacidade energética [15, 16], o que os tornam mais vulneráveis. Devido a essas limitações de recursos, soluções muito complexas não são implementadas dentro da IoT.

Uma contramedida muito utilizada para a detecção de adversários nas redes são os sistemas de detecção de intrusão [17]. Um sistema de detecção de intrusão (IDS) tenta garantir a sobrevivência e a existência de uma rede robusta e confiável [18]. Nesse sentido, os IDSs são essenciais no fornecimento de serviços confiáveis na IoT, visto que eles são usados para detectar várias anomalias e comportamentos maliciosos que podem comprometer a robustez e a confiabilidade de uma rede. O uso destes sistemas proporciona vantagens à detecção de um atacante, maior confiabilidade entre os dispositivos pertencentes à rede, menor consumo de recursos garantindo uma rede segura.

1.1 Problema

Claramente, a Internet das coisas será mais suscetível a ataques do que a Internet tradicional [19], devido à forma em que ela é organizada, ao meio de comunicação sem fio e as limitações dos recursos que possuem os dispositivos, como baixa energia, limitada capacidade de processamento, armazenamento, conexão através de links com perdas e outras características [3]. Por estas razões, a IoT torna-se vulnerável a diversas formas de ataques [13]. Esses ataques são classificados de várias formas: ataques externos ou internos, ataques passivos ou ativos ou por comprometer um host ou uma rede [20]. Alguns desses ataques são de falsificação (*spoofing*), informação alterada ou reproduzida (*replaying*), encaminhamento seletivo (*selective forwarding*), ataque sumidouro (*sinkhole*), ataque de personificação (*sybil*) e outros [21, 22, 23].

Dentre esses tipos de ataques na IoT, se destaca o ataque ***sinkhole***, que é considerado uns dos ataques de roteamento mais destrutivos para as redes sem fio. O *sinkhole* é empregado por um dispositivo atacante [24, 25, 14], com o objetivo de atrair a maior quantidade de tráfego de certa área prejudicando um ponto de coleta, como a estação-base, de receber os dados completos e corretos dos nós [26]. No ataque *sinkhole*, um dispositivo atacante se manifesta de modo **atraente** para os demais dispositivos da rede no encaminhamento do tráfego de uma determinada região. Em seguida, este dispositivo descarta pacotes ou encaminha apenas alguns pacotes à estação-base. Este comportamento malicioso pode inclusive resultar na negação de serviços (*DoS*) nas aplicações da IoT.

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) [27, 28, 29, 30, 31, 32]. Estes trabalhos são classificados como contramedidas de prevenção ou de detecção. Trabalhos como [27, 29] aplicam métodos e técnicas para a prevenção do ataque. Para isso, eles empregam métodos criptográficos, de distribuição e gerenciamento de chaves, e de métodos de autenticação. Os trabalhos como [28, 32, 31, 30, 33] utilizam mecanismos de detecção, conseguindo identificar o ataque na rede. Esses mecanismos são baseados: no uso de abordagens estáticas, em regras, no uso de *watchdog*, em agentes móveis e outras abordagens. Portanto, estas soluções geram outros problemas para a rede denominados *efeitos adversos*, como elevadas taxas de falsos positivos e falsos negativos, elevado consumo de energia, baixo desempenho do sistema, entre outros.

Entretanto, poucas pesquisas têm sido desenvolvidas para a proteção e a segurança da IoT na transmissão de informação [34, 35, 36], e estes trabalhos são inadequados para um funcionamento dinâmico porque não consideram a mobilidade dos dispositivos, sendo isso fundamental para seu uso das por pessoas e objetos. Porém, para resolver esses problemas é necessário o uso de métodos ou mecanismos mais simples, porém eficazes, com a finalidade de obter o resultado desejado. Outro problema dos métodos de detecção desenvolvidos até o momento é que eles são apenas capazes de detectar atividades muito pontuais [28, 29, 31], não identificando o vínculo existente entre essas atividades.

Portanto, é preciso desenvolver um sistema de detecção de intrusão para a IoT que garanta a proteção e o isolamento de ataques *sinkhole*, assim como oferecer uma solução que seja dinâmica, auto-organizada e auto-reparável. Auto-organizada para identificar a origem da ameaça em tempo real. Auto-reparável quando ocorre uma falha, quando os nós se movem fora do agrupamento ou quando é detectado um adversário na rede. Essas características são encontradas nos sistemas de reputação, sendo estes considerados um componente importante de qualquer sistema de segurança contra as ameaças.

1.2 Objetivos

Este trabalho tem como objetivo prevenir, detectar e isolar a presença de ataques *sinkhole* dentro do serviço de roteamento da IoT, e ao mesmo tempo evitar que a solução proposta tenha *efeitos adversos*. Para alcançar este objetivo, é proposto um Sistema de *Detecção de**I**ntrução contra ataques Si**N**khole sobre 6LoWPAN para a Interne**T** das Co**I**sas*, denominado INTI. No desenvolvimento do sistema, deverão ser propostos métodos e técnicas que permitam a continuidade do funcionamento normal da IoT, mesmo durante a ocorrência de um ataque sobre o serviço de roteamento.

O método proposto tem como base o comportamento do nó, em que os nós monitoram e avaliam os nós que se encontram próximos de acordo com o próprio comportamento observado ou mediante as observações feitas por outros. Desta forma, o comportamento do nó permite a identificação das atividades dos nós dentro da rede possibilitando determinar quando uma atividade é normal ou ataque. Os dispositivos são considerados bons quando o comportamento segue o padrão da rede, e são considerados maus quando diferem do esperado. Além disso, os nós atacantes devem ser isolados não participando do serviço de roteamento da rede.

Pesquisas relacionadas ao tema de segurança mencionam que um cenário de ameaças exige a detecção de ataques em tempo real a partir de uma inteligência coletiva sobre alguma entidade, e que atue com critério nessas informações [37, 38]. Entre as técnicas existentes para determinar o comportamento de um nó é considerada uma opinião maioritária baseada na reputação e na confiança do nó [39]. Com a reputação, pode-se determinar se um nó apresenta um bom ou mau comportamento dentro da rede. O sistema de reputação apresenta características importantes como a alta precisão, a rápida convergência, a adaptação dinâmica aos nós da rede, entre outras características [40]. Ele tem sido normalmente empregado para apoiar decisões em diversos serviços de computação e comunicação em redes de modo a garantir um bom desempenho e evitar a participação de nós de má conduta [41, 42, 43].

1.3 Contribuições

Este trabalho apresenta as seguintes contribuições:

- Um estudo sobre os métodos e mecanismos contra os ataques *sinkhole* existentes na literatura. Estes métodos e mecanismos foram classificados em contramedidas de prevenção e contramedidas de detecção. Com tal estudo foram levantados os requisitos desejáveis para um sistema de detecção de intrusão (IDS) contra ataques *sinkhole* para a IoT.

- A proposta e especificação do Sistema INTI (*Detecção de **I**ntrução contra ataques*

*Si**N**khole sobre 6LoWPAN para a Interne**T** das Co**I**sas*), um sistema que provê proteção e segurança à IoT. A arquitetura do INTI está organizada em quatro módulos: o módulo configuração dos agrupamentos, o módulo de monitoramento do encaminhador, o módulo de detecção de atacante e o módulo de isolamento de atacante. Juntos permitem detectar e isolar o ataque da rede para que esta siga funcionando de maneira normal.

- A especificação do sistema INTI combina o uso de diferentes técnicas inspiradas no comportamento de cada dispositivo, para a detecção de ataques *sinkhole*. Foi também implementado um protocolo que permite a formação de agrupamentos, além de permitir a mobilidade dos dispositivos da rede para, assim, aproximar à realidade.

- A avaliação do sistema INTI diante os ataques *sinkhole*. A avaliação mostrou que o sistema proposto provê uma melhora considerável na detecção do ataque *sinkhole*. Desta forma, o sistema proposto foi capaz de detectar e isolar os ataques *sinkhole* aumentando o desempenho da rede e diminuindo o consumo de recursos e portanto reduzindo os *efeitos adversos*.

1.4 Estrutura da dissertação

Esta proposta de dissertação está organizada da seguinte forma. O capítulo 2 apresenta os fundamentos relacionados à Internet das coisas necessários no entendimento do problema tratado neste trabalho e da solução proposta. Ele também detalha os ataques que exploram as vulnerabilidades das IoT, sobretudo o ataque *sinkhole*, e explica os conceitos relacionados aos sistemas de detecção. O capítulo 3 apresenta os trabalhos mais relevantes encontrados na literatura que abordam questões de mecanismos de detecção, métodos de reputação e confiança. O capítulo 4 descreve o sistema INTI, que tem como base o comportamento dos dispositivos na detecção do ataque *sinkhole*. Esse capítulo detalha o funcionamento do sistema e de seus elementos. O capítulo 5 apresenta a análise de desempenho realizada, avaliando um cenário móvel, o sistema INTI e comparado com outro IDS. Por fim, o capítulo 6 conclui apresentando as conclusões e direções futuras.

CAPÍTULO 2

FUNDAMENTOS

Este capítulo apresenta os fundamentos relacionados à Internet das coisas (IoT), que são importantes no entendimento do problema tratado neste trabalho e da solução proposta. A Seção 2.1 contextualiza as características da IoT e descreve suas aplicações no mundo real. A Seção 2.2 detalha a arquitetura da IoT e as camadas que a compõem. Na Seção 2.3, são apresentadas as principais tecnologias da IoT. A Seção 2.5 apresenta os requisitos de segurança na IoT. A Seção 2.6 descreve os benefícios da tecnologia 6LoWPAN e as vulnerabilidades, que acontecem na tecnologia 6LoWPAN dentro da IoT. A Seção 2.7 contextualiza o ataque *sinkhole*, descreve as medidas de defesa existentes na literatura e apresenta os requisitos para evitar ataques *sinkhole* na IoT.

2.1 Internet das coisas

A Internet das coisas (IoT, do inglês *Internet of Things*) é fruto de uma revolução tecnológica que representa o futuro da computação e da comunicação. A ideia da IoT foi apresentada pelo centro Auto-ID no Instituto Tecnológico de Massachusetts (MIT, do inglês *Massachusetts Institute of Technology*) em 1999 [44, 45]. Do mesmo modo, com especial destaque dos fundadores Kevin Ashton e David L. Brock, que introduziram a ideia no contexto da gestão [46, 47]. Além disso, a IoT ganhou esse nome porque parte do conceito de um objeto é utilizar um Código Eletrônico de Produto (EPC, do inglês *Eletronic Product Code*) [48]. A IoT foi considerada a terceira onda na indústria global da internet no ano de 2009 e catalogada como uma visão do futuro no ano de 2010 [49].

As redes da IoT são consideradas redes híbridas, abertas e heterogêneas que integra dispositivos inteligentes chamados de coisas *things*, como livros, eletrodomésticos e chave, entre outros objetos que não pertencem à computação interatuando com computadores, GPS, sensores, e outros dispositivos. Estes dispositivos buscam compartilhar informações, a fim de obter uma rede de gerenciamento simultânea e inteligente [49]. Sendo definida como uma rede que pode conectar todas as coisas [50]. A miniaturização e a nanotecnologia dentro das coisas ou dispositivos inteligentes permitem que a informação a ser processada, decisões e respostas para os dados possam ser feitos. Desta forma, a IoT é vista como um dos pilares da internet do futuro [2].

Com a Tecnologia da Informação e Comunicação (TIC), espera-se uma mudança no paradigma do estilo atual da comunicação, isto é, de humano-humano e humano-coisa para coisa-coisa [51]. Deste modo, os sistemas permitiram ter controle e acesso total aos outros sistemas para fornecer comunicações, com o objetivo de uma interação total,

não somente de celulares, computadores, televisores, sensores típicos, mas também de dispositivos como mesa, cadeira, chaveiro, geladeira, caneta, agenda, um medidor de eletricidade, uma peça de automóvel, entre outros itens ou objetos que não pertencem à computação, a fim de que estes objetos interajam de maneira autônoma. Esses objetos possuem características especiais como identidades, atributos físicos e usam interfaces inteligentes para comunicar-se [52]. Além disso, estes objetos (nós) possuem limitações dos recursos como baixa energia, limitada capacidade de processamento, rádio de curto alcance, limitada capacidade de armazenamento, conexão através de links com perdas e outras características [3].

A IoT está se desenvolvendo rapidamente e ganhando força no mundo. Do mesmo modo, ela tem uma ampla gama de aplicações na vida real, como ilustrado na Tabela 2.1. Algumas destas aplicações, encontramos no transporte, na logística, na saúde, para monitorar e coletar informações sobre a cidade [3], além de oferecer diversas funções, tais como a identificação, a localização, o rastreamento, o monitoramento [8]. Estas aplicações e serviços são usualmente oferecidos por terceiros.

Rede	**Aplicação**	**Exemplos**
Sensoriamento	Monitoramento do mundo físico e coleta de dados	Segurança nas ruas, temperatura, humidade, fauna, floresta e outras
Industrial	Melhoras da qualidade do produto	Telecomunicações, medica e saúde, transporte, farmacêuticas.
Civil	Monitoramento cidadão	Comercial, veicular e doméstica, shooping, estacionamentos, casas
Resgate	Comunicação no ambiente de resgate e coleta de dados	Tsunamis, desastres naturais.
Militar	Comunicação no campo de guerra	Aviso de ataques

Tabela 2.1: Aplicações da IoT

Cada vez mais novos objetos se comunicaram entre si, sem a interação do ser humano, e assim deixando de ser só provedores de informação, entretenimento e tornando-se algo maior do que a internet tradicional [9]. No entanto, estes objetos requereram o uso de mais endereços IP como o uso do IPv6 [53, 10], para identificar cada nó e ter um melhor controle da rede IoT. O protocolo 6LoWPAN permite o roteamento de pacotes IPv6 na rede 6LoWPAN (IPv6 baixo consumo de energia 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. Sendo que a implementação em larga escala da IoT seja uma realidade.

2.2 Arquitetura da IoT

A arquitetura da IoT é formada por três camadas principais, denominadas de camada sensitiva ou perceptual, camada de rede e, por último, a camada de aplicação. Através desta arquitetura, os usuários facilmente trocam informações entre o mundo virtual e o mundo físico, fazendo uso de serviços inteligentes. A Figura 2.1 ilustra a arquitetura da IoT definida pela China Mobile [54].

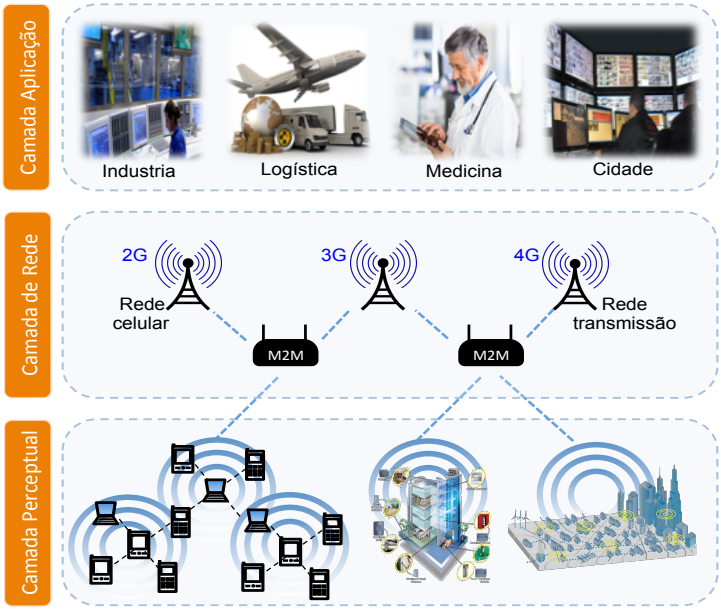

Figura 2.1: Arquitetura da IoT

Camada Sensitiva ou Perceptual

Considerada a base da IoT, a **camada sensitiva ou perceptual** tem como funções principais o reconhecimento e a coleta de informações. Desta forma, cada objeto (nó) possui um identificador único dentro da IoT e a coleta de informação identifica os dados enviados pelos objetos através da rede. Esses objetos são: de uma rede de sensores sem fio (RSSF) tradicional, de sistemas RFID, de celulares 3G ou 4G, GPS, de dispositivos embarcados, de código de barras e de elementos de controle final. Após a fase de reconhecimento e coleta, a informação é transmitida para a camada de rede. A transmissão é feita através dos dispositivos de acesso, por exemplo, através de gateways e sensores, terminal M2M ou terminal portátil. Esta camada é a origem da IoT.

Camada de Rede

A **camada de rede** é composta por diversas redes de comunicação e redes integradas baseada na internet. Estas redes são baseadas em IPv4 ou IPv6, por exemplo, as redes

móveis, as redes sem fio e vários tipos de redes privadas. Em seguida, cria-se uma grande rede inteligente. A principal característica desta camada é a transmissão da informação entre longas distâncias. Além disso, esta camada deve gerenciar e controlar os dados massivos em tempo real para reorganizá-los, filtrá-los e integrá-los de modo que eles sejam transformados em algum serviço.

Camada Aplicação

A principal função da **camada aplicação** consiste da descoberta dos serviços para o usuário final. Esta camada tem como objetivo integrar todas as funções das camadas inferiores e fornecer vários serviços específicos e inteligentes para os usuários finais da IoT. A questão-chave desta camada é o compartilhamento de informações e segurança da informação [55]. A camada de aplicação é o alvo final no desenvolvimento da IoT, por exemplo, construção de aplicações típicas para o monitoramento da ecologia, a preservação de relíquias culturais, o transporte inteligente, a agricultura de precisão, a logística da empresa, as casas inteligentes, entre outros serviços.

2.3 Tecnologias da IoT

Esta seção apresenta as tecnologias utilizadas na IoT e detalha as características principais dos dispositivos que possibilitam o desenvolvimento da IoTs.

2.3.1 Rede de sensores sem fio

As Redes de Sensores Sem Fio (RSSFs, do inglês *Wireless Sensor Networks*), compreendem uma *tecnologia emergente* que está em evolução contínua [56, 57]. Uma RSSF consiste de centenas ou milhares de pequenos dispositivos (nós) com capacidades de sensoriamento, processamento, armazenamento dos dados coletados do ambiente real e transmitidos pelo meio sem fio [58]. As RSSFs possuem características especiais como: fluxo de dados predominantemente unilateral, topologia dinâmica, grande número de elementos, recursos computacionais limitados, tendem a serem autônomas e requerem um alto grau de cooperação podendo ser organizadas em grupos [59]. Esses tipos de redes são homogêneas ou heterogêneas em relação aos tipos de dimensões e funcionalidades dos nós. Cada nó que compõe as RSSFs é composto de bateria, rádio, processador, memória, sendo a bateria o componente crítico para este tipo de rede já que ela representa o armazenador de energia [60]. Ademais, estas redes são comumente utilizadas em regiões de difícil acesso, onde o ser humano não pode ingressar de forma fácil [61]. Essas redes são utilizadas em diferentes aplicações, tais como militares, ambientais, de saúde, entre outras [62, 63, 64]. As RSSFs são consideradas fundamentais para o progresso da IoT [65], já que elas têm a capacidade de agir com autonomia para coletar os dados capturados do ambiente.

2.3.2 Identificador por radiofrequência

A Identificação por Radiofrequência (RFID, do inglês *Radio Frequency Identification*) é uma tecnologia de comunicação sem fio de *identificação automática e captura de dados* (AIDC) [66], tendo sido inventada pelo exército inglês na Segunda Guerra Mundial [67]. Esta tecnologia utiliza indução eletromagnética ou propagação eletromagnética permitindo identificar em tempo real objetos ou pessoas [68, 69].

Os dispositivos que compõem as redes RFID são etiquetas RFID, o leitor RFID e os servidores. As etiquetas RFIDs são pequenos microchips projetados para transmissão de dados sem fio. Este microchip pode ser tão pequeno que alguns podem chegar a $0{,}4mm^2$ [70]. Essas etiquetas são classificadas em ativas e passivas. As *etiquetas ativas* têm sua própria bateria para fornecer energia, normalmente têm um maior poder de computação e alcance de transmissão maior do que as etiquetas passivas. Ao contrário, as *etiquetas passivas* não possuem bateria, elas são alimentadas pelo leitor, por conseguinte, o poder de computação é menor, mas a diferença é que operam em qualquer banda de frequência. As etiquetas RFID transmitem os dados através do ar, em resposta a interrogatório por um leitor RFID.

O *leitor* RFID permite reconhecer e detectar a presença da etiqueta RFID e ler sua informação; esta leitura não precisa ter alguma linha de visão para a transferência de dados, não requerendo o contato físico [71]. Estes leitores têm duas interfaces: a primeira é uma interface de RF (radiofrequência) que se comunica com as etiquetas, a fim de recuperar a identidade destas. A segunda é uma interface de comunicação geralmente IEEE 802.11 ou 802.3 para comunicar com os servidores [69]. Finalmente, o último componente são os *servidores* que armazenam as informações fornecidas pelos leitores RFID.

Desta forma, esta tecnologia supera as limitações de outros métodos de coleta de dados manuais, por exemplo, os códigos de barras. As principais razões porque a tecnologia RFID têm sido estudada nos últimos anos são suas próprias características, como alta capacidade de armazenamento, tamanho pequeno e longa vida útil. A tecnologia RFID é empregada em muitas aplicações como na manufatura, na saúde, no transporte, na logística, na indústria. Assim, o RFID será universal para rastrear objetos, produtos, animais, remessas e até seres humanos [72]. Contudo, são várias as preocupações neste tipo de tecnologia, como a segurança e privacidade [73, 74, 75].

2.3.3 Comunicação de campo próximo

A Comunicação de Campo Próximo (NFC, do inglês *Near Field Communication*) é uma tecnologia de comunicação de *curto alcance* que permite a troca de informações de forma segura entre dispositivos eletrônicos. A troca de informação ocorre quando dois dispositivos estão próximos um do outro, usando indução magnética. A NFC é baseada na

tecnologia RFID e normas vigentes.

A NFC foi desenvolvida por Philips e Sony e seu padrão foi denominado NFCIP-1 (Near Field Communication Interface and Protocol 1), incluído nos documentos (ISO/IEC 18092:2004) e ECMA (*European Computer Manufacturers Association*) subjacentes. Este padrão especifica os esquemas de modulação, codificações de bit, taxas de transmissão e formato de quadro para a interface aérea, assim como os mecanismos de inicialização e controle de colisão. Na NFC existem dois modos de operação: ativa e passiva. Na operação ativa, os dispositivos geram seu próprio campo de radiofrequência para transmitir seus dados *peer-to-peer*. Na operação passiva, um dos dispositivos gera o campo de radiofrequência, enquanto o outro é usado para carregar a modulação para a transferência de dados.

Uma das principais características da NFC que é de curto alcance e permite uma interligação entre dispositivos eletrônicos de uma forma intuitiva, fácil e simples. Esta tecnologia usa alta frequência (HF, do inglês *High Frequency*) e opera na faixa de frequência 13.56 MHz, sob a ISO 14443, então nenhuma restrição é aplicada e nenhuma licença é necessária para seu uso. Outra característica da NFC é que possui um alcance de entre 0 e 20 centímetros (uma média de 10 cm) e com velocidades de transmissão de 106 Kbits/s, 212 Kbits/s e 424 Kbits/s. O protocolo de segurança utilizado por NFC é o protocolo SWP (Single Wire Protocol). Este protocolo se trata de uma interface que oferece comunicação segura entre o cartão SIM (popularmente conhecido como *chip de celular*) e o chip NFC do aparelho. O problema do protocolo SWP é não ser amplamente adotado, até porque não se trata de uma solução totalmente pronta.

A tecnologia NFC é utilizada em uma infinidade de aplicações, inclusive naquelas mais críticas que envolvem dados sigilosos do usuário. As principais aplicações onipresentes foram propostas fazendo uso de NFC como pedidos de pagamento, a emissão de bilhetes [76], no turismo, na localização, na assistência à navegação, em Ambientes de Vida Assistida (AAL) [77], em prédios inteligentes ou ambientes onde ele tem sido estudado para ser sensível ao contexto na interação do usuário com o cenário [78, 79]. Os problemas de segurança em NFC e possíveis soluções são mencionados em [80].

2.4 Comunicação na IoT

A IoT e as RSSFs possuem atributos similares, como a limitação de energia, armazenamento de recursos, enlaces sem fios com perdas e comunicação multi-salto. Por outro lado, a IoT usa o IPv6 no encaminhamento dos dados. Além disso, proporcionar segurança na comunicação é um desafio para IoT, isso ocorre porque os dispositivos, além de serem heterogêneos, alguns deles possuem mobilidade, sendo conectados através de ligações sem fio e exigindo uma comunicação multi-salto.

Os protocolos utilizados recentemente na IoT são 6LoWPAN, RPL e CoAP: O pro-

tocolo 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 [81]. Com esta rede é possível conectar dispositivos com recursos limitados com a Internet convencional para formar a IoT. Permitindo estender redes IPv6 para redes de IoT.

O Protocolo de roteamento IPv6 para rede de baixa potência e com perdas (RPL, do inglês *IPv6 Routing protocols for Low Power and Lossy Network*) [82] é projetado para redes formadas por dispositivos com restrições de energia e baixa capacidade de memória. Assim, a transmissão de dados neste tipo de redes não é confiável e tem baixa taxa de dados e alta taxa de perda. A desvantagem deste protocolo é que ele funciona só em ambientes estáticos. 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, do inglês *Constrained Application Protocol*) [83], tem sido padronizada para a IoT. Este protocolo também pode suportar *broadcast* com pouca sobrecarga. Portanto, a comunicação na rede da IoT ocorre fazendo uso destes protocolos. A Figura 2.2 ilustra a comunicação na IoT.

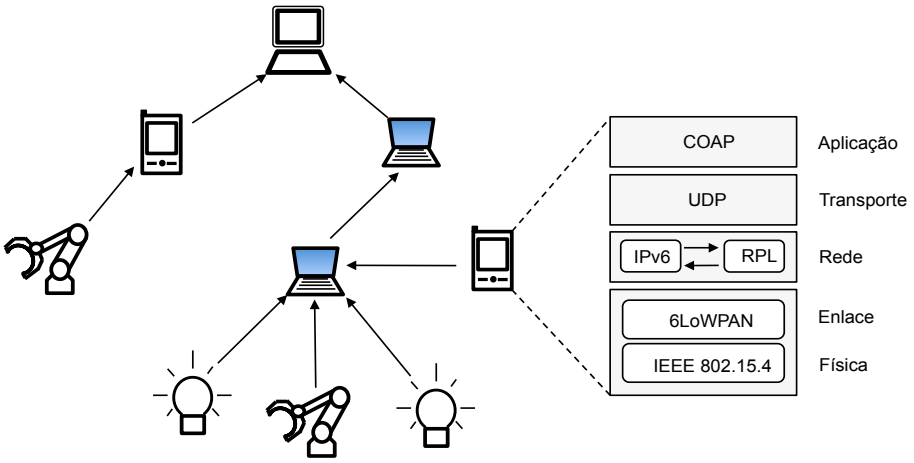

Figura 2.2: Comunicação na rede da IoT

2.5 Segurança na IoT

Os dispositivos que compõem a IoT devem interagir como um roteador, cooperando e encaminhando as informações para outros dispositivos da rede. Estes dispositivos são extremamente vulneráveis a ataques devido à limitação de recursos computacionais que possuem. Desta forma, o uso de métodos e mecanismos de segurança são necessários para garantir a proteção dos dispositivos utilizados na IoT [15, 16]. A seguir são descritos alguns dos requisitos de segurança necessários na IoT.

2.5.1 Requisitos de segurança na IoT

A *confidencialidade* deve fornecer condições para garantir que uma informação seja acessada somente por dispositivos autorizados dentro da rede, sendo um serviço essencial para muitas aplicações da IoT. Assim, em uma aplicação da IoT que ofereça o serviço de confidencialidade, mesmo que um adversário intercepte um pacote da rede, ele não deve ser capaz de ler o conteúdo. Atualmente, existem soluções que podem garantir confidencialidade à rede, mas o problema com a IoT é que seus dispositivos não utilizam técnicas sofisticadas devido à limitação dos recursos que estas possuem.

A *integridade* é a propriedade que assegura que os dados são recebidos tais e como foram enviados pelo dispositivo de origem. Estes dados não são modificados, eliminados e nem alterados pelo dispositivo adversário. Além disso, a integridade está relacionada com a autenticação, esta por sua vez permite conhecer quem produziu, modificou ou descartou alguma informação transmitida. O problema da integridade de dados tem sido extensivamente estudado em todos os sistemas de computação e comunicação tradicionais [84].

A *escalabilidade* é o incremento do número de dispositivos conectados à IoT, o que leva a um aumento no número de comunicação, transações e dados [85]. Em relação à IoT, o número de dispositivos conectados à internet ligará 50-100 bilhões [86] até 2020. Devido a este crescimento, cada sistema tem de se adaptar com o número crescente de dispositivos, a fim de ficar totalmente funcional. A quantidade está diretamente relacionada com o contexto de aplicação. A escalabilidade representa um atributo importante para qualquer tipo de rede.

A *disponibilidade* permite determinar se um dispositivo da IoT possui a capacidade de acessar a rede. Como qualquer medida de segurança complexa aumenta o consumo de energia dos dispositivos, a manutenção da disponibilidade dos dispositivos apesar de seus recursos limitados é um desafio; a falha de alguns dos dispositivos principais pode ameaçar a rede na sua totalidade. Daí a disponibilidade ser um fator importantíssimo de modo a manter a operacionalidade da IoT.

2.6 6LoWPAN

A tecnologia 6LoWPAN, (do inglês *IPv6 over Low Power Wireless Personal Area Network*) desenvolvida pelo Grupo de Trabalho de Engenharia da Internet (IETF, do inglês *Internet Engineering Task Force*) [87] é uma solução adequada para lidar com o desafio de prover escalabilidade e ter uma melhor gestão dos dispositivos para permitir que o conceito da IoT se torne uma realidade. Esta tecnologia permitirá a comunicação entre dispositivos com limitação de recursos computacionais, a fim de trocar dados utilizando o IPv6 [10, 88]. Desta forma é que se requer o uso de IPv6 para dar suporte à grande quantidade de nós conectados à IoT.

Com o desenvolvimento da tecnologia 6LoWPAN, aumentou o tamanho de endereços de 32 bits para 128 bits (2^{128} endereços únicos), permitindo que mais nós estejam ligados à IoT para trocar informações. Este padrão é considerado o elemento adequado para introduzir o conceito de *Internet das coisas* no mundo real [89]. Os dados em um quadro 6LoWPAN ocupam apenas 33 bytes, o cabeçalho IPv6 ocupa 40 bytes, UDP 8 bytes, o 802.15.4 MAC cabeçalho 23 bytes, o AES-CCM-128 21 bytes e 2 bytes para FSC (Frame Check Sequence). O 6LoWPAN define um esquema de fragmentação em que cada fragmento contém uma etiqueta de remontagem e um deslocamento. O IEEE 802.15.4 pode exceder a unidade máxima de transmissão (MTU) com tamanho de 127 bytes, caso em que são necessários fragmentos adicionais. Também suportam comunicação multisalto (*multi-hop*) onde os nós transmitem pacotes em nome de outros nós. O 6LoWPAN trabalha sobre o protocolo IPv6 com base no padrão IEEE 802.15.4 [11]. Por isso, tem as características de baixo custo, baixo consumo de energia, tecnologia portátil sem fio para acessar dispositivos fixos ou móveis. Mas isso foi apenas o começo de uma série de desafios e problemas, como o caso de como proteger esse novo tipo de redes.

Ao contrário da internet onde os dispositivos são mais poderosos e, ao contrário das RSSFs onde os nós possuem recursos limitados, os objetos na IoT são extremamente heterogêneos. Os nós que utilizam a tecnologia 6LoWPAN possuem recursos limitados em termos de capacidade computacional, memória, largura de banda de comunicação e de energia da bateria, da mesma forma que os nós da IoT. Como resultado, é difícil de implementar e usar os algoritmos criptográficos e protocolos necessários para a criação de serviços de segurança [90].

2.6.1 Ataques em 6LoWPAN

Devido à limitação de recursos computacionais, as redes 6LoWPAN são vulneráveis à maioria dos ataques disponíveis contra RSSFs. Um nó atacante inicialmente audita os pacotes em busca de informações privadas, como se fora um nó legítimo da rede, mas este se manifesta como nó atacante *comportando-se de maneira inapropriada ou não autorizada*. O atacante dentro da rede pode ter informação e a confiança dos nós vizinhos com a finalidade de interromper a comunicação. Estes ataques são difíceis de serem detectados e inclusive geram outros tipos de ataques.

Os ataques podem vir de várias direções e alvejar qualquer nó da rede, basta que o nó atacado esteja dentro do alcance de transmissão do nó atacante. Quando um nó atacante tem acesso às informações sigilosas, este pode alterar mensagens em trânsito ou ainda tentar enviar informação falsa para outros nós da rede. Desta forma, o preço que se paga pelas facilidades oferecidas pela comunicação sem fio é a ausência de uma barreira de defesa. Portanto, cada nó da rede deve estar preparado para lidar direta ou indiretamente com ações maliciosas.

Os ataques são classificados de dois tipos: ataques passivos e ataques ativos [91]. Os ataques passivos acontecem quando um nó se encontra utilizando a comunicação sem fio e um nó atacante escuta todos os pacotes trocados entre os nós da faixa de transmissão, mas o nó atacante não interfere ou perturba a comunicação. Estes ataques são extremamente difícil de detectar o nó atacante por não alterar o comportamento da rede. Os ataques ativos são aqueles em que o nó atacante tenta contornar ou invadir redes protegidas; este ataque tenta quebrar a segurança para modificar, roubar, alterar ou eliminar a informação.

Um claro exemplo de um ataque, é o de negação de serviço (DoS, do inglês *Denial of Service*). Este ataque interrompe a disponibilidade da rede. Os ataques mais simples de DoS esgotam os recursos disponíveis para o nó vítima, enviando pacotes desnecessários. Desta forma, este ataque impede que os usuários legítimos da rede tenham acesso aos serviços ou recursos a que têm direito. O ataque DoS é destinado não só para tentativa do atacante de perturbar ou destruir a rede, mas também para qualquer evento que diminui a capacidade ou desempenho de uma rede de fornecer um serviço. Vários tipos de ataques DoS acontecem nas diferentes camadas da IoT. A Figura 2.2 ilustra os ataques que acontecem nas diferentes camadas da tecnologia 6LoWPAN. Este trabalho investiga um dos ataques de roteamento mais severos, seu nome é *sinkhole*.

Camadas	**Ataques em 6LoWPAN**
Física	Jamming, Tampering
Enlace	Collisions, Exhaustion, Unfairness, Interrogation, Sybil
Rede	Hello flood, Selective-forwarding, Sybil, Wormhole, Spoofed, Misdirection, Smurf, Homing, **Sinkhole**
Transporte	Flooding, De-synchronization
Aplicação	Overwhelm, Path-based DoS

Tabela 2.2: Ataques em 6LoWPAN

2.7 Ataque sinkhole

O ataque *sinkhole* é um ataque de negação de serviço, considerado o ataque de roteamento mais destrutivo para as redes sem fio empregado por um atacante interno na rede [14, 92]. Este ataque acontece na camada de rede e é muito complexo de ser detectado, já que seu comportamento é aparentemente transparente. Este ataque obtém certo conhecimento do funcionamento da rede antes de revelar-se como um atacante.

O nó atacante *sinkhole* anuncia para seus vizinhos que possui um caminho ideal, que possui o caminho mais curto para o destino pretendido, assim como a melhor largura de banda, uma rota de alta qualidade [93, 94, 95]. Desta forma, tenta atrair quase todo o tráfego de uma determinada área, criando um *sinkhole* metafórico. Os nós próximos podem considerar o caminho através do nó atacante melhor do que o utilizado atualmente

e mover seu tráfego com direção ao nó atacante. Uma vez que os nós afetados dependem do atacante para comunicar-se, o caminho que utilizam os pacotes oferecem muitas oportunidades para a manipulação de dados, injeção de pacotes maliciosos, dados errados ou não encaminhar informações para o destino pretendido. Além disso, o ataque *sinkhole* permite realizar outros ataques eficientes, como o ataque *Selective Forwarding*, por exemplo. Portanto, para que o ataque *sinkhole* seja efetivo o nó atacante deve posicionar-se o mais perto do destino pretendido para, assim, obter a maior quantidade de nós afetados com o menor esforço e menor consumo de recursos possíveis. A Figura 2.3 ilustra o ataque *sinkhole* dentro de uma rede.

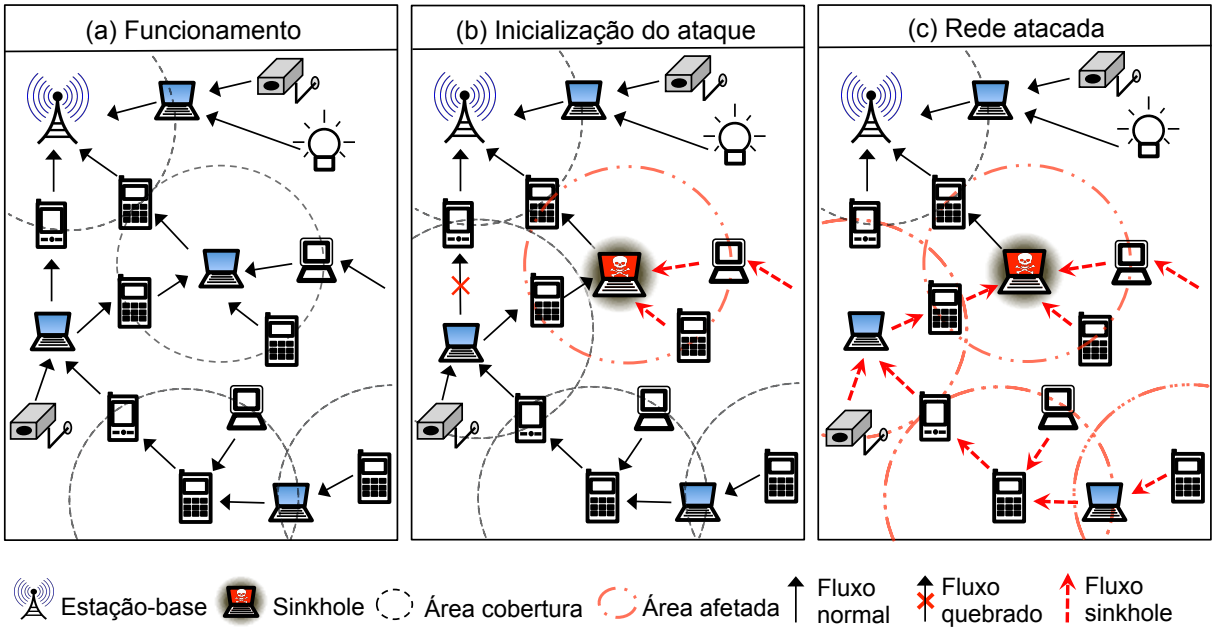

Figura 2.3: Ataque sinkhole

2.7.1 Desafios na detecção de ataques sinkhole

Os desafios encontrados na literatura ante a detecção de ataques *sinkhole* são detalhados a seguir:

Comunicação com o destino: Todas as mensagens são enviados para um destino, mas muitas vezes encaminhados por outros dispositivos, criando uma oportunidade para lançar um ataque *sinkhole*. Portanto, o intruso só precisa posicionar-se o mais perto do destino pretendido.

Mobilidade: A mobilidade dos dispositivos se torna mais vulnerável a ataques de roteamento. Um dispositivo adversário pode introduzir-se no caminho entre a origem e o destino para absorver o tráfego da rede com o objetivo de depreciar o desempenho da rede.

O sinkhole dependendo do protocolo de roteamento: Os pacotes em uma rede são transmitidos com base nas métricas de encaminhamento que variam, dependendo do protocolo utilizado. Um nó atacante pode explorar isso para mentir a seus vizinhos, a fim de lançar um ataque *sinkhole*.

Restrição de métodos de detecção pela limitação de recursos: A limitação dos recursos que possuem os dispositivos faz com que sejam vulneráveis a diferentes tipos de ataques. Isto dificulta a implementação de mecanismos de segurança sofisticados, a fim de evitar ataques. Por isso, devem ser usados métodos menos sofisticados compatíveis com os recursos disponíveis.

2.7.2 Requisitos para prevenir ataques sinkhole na IoT

Existem algumas medidas encontradas na literatura para evitar ataques *sinkhole* e métodos para detectar *sinkhole* nas redes sem fio [96]. Essas medidas ajudam a prover segurança aos dispositivos, além de melhorar o desempenho da rede. A seguir são detalhados alguns requisitos para evitar ataques *sinkhole*: (i) os métodos de detecção que abordam o comportamento normal do dispositivo, este método busca encontrar algum comportamento anômalo na rede. Se considera uma atividade anômala quando esta apresenta um desvio comparada ao comportamento normal; (ii) o método baseado em regras é projetado com base no comportamento ou técnicas usadas para lançar ataques *sinkhole*, onde os pacotes enviados são analisados de acordo com estas regras, um dispositivo será considerado atacante quando viola estas regras; (iii) métodos estatísticos são associados com certas atividades dos dispositivos dentro da rede. O dispositivo adversário pode ser detectado através da comparação do comportamento real com o valor do limiar, que é usado como referência, qualquer dispositivo que excede o limiar é considerado um atacante; (iv) método de prevenção: nesta abordagem, a integridade e autenticidade dos pacotes que viajam dentro da rede estão protegidas usando chaves para criptografar e descriptografar.

2.8 Resumo

Este capítulo apresentou os conceitos relacionados ao funcionamento da tecnologia da Internet das coisas (IoT), assim como também sua arquitetura, tecnologias utilizadas e a comunicação empregada pelos dispositivos. O capítulo também apresentou o uso das redes 6LoWPAN dentro do contexto da IoT. Foram abordadas as vulnerabilidades, sendo estas classificadas de acordo com as camadas da rede, destacando o ataque *sinkhole*, e foram apresentados alguns requisitos para prevenir estes ataques.

CAPÍTULO 3

MECANISMOS DE DETECÇÃO E PREVENÇÃO

Este capítulo apresenta os principais trabalhos existentes na literatura para prevenção ou detecção de ataques *sinkhole* nas redes sem fio. A Seção 3.1 introduz o conceito e descreve os tipos de sistemas de detecção de intrusão. Mostrando uma análise dos trabalhos baseados nas técnicas mais comuns empregadas na detecção de intrusão de ataques *sinkhole*. Essas técnicas são classificadas em contramedidas de prevenção ou de detecção. A Seção 3.2 mostra uma análise dos trabalhos baseados na reputação. Sendo algumas delas inspiração à solução proposta neste trabalho. A Seção 3.3 descreve as soluções existentes para detecção de intrusão na IoT.

3.1 Sistemas de detecção de intrusão

Os sistemas de detecção de intrusão (IDS, do inglês *Intrusion detection system*) são técnicas, métodos, mecanismos ou recursos usados que visam melhorar a segurança diante de ataques e ameaças aos sistemas computacionais ou redes de computadores [97, 98]. Os IDSs são considerados como a segunda linha de defesa, depois dos *firewalls* e geralmente os IDSs são projetados para funcionar em redes cabeadas. Além disso, a detecção de intrusão é o processo de monitorar os eventos que ocorrem em um sistema à procura de sinais de intrusão. A intrusão é definida como uma tentativa de comprometer a confiabilidade, integridade, disponibilidade ou burlar a segurança de um sistema ou rede. A principal motivação no desenvolvimento de sistemas de detecção de intrusão é o fato de não ser possível criar um mecanismo de defesa totalmente seguro. Com o desenvolvimento da IoT e suas aplicações, a mobilidade tornou-se um atributo importante em suas aplicações. Novos modelos de IDSs tornaram-se necessários para lidar com a mobilidade, com a finalidade de identificar problemas e garantir o correto funcionamento na comunicação e no acesso às aplicações.

Um sistema de detecção de intrusão é dividido em duas categorias baseadas em: máquina e rede. Os IDSs em máquina (HIDS, do inglês *host-based intrusion detection system*) são sistemas que monitoram, detectam e respondem às atividades de ataques em uma determinada máquina (*host*). Qualquer decisão tomada é influenciada pelas informações coletadas na estação especifica. Contudo, essa abordagem não é viável em uma rede com recursos limitados, devido à sua natureza distribuída. Os IDSs em rede (NIDS, do inglês *network intrusion detection system*) é uma máquina ou um software que escuta, captura e examina os pacotes em tempo real à procura de sinais de invasão. Os NIDSs são configurados em pontos de concentração como em roteadores, onde qualquer nó pode funcionar

como roteador, sendo possível monitorar o tráfego da rede.

O uso de IDS fornece algumas ou todas as seguintes informações: (i) identificação do intruso; (ii) localização do intruso; (iii) o tempo de intrusão; (iv) a atividade de intrusão (por exemplo, ativa ou passiva); (v) o tipo de intrusão (ataque *wormhole*, *blackhole*, *sinkhole* e outros). Portanto, os IDSs aplicam essas informações para mitigar (terceira linha de defesa) e corrigir o resultado de ataques [38].

A maioria dos IDSs operam em diferentes modos como: modo autônomo e modo cooperativo. Um IDS no modo autônomo funciona em cada nó para detectar atividades indesejadas. O IDS no modo cooperativo é baseado em agrupamentos (*clusters*) [99], em que cada nó monitora seus vizinhos e se for detectada qualquer atividade maliciosa, o nó líder (*cluster head*) é informado. Na literatura existem diversos IDSs que empregam mecanismos para descoberta e detecção de nós atacantes. Os IDSs são basicamente projetados para detecção de ataques de roteamento e muitas das soluções existentes estão relacionadas à segurança para RSSF, para redes móveis *ad-hoc* (MANET) e para redes veiculares (VANETs). A seguir são descritos alguns trabalhos que propõem o uso de IDS para proteção destas redes.

3.1.1 Tipos de sistemas de detecção

Existem três tipos de sistemas de detecção que atuam a partir de assinaturas, anomalias ou de forma híbrida. A detecção por *assinaturas* também é chamada de detecção por regras. O IDS por assinatura tem a função de comparar a informação que está monitorando com as assinaturas (regras) pré-definidas de um ataque [100] para detectar um padrão. Desta forma, o IDS por assinaturas é eficiente para ataques conhecidos, mas não detecta novos ataques como o IDS apresentado nos trabalhos [22, 65].

A detecção por *anomalias* apoia-se na ideia de que um ataque gera um desvio no comportamento padrão da rede, assim o IDS por anomalias monitora as atividades da rede e as classifica como comportamento normal ou anômalo. O IDS por anomalias usa perfis que se desenvolvem através do monitoramento das atividades ao longo de um período de tempo [101] e é eficiente para detecção de ameaças desconhecidas, porém gera elevadas taxas de falsos positivos. Um exemplo de um IDS baseado em anomalias é apresentado no trabalho [30].

O IDS *Híbrido* geralmente contêm dois módulos de detecção, isto é, um módulo que é responsável por detectar ataques conhecidos a partir de assinaturas pré-definidas e outro módulo responsável por detectar e aprender os padrões normais e anormais ou monitorar o comportamento da rede para detectar alguma anomalia [102]. Os sistemas de detecção híbridos são mais precisos em termos de detecção de ataques com menor número de falsos positivos, porém geram mais consumo de recursos como é apresentado no trabalho [103].

3.1.2 Estratégias de contramedidas contra ataques de roteamento

Para detectar um ataque é necessário conhecer e planejar estratégias que permitam proteger e dar segurança à rede. Atualmente, existem duas principais abordagens para classificar as contramedidas de segurança propostas para ataques *sinkhole* encontradas na literatura. Estas contramedidas são: as contramedidas de prevenção [27, 29] e as contramedidas de detecção [103, 28, 30, 104, 105, 32].

3.1.2.1 Prevenção

As contramedidas de prevenção impedem que nós atacantes dentro da rede sejam capazes de efetuar um ataque *sinkhole*. Para isso, estas contramedidas de prevenção se concentram no uso de métodos criptográficos, métodos de autenticação, distribuição e gerenciamento de chaves. Estes métodos citados anteriormente proíbem aos nós adversários de modificar mensagens existentes e a criação de pacotes falsos.

O esquema TMW (*Time-Endorsement by Mobile Agent in Wireless Sensor Network*) [27] foca na *prevenção* de diversos tipos de ataques como *sybil, DoS e sinkhole* fazendo uso de criptografia simétrica para criptografar os dados. Este trabalho usa agentes móveis para distribuição e autenticação de chaves secretas usando o algoritmo *one-time pad*. Este algoritmo é uma técnica de criptografia usada para distribuir as chaves pelo agente móvel. Isto assegura um certo grau de segurança à rede. Para garantir a integridade da rede, são usados nós monitores que oferecem garantia aos dados comunicados. A estação-base analisa os dados recebidos pelos nós monitores e pelos nós líderes comparando suas informações; se é diferente, conclui-se que o nó líder está comprometido. Esses detalhes são transmitidos para toda a rede, de modo que todos os nós líderes coloquem o nó líder comprometido na lista negra ou *blacklist*. Uma representação do TMW é ilustrada na Figura 3.1.

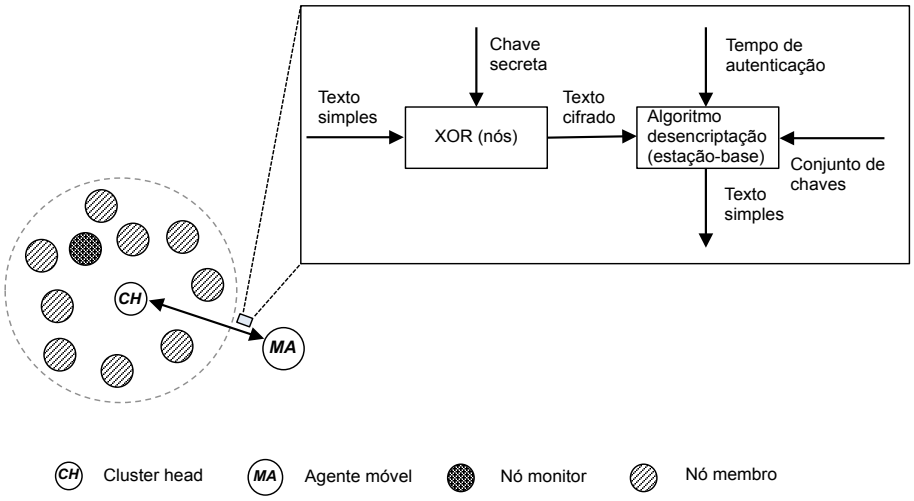

Figura 3.1: Funcionamento do TMW

O esquema proposto em [29] visa *prevenir* contra ataques de roteamento nas RSSFs. Esse esquema fornece uma abordagem orientada à segurança usando um algoritmo para encontrar um caminho alternativo para cada transmissão de dados, a fim de superar o nó atacante. A vantagem é que o nó adversário não é capaz de capturar as informações, já que o adversário desconhece a nova rota das informações. Assim, estas informações chegarão ao seu destino sem nenhuma interceptação e alteração. O esquema proposto é formado por quatro fases: a fase de inicialização, onde todos os nós sensores estão em modo desligado, este modo é mudado para o modo ativo. A fase de seleção de agendamento, se executa quando um nó deseja encaminhar pacotes de dados, então é selecionada e mantida uma fila de prioridade. A fase de processamento, remove o primeiro nó presente na fila depois de adicionar todos seus vizinhos à extremidade traseira da fila de prioridade e não permite duplicidade de nós na fila. Por último, a fase de caminho alternativo onde o algoritmo se detém no caso do destino ser alcançado e o caminho alternativo é determinado pela remoção dos nós da pilha.

Considerando as características dos sistemas de encriptação e autenticação para prevenção de ataques *sinkhole*, percebe-se que estas características são muito sofisticadas para o uso dentro da IoT. O uso de métodos ou técnicas sofisticados originará gargalos na comunicação da IoT.

3.1.2.2 Detecção

A prevenção nem sempre é possível mas os ataques *sinkhole* e qualquer outro tipo de ataque precisa ao menos ser detectado. Para isso, se usa métodos que empregam técnicas cooperativas ou de colaboração. A seguir são apresentadas algumas técnicas encontradas na literatura.

Hichem Sedjelmaci *et al.* [103] propuseram um IDS híbrido que usa agrupamentos para uma RSSF. Este IDS híbrido emprega uma combinação entre a detecção por anomalias baseado em máquina de vetor de suporte (SVM) e a detecção através de assinaturas. A detecção híbrida proposta apresenta uma arquitetura para detecção de ataques de roteamento. Na arquitetura do IDS híbrido, o ataque é detectado pelo módulo de detecção híbrida (HIDM) ou pela detecção cooperativa (CDM) dos nós. O HIDM é o processo de treinamento local, onde cada agente IDS treina o SVM localmente, em seguida, calcula o vetor de suporte que será enviado para um nó adjacente do mesmo agrupamento. Cada nó monitor recebe o vetor de suporte de seus IDS vizinhos, este nó monitor realizará uma combinação entre a informação recebida e seu próprio vetor de suporte. Após isso, estes nós atualizam seus vetores de suporte e calculam o hiperplano, transmitindo o resultado do vetor de suporte aos nós IDS mais próximos. Este procedimento se repete por todos os nós IDS do mesmo agrupamento até alcançar o mesmo SVM. O HIDM possui um banco de dados com alguns sinais predefinidos de intrusão. Se a detecção ocorre, o nó

IDS envia um alarme para o nó líder para que remova o nó atacante e avisa aos demais nós líderes sobre o ataque, caso contrario é lançado um processo de cooperação (CDM), se não houver nenhuma relação entre a intrusão detectada pelo mecanismo de detecção de anomalias com algumas assinaturas predefinidas, o agente IDS envia o relatório para o nó líder. Esse nó executa um mecanismo de votação para fazer uma melhor decisão sobre os nós suspeitos. No caso de mais da metade de nós IDS decidirem que o nó suspeito é um atacante, o nó suspeito é isolado e o banco de dados de assinaturas é atualizado.

Soo Young Moon *et al.* [30] apresentaram uma abordagem de detecção de intrusão contra ataques *sinkhole* para RSSF. Esta abordagem usa a lógica fuzzy na detecção de nós adversários e também usa nós mestres (MNs) para monitorar a comunicação entre os nós sensores. Cada MN envia periodicamente o número de mensagens de roteamento escutadas na área monitorada para o nó *sink*. O nó *sink* detecta a existência de um nó adversário a partir dos dados coletados pelos MNs usando um limiar de segurança que controla o grau de detecção. Com o uso desse limiar de segurança a proporção de falsos negativos diminui, mas a taxa de falsos positivos aumenta. Para isso, se usa a lógica fuzzy para o cálculo do valor de detecção para cada área a partir de determinados valores. Estes valores são a taxa de reforço e o raio da área. Dos dois valores, a lógica fuzzy deriva o valor de detecção. Se o valor de detecção é maior do que o valor do limiar de segurança que foi definido anteriormente, o ataque *sinkhole* é detectado, caso contrario não existe nó adversário. A Figura 3.2 apresenta o fluxograma do funcionamento da abordagem proposta.

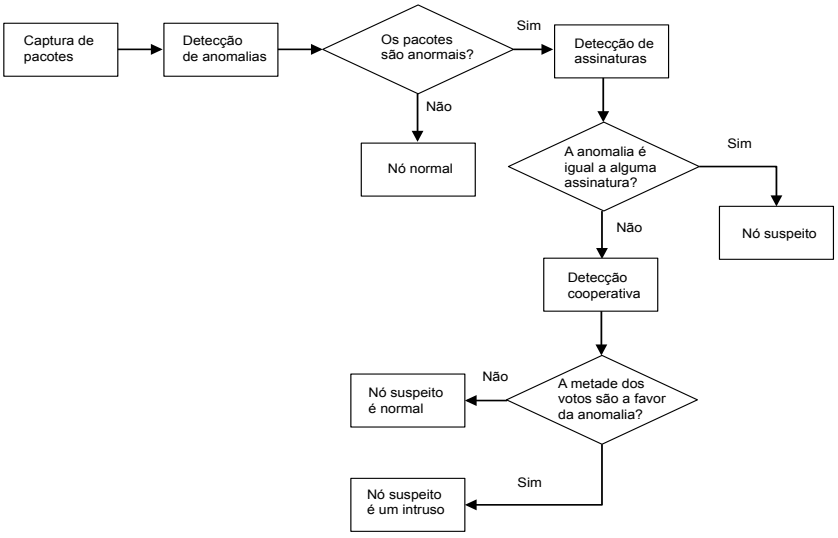

Figura 3.2: Fluxograma do funcionamento da detecção

H. Shafiei *et al.* [104] propuseram duas abordagem para detectar ataques *sinkhole*. A lógica desse enfoque é que os nós ao redor do *sinkhole* esgotam sua energia mais rápido do que os outros nós da rede. Assim forma-se um buraco de energia em torno de cada *sinkhole*. Na primeira abordagem a estação-base usa um método de geoestatística para

avaliar e corroborar a energia residual de cada região e estima a possibilidade de existência de um *sinkhole* usando um estimador estatístico. A partir do valor do estimador, a estação-base comunica a todos os nós para evitar a região suspeita no encaminhamento. A segunda abordagem é um método de monitoramento distribuído para detectar regiões com o menor nível de energia residual. Para realizar a mitigação, a estação-base transmite periodicamente uma lista com os IDs dos nós que residem nos buracos, a fim de evitar a adulteração do adversário na lista. A estação-base usa uma transmissão confidencial e segura, como a usada em [106]. Há dois casos que são considerados: o primeiro caso, o nó se encontra fora da região suspeita e, no segundo caso, o nó reside dentro da região. No primeiro caso, o nó remove os nós mencionados na lista de seus encaminhamentos futuros, assim, a ameaça do *sinkhole* é mitigada. No segundo caso, o nó seleciona um nó intermediário longe da sua vizinhança e envia os seus pacotes. O nó intermediário, então, tenta encaminhar o pacote para o destino. No entanto, o roteamento na presença de buracos é um desafio.

Wahab *et al.* [105] apresentam um modelo para detectar nós egoístas para redes veiculares (VANET). Esse modelo cria uma hierarquia baseada em líderes de agrupamentos, como é ilustrado na Figura 3.3. O modelo possui duas fases: uma que é capaz de motivar os veículos (nós) a se comportar cooperativamente durante a formação de agrupamentos e a outra detectar nós egoístas após formados os agrupamentos. Na primeira fase, os incentivos são oferecidas na forma de reputação que permitem motivação dos nós a se comportarem de maneira cooperativa durante a formação dos agrupamentos. Os serviços de comunicação são oferecidos a partir da reputação acumulativa do nó. Na segunda fase, o modelo aplica *watchdog* a partir da teoria de Dempster-Shafer para detectar nós egoístas, baseados nas evidencias cooperativas aumentando a probabilidade de detecção. Neste modelo, a comunicação entre dois agrupamentos é realizada através de nós que cumprem a função de retransmissores multipontos (MPR). Entretanto, o modelo proposto apresenta uma alta taxa de falsos positivos e falsos negativos na detecção de nós egoístas afetando a estabilidade e o desempenho da rede.

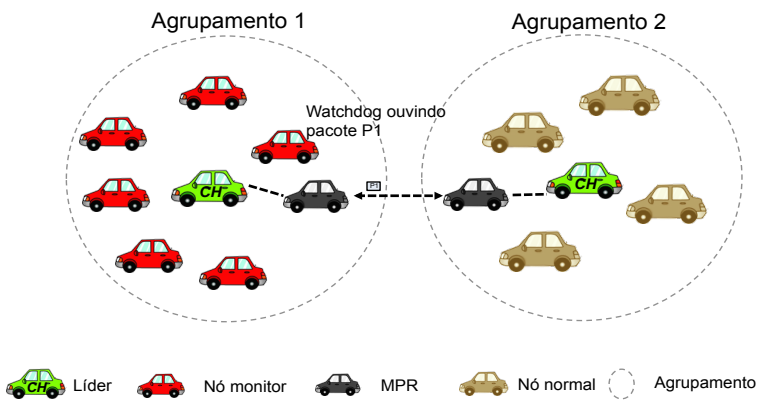

Figura 3.3: Modelo de detecção de nós egoístas para VANETs

Naveen Kumar *et al.* [32] definem uma detecção contra ataques *sinkhole*. A detecção proposta usa agentes móveis para detecção de nós adversários. Estes agentes empregam dois algoritmos: o algoritmo de navegação e o algoritmo de roteamento. O algoritmo de navegação descreve como é que um agente móvel deve fornecer 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. O uso desses algoritmos têm como finalidade a detecção de alguma anomalia, como quando um nó não responde para o agente móvel ou quando o agente detecta que o nó não está encaminhando as informações para o destino, sendo esse nó um nó adversário ou comprometido, que pode levar ao ataque *sinkhole*.

3.2 Sistemas de reputação

A partir da adaptação da reputação e da confiança para redes de comunicações sem fio, estudos formais foram realizados sobre como a reputação e a confiança são uma solução eficaz para melhorar a segurança. Nas redes sem fio o comportamento do nó envolve o processo de roteamento de mensagens e gerenciamento de pacotes das informações, onde estas informações são excluídas ou adulteradas por nós atacantes. A reputação e a confiança ajudam na tomada de decisões e promovem a colaboração dos nós em redes com fio e sem fio. As principais características da reputação estão no fato de serem temporais, dinâmicas e precisarem de atualizações de forma constante para identificar a origem da ameaça e determinar se a ameaça é legitima ou não. A reputação não é apenas um componente importante para qualquer sistema de segurança, mas também é essencial e efetiva contra as ameaças. Portanto, não se pode confiar em técnicas tradicionais como, a proteção baseada em assinaturas e as listas negras ou *blacklist*. A seguir são apresentados alguns trabalhos que usam a reputação.

O arcabouço (*framework*) RFSN (*Reputation-Based Framework for High Integrity Sensor Networks*) [107] emprega uma abordagem para desenvolver uma comunidade de confiança, integrando ferramentas de estatística e teoria de decisão em uma estrutura distribuída e escalável. A Figura 3.4 ilustra a estrutura do RFSN, em que a direção das setas representam o fluxo de informação. A estratégia aplicada consiste em cada nó sensor calcula a métrica da reputação que representa o comportamento passado de outros nós e os dados das métricas são usados como um aspecto inerente a prever seu comportamento. Para isso, é usada uma formulação bayesiana para o sistema de reputação. A formulação bayesiana permite calcular, atualizar a reputação e a confiança para detectar nós comprometidos ou com defeito. O RFSN foi avaliado por meio de simulações usando Avrora. O resultado de desempenho do RFSN apresenta uma elevada taxa de detecção de nós atacantes. Além disso, o RFSN tem um grande consumo de recursos como de memória e de energia.

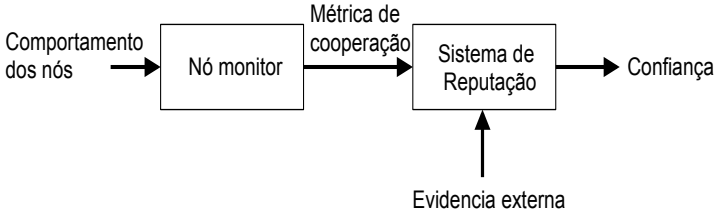

Figura 3.4: Representação do RFSN

O esquema ATRM (*Agent-based Trust and Reputation Management scheme for WSN*) [43] é baseado em agrupamentos e no uso de agentes móveis em uma RSSF. Os agentes moveis do ATRM controlam e desenvolvem a função de observadores e mensageiros quando detectam algum comportamento estranho de algum nó da rede. Este comportamento tem como base a reputação de cada nó já que a reputação de um nó é a percepção global sobre normas de comportamento do nó a partir da confiança de nós vizinhos. O principal objetivo do esquema ATRM é a gestão da confiança e reputação com sobrecarga mínima em termos de mensagens extras e demora de tempo.

O protocolo RDAS (*Reputation-based Resilient Data Aggregation in Sensor Network*) [108] permite a agregação de dados que usa uma abordagem fundamentada na reputação para identificar e isolar nós maliciosos de uma RSSF. O RDAS considera a formação de agrupamentos dos nós, onde o nó líder analisa os dados coletados dos nós do agrupamento para determinar a localização de um evento malicioso, usando a redundância dos dados como é ilustrado na Figura 3.5. Os nós fazem parte de um sistema de reputação distribuída, onde eles compartilham informações sobre o desempenho de outros nós na comunicação de dados e usam as avaliações da reputação para remover os relatórios de nós maliciosos. A integridade do RDAS é afetada quando um nó envia falsas acusações sobre o comportamento dos nós vizinhos.

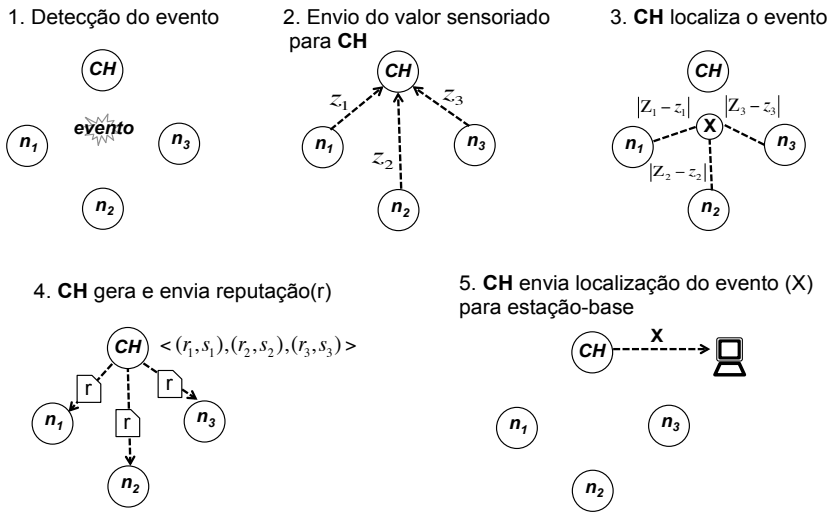

Figura 3.5: Funcionamento do RDAS

O sistema EBTRM-WSN (*Enhanced Bio-inspired Trust and Reputation Model for WSN*) é uma extensão do modelo de confiança e reputação (BTRM-WSN) [41]. O objetivo do EBTRM-WSN é fornecer uma solução de segurança eficaz para RSSF, proporcionando um elevado nível de segurança, que leva em consideração a conservação de energia. Este sistema aumenta a precisão com sucesso em encontrar nós de confiança de forma eficiente, sendo que a quantidade extra de energia necessária para os *add-ons* é aceitável. O EBTRM-WSN é capaz de encontrar nós de confiança com mais precisão do que seu concorrente BTRM-WSN. O BTRM-WSN tem um consumo de energia maior quando se aplica um EBTRM-WSN para procurar sensores confiáveis. Entretanto, devido ao elevado consumo de energia do sistema, não pode atuar na IoT devido às características que possuem seus componentes.

3.3 Sistemas de detecção de intrusão em IoT

Na literatura, muitas soluções de detecção de ataques encontradas estão relacionadas à segurança para RSSFs, MANETs ou VANETs, mas poucas soluções relacionadas à proteção e segurança das IoTs. Estas poucas soluções encontradas é devido a que a rede da IoT é considerada uma nova tecnologia que representa o futuro da computação e da comunicação e cujo desenvolvimento depende da inovação técnica dinâmica em campos tão importantes como os sensores *wireless* e a nanotecnologia. A seguir são descritos alguns trabalhos que propõem o uso de IDS para proteção e segurança da IoT diante de dispositivos (nós) maliciosos.

O sistema SVELTE [34] é a primeira tentativa de desenvolver um IDS projetado especificamente para a IoT. Este sistema é composto por três módulos centralizados permitindo detectar ataques de roteamento, estes módulos são: o módulo de mapeamento chamado (*6Mapper*), o módulo de detecção de intrusão e também foi implementado um mini-firewall, como é visto na Figura 3.6. Os ataques detectados pelos mecanismos empregados por o sistema SVELTE são de falsificação (*spoofed*) ou alteração de informação, o *sinkhole* e o ataque de encaminhamento seletivo (*selective forwarding*). Uma das desvantagens do sistema SVELTE é que considera consultas realizadas a partir de um roteador de borda, que percorre todos os nós de uma rede IoT, a fim de detectar inconsistências nela. Essas inconsistências são obtidas através de comparações da informação das posições de cada nó dentro da rede. Outra desvantagens encontrada no sistema SVELTE é que trabalha sobre uma topologia hierárquica em árvore onde os nós se encontram posicionados de maneira aleatória e não possuem mobilidade sendo estes nós estáticos. Além disso, outra desvantagem é que no momento que um nó pai é afetado por um dispositivo atacante, este afeta os nós ligados a ele perdendo assim a comunicação da parte afetada da rede. Estas desvantagens levam a obter resultados elevados no consumo de recursos e a ter um baixo desempenho.

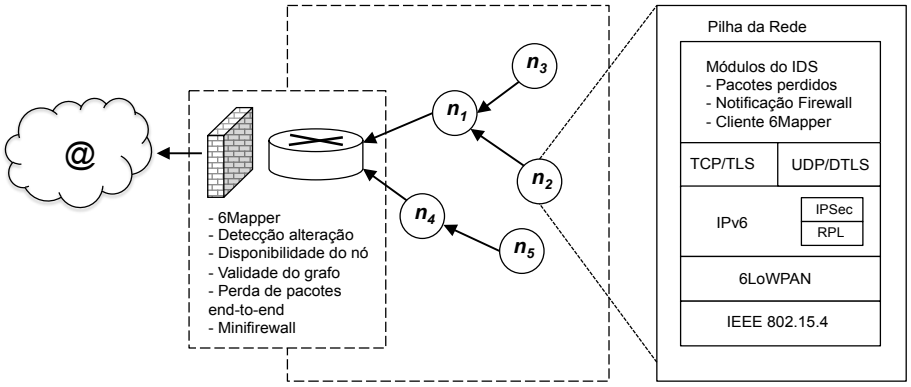

Figura 3.6: Módulos do SVELTE

A arquitetura proposta em [35] integra um sistema de detecção de intrusão (IDS) na estrutura de rede desenvolvida dentro do projeto Ebbits [109]. Esta proposta tem como principal característica a detecção de ataques DoS (*negação de serviço*) em redes 6LoWPAN para IoT. A proposta baseia-se no uso de um componente exploração (IDS_P) que permite escutar o trafego da rede 6LoWPAN enviando informações relacionadas da rede para o IDS (Suricata) a fim de examinar os pacotes da rede e se for o caso de detectar um comportamento irregular de um nó da rede, lança alertas para o componente de proteção DoS que recebe as mensagens de alerta para analisar e confirmar sobre o ataque. Dessa forma, o IDS detecta ataques DoS na rede. Além destas soluções encontradas para a proteção e segurança da IoT, a Tabela 3.1 mostra a comparação de algumas soluções existentes diante a detecção de ataques na IoT

IDS / **Características**	**SVELTE [34]**	**Ebbits [35]**	**IDS para IoT [36]**
Dispositivo	Estático	Estático	Estático
Cenário	Estacionário	Estacionário	Estacionário
Método Detecção	Híbrido	Híbrido	Assinaturas
Tipo de Ataque	Sinkhole, Selective-forwarding, Sybil, CloneID	DoS	DoS
Protocolo Roteamento	RPL	6LoWPAN	-
Abordagem	IDS baseado host, 6Mapper	Teste de invasão	Uso de AIS
Simulador	Cooja (Contiki)	PenTest (Linux)	-

Tabela 3.1: IDSs em IoT

Estes sistemas, embora propostos para IoT e atendendo às suas características, são muito restritos na forma da análise de um comportamento do nó. Uma das características comuns desses sistemas de detecção é que os nós que compõem a rede não possuem mobilidade. A maioria dessas propostas possuem elevadas taxas de consumo de recursos, falsos positivos e negativos, obtendo assim um baixo desempenho.

3.4 Resumo

Esse capítulo apresentou os esquemas e soluções existentes na literatura para prevenção e detecção de ataques *sinkhole*. Foi realizada uma breve contextualização dos mais recentes esquemas de prevenção e detecção para segurança da IoT. Além disso, as soluções propostas foram classificados dependendo do modo de abordagem.

CAPÍTULO 4

O SISTEMA INTI

Este capítulo apresenta um sistema de detecção e isolamento contra ataques *sinkhole* no âmbito da Internet das coisas (IoT). O sistema, denominado INTI, utiliza a técnica de detecção baseada no comportamento na transmissão de mensagens de cada dispositivo pertencente à rede. O INTI detecta e quantifica o impacto dos ataques *sinkhole* a fim de auxiliar as medidas reativas para o isolamento dos ataques *sinkhole*. Além disso, o INTI usa o cálculo da reputação e da confiança para cada um dos dispositivos da rede. A Seção 4.1 introduz uma visão geral do sistema, suas características e seus principais módulos. A Seção 4.2 detalha cada módulo que compõe o sistema INTI. A Seção 4.3 apresenta o funcionamento do sistema e exemplifica as funções de cada componente.

4.1 Visão geral

O sistema INTI (***I**ntrusion Detection Si**N**khole At**T**tacks 6LoWPAN Internet of Th**I**ngs*) tem como objetivo a detecção e isolamento diante da presença de ataques *sinkhole* dentro da rede de Internet das coisas (IoT). Para isso, o sistema INTI apresenta uma arquitetura composta por quatro módulos: o **módulo de configuração dos agrupamentos**, o **módulo de monitoramento do encaminhador**, o **módulo de detecção de atacante** e por último o **módulo isolamento de atacante**. O INTI é executado em cada dispositivo (nó) móvel que fazem parte da rede IoT. Além disso, cada nó pode assumir 3 estados: nó membro, nó associado ou nó líder. A Figura 4.1 ilustra os módulos que compõem a arquitetura do sistema INTI.

O *módulo de configuração dos agrupamentos* cria e repara os agrupamentos que compõem a rede, ou seja, ele agrupa os nós e define os agrupamentos estabelecendo a rota no encaminhamento de dados na rede. Ademais, se reconstrói os agrupamentos após acontecida alguma falha de um nó, abandono de agrupamento ou um ataque. Este módulo contém dois componentes: coleta das mensagens de controle e eleição de nós líderes e associados. O componente coleta de mensagens realiza um sensoriamento da rede a fim de obter os valores utilizados pelo sistema para a criação da rede. Em seguida, o componente eleição de nós líderes e associados realiza a eleição com base nos valores obtidos na coleta de mensagens. Considerando como nós líderes de cada agrupamento aqueles nós que possuírem a maior quantidade de nós vizinhos.

Após da eleição do líder, os agrupamentos são de fato determinados. Para isso, os nós líderes anunciam-se aos nós vizinhos como líderes e os nós vizinhos respondem escolhendo um deles formando assim os agrupamentos, sendo estes nós vizinhos classificados como

nós membros. Para a determinação do nó associado, o nó membro avisa para seus líderes que ele recebeu duas mensagens de diferentes líderes, sendo classificado pelo líder como nó associado para o encaminhamento dos dados. Neste módulo a reconstrução dos agrupamentos acontece quando uns dos nós da rede falha, abandona o agrupamento ou quando ocorre um ataque *sinkhole*, a fim de manter a estabilidade na comunicação da rede.

O *módulo de monitoramento do encaminhador* tem a finalidade de controlar e verificar o número de pacotes de dados trocados entre os nós. Ele possui dois componentes: o componente de determinação do encaminhador de dados e o componente de verificação do encaminhamento das mensagens de dados da IoT. O componente de determinação do encaminhador de dados contabiliza o número de pacotes enviados por um nó. O componente de verificação do encaminhamento de dados tem a finalidade de encontrar alguma suspeita na quantidade de pacotes enviados. Ao encontrar uma suspeita, este componente envia uma mensagem ao módulo de detecção avisando sobre a suspeita encontrada.

O *módulo de detecção de atacante* é baseado no cálculo da reputação e da confiança do nó encaminhador de dados da IoT levando em consideração o *status* do nó suspeito sobre seu comportamento na transmissão de mensagens, possibilitando a detecção do ataque *sinkhole*. O *módulo de isolamento de atacante* possui dois componentes: o componente de alerta sobre o nó atacante e o componente de reconstrução do agrupamento do nó atacante. O componente de alerta tem o objetivo de avisar e promover a separação do nó adversário fora da rede. O componente de reconstrução do agrupamento do nó atacante tem a finalidade de restaurar o agrupamento afetado para que continue funcionando normalmente; este módulo agrega robustez à rede. Portanto, os quatro módulos em conjunto oferecem segurança na comunicação e proteção dos dados dos nós da IoT permitindo detectar e isolar um nó adversário dentro da rede, isto ocorre devido o comportamento dos nós nas transmissões de mensagens dentro da rede.

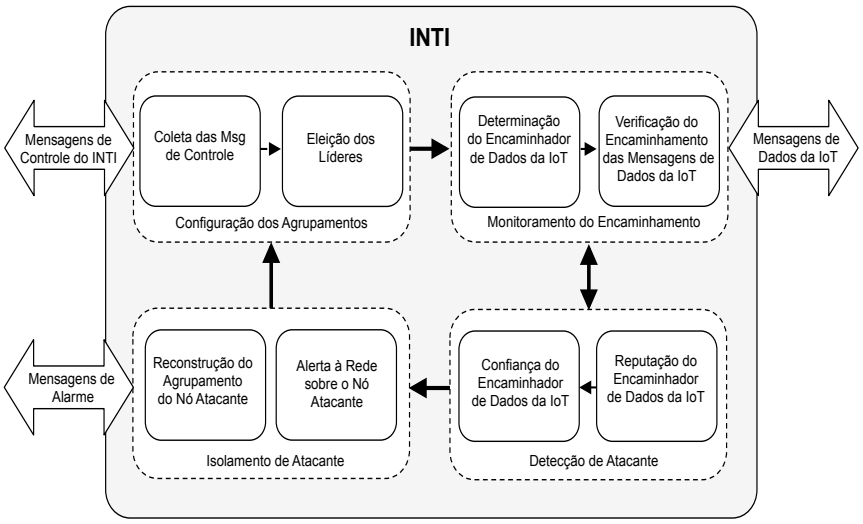

Figura 4.1: Arquitetura do INTI

O sistema INTI tem as seguintes propriedades: A **auto-organização** ajuda na coordenação e cooperação dos nós para a configuração da rede. A **auto-reparação** auxilia na detecção de um nó falho, onde se um nó for líder os nós ligados a ele procuram outro agrupamento ou formam seu próprio agrupamento fazendo a eleição de um novo líder para manter a estabilidade da rede.

4.1.1 Modelo da rede

A rede IoT está formada por dispositivos heterogêneos, sendo estes dispositivos móveis. Fatores como adaptabilidade e reconfiguração são essenciais para a formação dos agrupamentos, isso é necessário devido a dinamicidade da rede. É comum observar a dinamicidade de agrupamentos quanto aos seus líderes [110, 111], e quanto à mobilidade dos nós [112, 113], apresentando assim diferentes características e vantagens como menor consumo de energia e garantindo maior escalabilidade, entre outras. O uso de dispositivos móveis permite mobilidade para o s usuários e assim controlar suas (coisas/objetos), além de acessar a suas informações de forma decentralizada empregando objetos como *notebooks*, *PCs*, *PDAs*, *smartphones* e *tablets*, por exemplo.

Assume-se que inicialmente todos os dispositivos começam livres assumindo um de três papeis: nó membro, nó associado ou 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 no encaminhamento de dados. Os nós líderes tem a função de coletar as informações dos nós membros e encaminhar para o destino. A Figura 4.8 ilustra as entidades da rede.

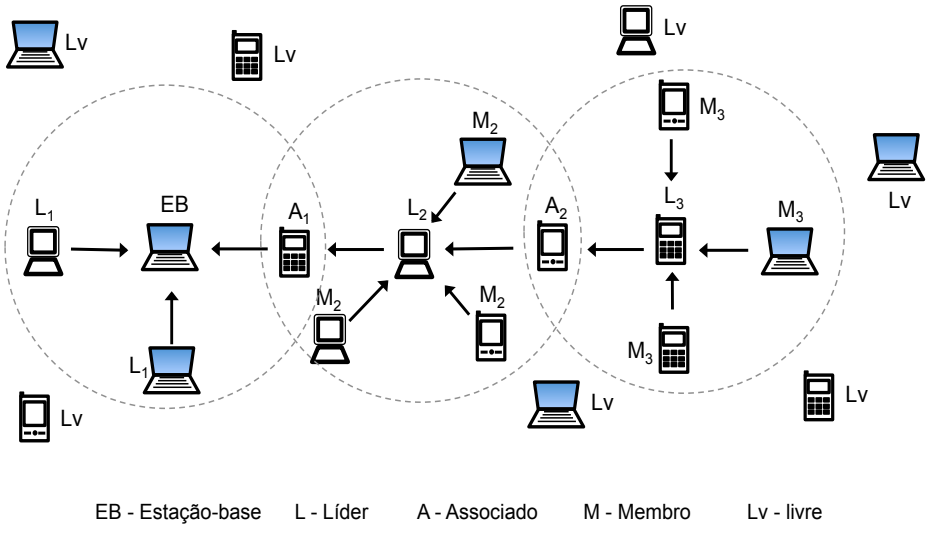

Figura 4.2: Entidades na rede

Assume-se que a composição da rede utiliza agrupamentos provendo escalabilidade e gerência de forma eficiente. 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 transmissão dos pacotes de dados da IoT para o destino pretendido ocorre nesta hierarquia. 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 e contribuindo para um melhor controle dos nós membros da rede. A Figura 4.3 ilustra a estrutura da topologia da rede, em que H. principal e H. auxiliar representas as hierarquias da rede.

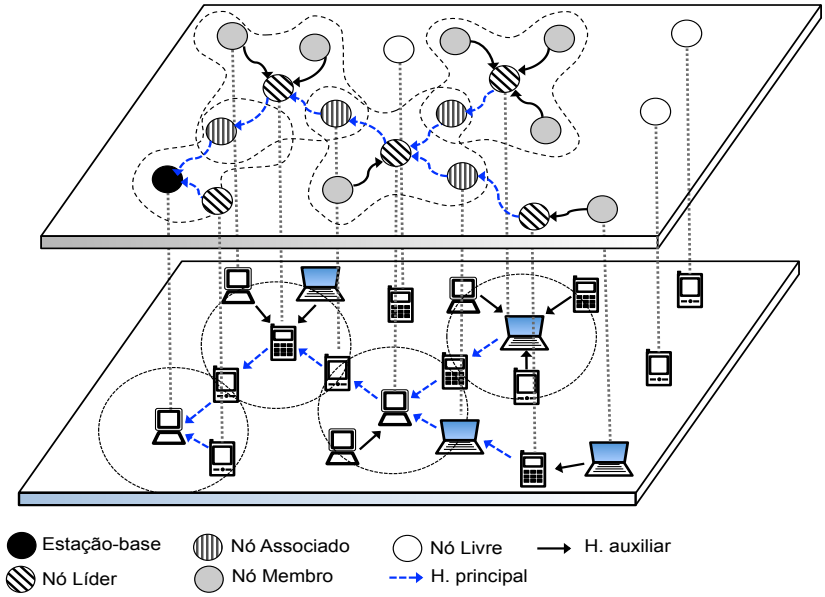

Figura 4.3: Estrutura da topologia

O INTI assume que a comunicação entre os nós móveis ocorre de duas formas, direta ou indireta. A comunicação direta acontece quando os nós membros localizam-se no raio de transmissão do nó líder ou quando os nós livres estão dentro do raio de cobertura da estação-base. Na comunicação indireta o encaminhamento de pacotes advém de múltiplos saltos (*multi-hop*), onde os nós membros dependem de outro nó para alcançar seu destino. Portanto, esta comunicação também permite ao sistema economizar o consumo de energia do nó. A abordagem de detecção escolhida para o ataque *sinkhole* tem como parâmetro o comportamento do nó na rede. Este tipo de detecção é vantajoso devido aos efeitos do ataque dentro da rede. Desta forma, a técnica de detecção baseada no comportamento na transmissão de mensagens utilizada no sistema é a reputação e na confiança de cada nó da rede. Esta técnica permite ao sistema detectar e tomar medidas reativas para o isolamento do ataque. A rede possui três modelos: o **modelo físico da rede**, o **modelo de comunicação** e o **modelo de ataque**.

Modelo físico da rede: O sistema INTI assume que a rede consiste em um conjunto P composto por n objetos (nós) identificados por $\{n_1, n_2, n_3, ..., n_i\}$, onde $n_i \in P$. Cada nó n_i possui um endereço físico ou identificador (ID) único. Além disso, cada nó periodicamente transmite uma mensagem de controle, mensagem de dados relacionados à IoT e se acontece um ataque propaga uma mensagem de alarme. A mensagem de controle é apresentada na Figura 4.4 ilustrando os campos utilizados na configuração dos agrupamentos.

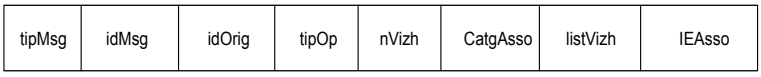

Figura 4.4: Mensagem de Configuração do Sistema INTI

A mensagem de controle contém os seguintes campos: o campo *tipMsg* permite diferenciar o tipo de mensagem realizada, que pode ser de controle, de dados ou de alarme. O campo *idMsg* guarda o identificador da mensagem enviada pelo nó origem, ele serve para contabilizar as mensagens que foram enviadas. O campo *idOrig* identifica o nó que enviou a mensagem. O campo *tipOp* identifica o tipo de operação a realizar. Este campo possui seis tipos de operações: (1) emissão é o anuncio de um nó dentro da rede; (2) publicação determina o número de nós vizinhos que um nó possui; (3) eleição do líder é o nó com o maior número de vizinhos. Caso dois líderes possuam o mesmo número de vizinhos o nó com o maior ID será o nó líder; (4) agrupar permite a formação dos agrupamentos, consistindo em que os nós vizinhos aceitam um nó como líder; (5) determinação dos nós associados no encaminhamento de dados de um agrupamento, caso em que dois nós associados encontram-se dentro da mesma área em comum de diferentes agrupamentos o nó com o maior índice de energia (IE) será escolhido como nó associado; (6) reconstrução permite realizar a manutenção do agrupamento afetado por uma falha, abandono do agrupamento ou por um ataque *sinkhole*. O campo *nVizh* armazena a contagem do número de vizinhos que possui um nó. O campo *CatgAsso* representa a classificação e função que desempenhará o nó. O campo *ListVizh* contém a lista dos nós vizinhos. Por último, o campo *IEAsso* representa o índice de energia do nó.

A mensagem de dados utilizada na IoT pelo INTI consistem em sete campos: o tipo de mensagem, o identificador da mensagem, o ID do origem, o identificador do nó encaminhador, o ID do destino, o *status* do nó e por último os dados da IoT, a Figura 4.5 mostra os sete campos da mensagem de dados da IoT.

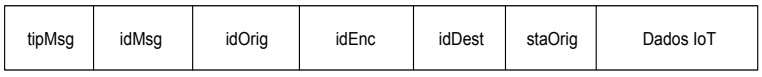

Figura 4.5: Mensagem de Dados do INTI

O campo *tipMsg* identifica a mensagem enviada, que pode ser de controle, dados ou de alarme. O campo *idMsg* corresponde ao identificador da mensagem enviada. O

campo *idOrig* é preenchido pelo nó que enviou a mensagem. O campo *idEnc* contém o identificador do nó que encaminhará as mensagens de dados para o destino. O campo *idDest* identifica o nó que receberá os dados enviados pelo nó origem. O campo *stOrig* armazena o valor do status do comportamento do nó na transmissão de mensagens. O campo *Dados IoT* possui a informação do dado sensoriado.

Outra mensagem utilizada pelos nós da rede ante a ocorrência de ataque é a mensagem de alarme. Esta mensagem está formada pelos seguintes campos: o campo *tipMsg* identifica a mensagem realizada, que pode ser de controle, dados ou de alarme. O campo *idMsg* guarda o identificador da mensagem enviada. O campo *idOrig* é preenchido pelo nó que enviou a mensagem. O campo *idAtaq* contém o identificador do nó *sinkhole*. A representação da mensagem de alarme é ilustrada na Figura 4.6.

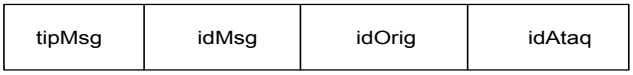

Figura 4.6: Mensagem de Alarme do INTI

Os nós utilizam o meio sem fio para comunicar-se. Esta comunicação é de forma assíncrona, ou seja, não existe tempo estabelecido para a transmissão dos dados. Desta forma, o canal de comunicação não é confiável, porque está sujeito à perda de pacotes devido a colisões e à entrada e saída dos nós devido à mobilidade que possuem. Todos os nós da rede começam livres, com os mesmos recursos e características como energia, capacidade de processamento, raio de transmissão, entre outras. A estação-base está fisicamente protegida, assim ela atua como uma autoridade central de confiança.

O sistema INTI assume que cada nó da rede desempenha a função de observador em relação aos vizinhos com a finalidade de conhecer seus comportamentos nas transmissões de mensagens. Sendo esta observação realizada da seguinte forma: a estação-base observa o comportamento de nós líderes e nós associados que encontram-se dentro de seu alcance de cobertura. Um nó membro e associado observam o comportamento de seu nó líder. Caso não existir um nó associado dentro do agrupamento, os nós membros observam o comportamento de seu líder. Por último, o nó líder observa o comportamento do nó associado pelo qual encaminhará as mensagens do agrupamento.

Modelo de comunicação: No funcionamento do sistema INTI, o protocolo de comunicação utilizado é uma variação do protocolo RPL. Este protocolo de roteamento respeita as limitações dos dispositivos que compõem a IoT como a energia, memória, processamento, entre outros. Sua desvantagem que ele funciona só em ambientes estáticos, ou seja, ele não foi projetado para aplicações em cenários móveis [114, 115]. O protocolo de comunicação empregado pelos dispositivos do sistema INTI possibilita a formação de agrupamentos e a mobilidade destes.

Modelo do ataque na rede: Cada nó da rede P não funciona apenas como um terminal de dados, ele também é responsável pelo envio e encaminhamento dos pacotes de

dados. Muitos ataques lançam informações maliciosas, roubando informações de privacidade. Desta forma, esses ataques afetam as propriedades de disponibilidade e integridade dos dados da rede. Um ataque tem como objetivo afetar o funcionamento normal da rede e pôr em perigo a sua segurança. O ataque *sinkhole* é uns dos ataques mais destrutivos em redes sem fio [31] porque o nó atacante não colabora no encaminhando dos dados descartando todos os pacotes ou encaminhando informação falsa para os demais nós da rede [116]. No sistema INTI, é assumido que um nó atacante pode vir a atuar como nó líder, nó associado ou nó membro, como ilustrado na Figura 4.7.

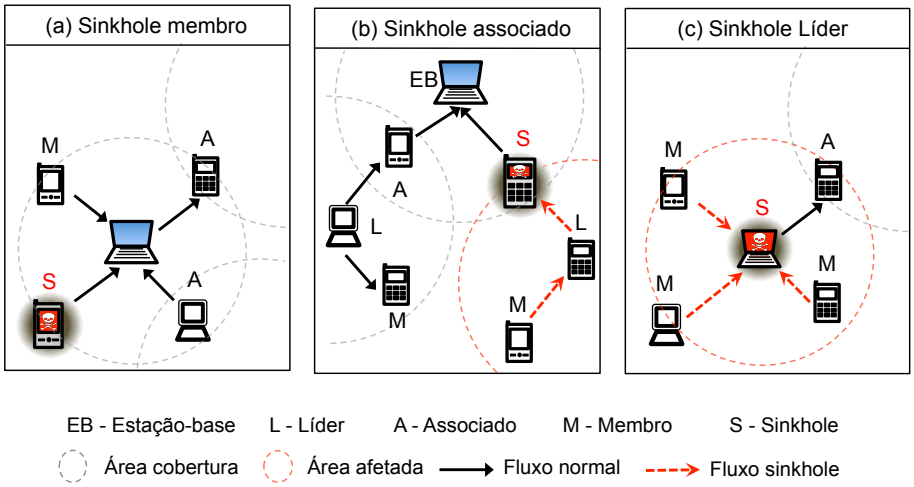

Figura 4.7: Modelo do Ataque Sinkhole

O ataque de roteamento *sinkhole* tem a caraterística de absorver o tráfego de uma certa área da rede ou posiciona-se entre a origem e o destino com o objetivo de depreciar e prejudicar o desempenho da rede. A detecção do nó atacante *sinkhole* ocorre por seu mau comportamento dentro da rede ao não encaminhar as informações enviadas pelos demais nós ou por injetar pacotes maliciosos para comprometer outros nós. Assume-se que qualquer nó da rede pode ter um bom comportamento durante um tempo e logo tornar-se um nó adversário.

4.2 INTI

O INTI possui quatro módulos: o *módulo de configuração dos agrupamentos*, *monitoramento do encaminhador, detecção de atacante* e de *isolamento de atacante*. Esses quatro módulos executam funções específicas para o funcionamento efetivo do sistema INTI na detecção e isolamento de ataques *sinkhole* garantindo proteção e segurança aos dispositivos em uma rede IoT. As próximas subseções descrevem detalhadamente cada um dos módulos mencionados que constituem o sistema INTI.

4.2.1 Configuração dos agrupamentos

Com a grande quantidade de dispositivos ligados à IoT surge um desafio, a necessidade de controlar esses dispositivos. Desta forma, o **módulo de configuração dos agrupamentos** gera uma hierarquia baseada em líderes, isto é, para a criação da topologia da rede. A técnica de agrupamento é muito difundida na organização de dispositivos (nós) na rede, o que pode, melhorar a qualidade dos dados, garantindo escalabilidade, estendendo a vida útil da rede e permitindo equilibrar a carga de comunicação e consumo energético. Esta abordagem é ideal para o controle de nós que formam a IoT.

Este módulo é subdividido em dois componentes: **Coleta das mensagens de controle** e de **Eleição dos líderes e associados**. Inicialmente todos os nós da rede começam livres transmitindo e *coletando mensagens de controle* dos nós vizinhos para a composição da rede. Estas transmissões de mensagens de controle são realizadas em *broadcasts* a fim de serem escutados por nós próximos. Neste componente, a coleta de mensagens de controle estima a quantidade de nós vizinhos possuem cada nó. Essas mensagens também são responsáveis por criar e manter a formação dinâmica da rede. Para a *eleições dos nós líderes e associados* são realizadas. A eleição dos nós líderes ocorre quando um nó possui a maior quantidade de nós vizinhos em relação aos nós que se encontram mais próximos.

Para a definição dos agrupamentos, os nós líderes anunciam-se aos nós vizinhos e aguardam sua solicitação a fim de criar o agrupamento. Cada nó livre elege um líder enviando uma mensagem de controle para o líder para juntar-se ao agrupamento. Formados os agrupamentos, os nós líderes verificam se alguns de seus nós membros receberam mais de uma mensagem controle de outro líder. Se um nó membro recebeu duas ou mais mensagens de diferentes líderes este nó membro é classificado como nó associado. Um nó associado estabelece a comunicação entre dois ou mais agrupamentos, sendo localizado dentro da área em comum entre ambos agrupamentos, como visto na Figura 4.8.

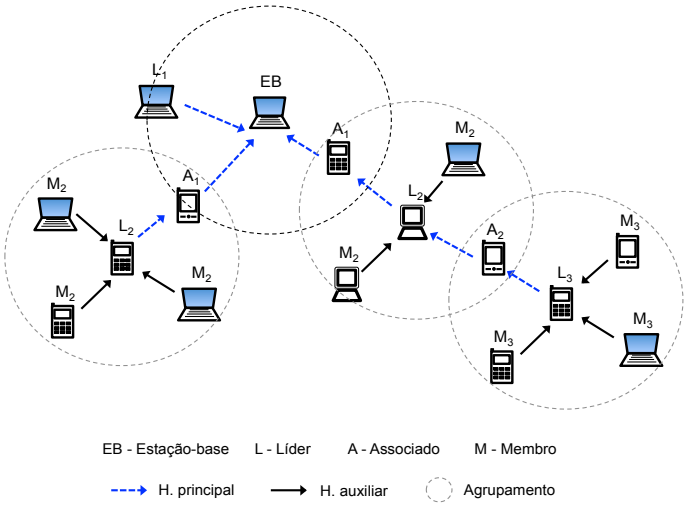

Figura 4.8: Configuração dos Agrupamentos

Caso existam dois nós membros dentro da mesma área de dois agrupamentos, o nó membro que possui a maior índice de energia (*IE*) tem a preferência. Por exemplo, no cálculo do IE_i do nó n_i é preciso saber o total de energia restante TEr_i que possui o nó n_i. A Equação 4.1 determina o valor calculado para TEr_i, onde TE_i é o total de energia do nó n_i e TEc_i é o total de energia consumida pelo nó n_i. Este cálculo mostra o total de energia restante no nó n_i. Permitindo assim ter um melhor controle sobre a quantidade de energia que possui cada nó livre.

$$TEr_i = TEi - TEc_i \tag{4.1}$$

Na Equação 4.2, observamos o cálculo do IE_i do nó n_i, onde TEr_i é o total de energia restante do n_i e TEc_i representa o total de energia consumida pelo nó n_i calculada na Equação 4.1.

$$IEi = \frac{TEr_i}{TEc_i} \tag{4.2}$$

A energia deve ser consumida de forma eficiente em todos os aspectos do sistema INTI para estender o tempo de vida da rede. A conservação da energia dos nós é a chave para a sobrevivência das redes sem fio. Algoritmos de agrupamento tais como [117, 118], são utilizados em redes sem fio para reduzir o consumo de energia. No sistema INTI a energia é considerada na escolha de um nó associado, no caso de ter dois ou mais nós membros dentro da mesma área comum entre dois ou mais agrupamentos.

No módulo de configuração dos agrupamentos, a reconstrução acontece quando um dos elementos da rede falha, abandona o agrupamento ou quando ocorre um ataque *sinkhole*. Se um nó membro é afetado por alguns destes problemas, o nó líder remove os IDs destes nós de sua lista, sendo que estes nós membros podem-se reagrupar em outros agrupamentos vizinhos. Se um nó líder falha ou abandona o agrupamento, os nós membros e associados realizam a operação de publicação para uma nova eleição de nó líder. Se um nó líder é um atacante *sinkhole*, os nós membros e associados realizam uma nova configuração dos agrupamentos. No caso que um nó associado falha ou abandona o agrupamento, existe a possibilidade do líder escolher outro nó associado, desde que este esteja dentro da área em comum. Uma área comum é o espaço que compartem diferentes agrupamentos. Sendo que o líder remove o ID deste nó de sua lista de vizinhos. Se o nó associado é um atacante *sinkhole*, o nó líder propaga uma mensagem de reconstrução para que os nós afetados realizem uma nova configuração dos agrupamentos e o nó líder superior coloca o identificador de nó atacante em sua *blacklist*. Caso contrario, se ambos líderes estão dentro do mesmo raio de transmissão, realiza-se uma fusão dos agrupamentos.

Para isso, o agrupamento que possui a maior quantidade de nós membros conterá ao outro agrupamento. Este método tem como finalidade minimizar o número de líderes da hierarquia principal e prover um melhor controle dos nós garantindo a escalabilidade da rede.

4.2.2 Monitoramento do encaminhador

Após estabelecidos os agrupamentos e classificados os nós como nós membros, associados e líderes, começa a coleta das mensagens de dados da IoT dos nós do agrupamento, a fim de encaminhar esses dados para o destino. Com as mensagens de dados enviadas desde os nós membros a seus nós líderes ou de um nó líder para um nó associado **encaminhador**. Um nó é considerado encaminhador quando este nó encaminha as mensagens de dados enviada por outros nós, como os nós associados e nós líderes, por exemplo. O **módulo de monitoramento do encaminhador** visa identificar nós suspeitos. Desta forma, este módulo permite alguns nós escutar as comunicações dos nós que se encontram localizados dentro de seu alcance de transmissão. Este módulo tem dois componentes: **determinação do encaminhador de dados da IoT** e de **verificação do encaminhamento das mensagens de dados da IoT**.

O componente de *determinação do encaminhador de dados da IoT* contabiliza o número de transmissões de entrada e saída realizadas pelo nó encaminhador. Para isso, os nós membros, associados e líderes monitoram e computam a quantidade de transmissões realizadas pelos nós encaminhadores em relação a suas próprias mensagens. Após realizada a contabilização das transmissões o valor é enviado ao componente de *verificação do encaminhamento das mensagens de dados da IoT* a fim de encontrar alguma suspeita. Este componente realiza uma verificação da quantidade de transmissões de entrada e saída realizadas pelo nó encaminhador. Se a quantidade de entrada é igual ao número de saída o nó encaminhador é considerado como nó normal. Caso contrario, o componente de verificação do encaminhamento das mensagens de dados da IoT assume uma suspeita. Este componente avisa ao módulo seguinte que encontrou uma suspeita entre os valores verificados. Para isso, este componente envia o $< ID, St >$ do nó suspeito. O ID representa o identificador do nó suspeito e o (St) representa o *status* do nó que determina o comportamento na transmissão de mensagens. Para isso, cada nó calcula seu *status*, utilizando a probabilidade da esperança futura *E(p)* calculado a partir da **função densidade de probabilidade Beta** ou simplesmente **função de densidade Beta** (FDP) [119, 120, 121, 39]. Com a função de densidade Beta pode-se determinar a probabilidade do comportamento futuro (*posteriori*) de um nó, baseado nos resultados de comportamentos passados (*priori*) para o cálculo do *status* de cada nó.

A função densidade de probabilidade (FDP) é denotada por $Beta(p|\alpha, \beta)$. Sendo, a distribuição a **priori** a função densidade de Beta uniforme [1;1], já no caso de ser inicial-

mente com valores de [0;1] representaria a ausência de informação sobre o comportamento do nó. Por isso, os valores assumidos por α e β são $\alpha = 1$ e $\beta = 1$. Entretanto, as iterações satisfatórias r e não satisfatórias s, seria a representação da distribuição a **posteriori**, sendo a FDP de Beta $\alpha = r + 1$ e $\beta = s + 1$ em que os valores das iterações são $r, s > 0$. Por exemplo, a FDP de Beta após de 6 iterações satisfatórias e 3 iterações não satisfatórias, então a distribuição *posteriori* é $\alpha = 7$ e $\beta = 4$. Para conveniência matemática a Equação 4.3 mostra a FDP que é denotada por $Beta(p|\alpha, \beta)$, sendo expressado através da função gamma (Γ), em que α e β representam as iterações satisfatórias e não satisfatórias passadas e em que p é a probabilidade de ocorrência de α e $(1 - p)$ é a probabilidade de ocorrência de β.

$$Beta(p|\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} = \frac{p^{\alpha-1}(1-p)^{\beta-1}}{B(\alpha, \beta)} \tag{4.3}$$

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

Essa densidade de probabilidade e sua expectativa estatística usa a função Beta, definida pela integral: $B(\alpha, \beta) = \int_0^1 t^{\alpha-1}(1-p)^{\beta-1}dt$, também chamada de integral de Euler de primeiro tipo. Onde o valor de p está entre $0 \leq p \leq 1$. Após calculado o FDP, a Equação 4.4 representa o cálculo do *status* de cada nó.

$$St = \frac{\alpha}{\alpha + \beta} \tag{4.4}$$

O valor do (St) é um valor continuo entre [0;1], onde os valores entre 0 e 0,4 apresentam um mau comportamento, e os valores maiores que 0,5 apresentam um comportamento normal. Portanto, este módulo atua durante todo o ciclo de vida da rede, a fim monitorar a quantidade de transmissões de entrada e saída pelos nós.

4.2.3 Detecção

O **módulo de detecção de atacante** identifica e revela a identidade do nó atacante. Este módulo utiliza duas avaliações determinando se um nó é bom ou atacante. Essas avaliações fundamentam-se nos cálculos da confiança e da reputação a fim de detectar um nó *sinkhole*. Tais avaliações são calculadas e atualizadas de forma constante mantendo a segurança e a integridade dos nós na rede. A seguir são descritos as medidas para a detecção de um nó atacante *sinkhole* dentro da IoT.

A primeira medida é conhecer o ataque *sinkhole*. Este ataque anuncia informações de roteamento erradas para atrair o trafego da rede [93, 95], depois de receber o trafego ele encaminha alguns ou nenhum pacote para o destino ou realiza alguma manipulação de

dados, além de injetar dados falsos para comprometer outros nós, a fim de prejudicar um ponto de coleta.

A segunda medida consiste em definir por qual característica detectar o ataque *sinkhole*. A detecção deste ataque é complexa devido a que pode ser "aparentemente transparente", no entanto, seus efeitos são bastante pronunciados [122]. A detecção do ataque se realizará **pelos pacotes que podem encaminhar ou não** para o próximo salto ou destino.

A terceira medida determina o método ou técnica para detectar o ataque *sinkhole*. Para isso, esta proposta adota uma abordagem baseada na reputação de cada nó que é representada por (R) e pela confiança representada por (C), a fim de detectar nós *sinkhole*. Desta forma, o cálculo da reputação e da confiança determinará se um nó é bom ou atacante *sinkhole*. Portanto, esses cálculos permitem brindar maior segurança e proteção aos nós da rede.

O *cálculo da reputação do encaminhador de dados da IoT* reflete o foco de uma relação de confiança. A reputação é a opinião ou percepção que uma entidade cria através de iterações, ações ou informações. Sendo estas iterações de modo direta ou indireta com base a tarefas passadas [120]. A distribuição Beta [39] fundamenta-se em dois tipos de iterações satisfatórias e não satisfatórias que cada nó realiza dentro da rede. Com o uso da distribuição Beta (α,β) pode-se representar a reputação e a confiança dos nós da IoT. A vantagem de usar esta distribuição é que os parâmetros utilizados são continuamente atualizados para determinar o comportamento de um nó dentro da IoT.

Na maioria dos sistemas existentes a reputação é representada como duas variáveis: crença e descrença sem considerar a incerteza. No entanto, o sistema INTI calcula essas três predições: incerteza (i), crença (c) e descrença (d) a partir da distribuição Beta (α,β). Os nós líderes, os nós associados e algumas vezes os membros do agrupamento realizam estes cálculos. Uma representação destas três predições no cálculo da reputação pode ser observada na Figura 4.9.

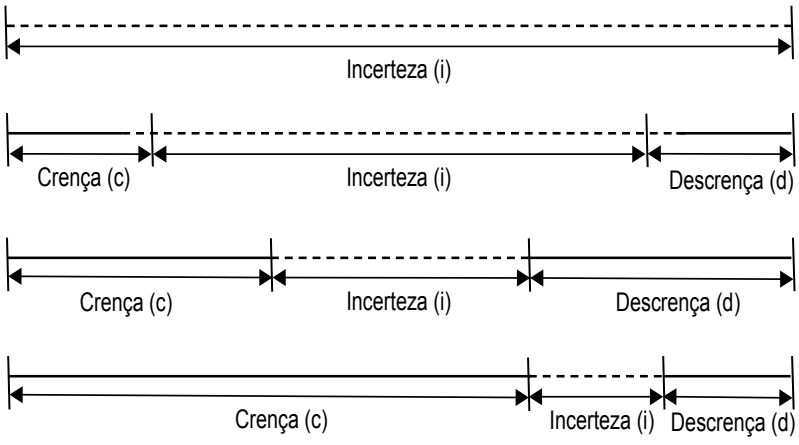

Figura 4.9: Representação das predições para a reputação

O cálculo destas três predições consiste em: $(i, c, d) \in (0, 1)^3 : i + c + d = 1$ respetivamente. Sendo que a somatória destas três predições seja igual a um. A Equação 4.5 representa o cálculo da incerteza computada pelos nós. Neste cálculo a incerteza é a variância normalizada da distribuição Beta. Sendo α e β obtidas da distribuição Beta.

$$i = \frac{12 * \alpha * \beta}{(\alpha + \beta)^2 * (\alpha + \beta + 1)} \tag{4.5}$$

A certeza total é $(1 - i)$ que pode ser dividida na crença (c) e na descrença (d) de acordo com a proporção de iterações. Considerando que a transmissão entre dois nós é de confiança é: $\frac{\alpha}{(\alpha+\beta)}$. A crença (c) é calculada seguindo a Equação 4.6.

$$c = \frac{\alpha}{(\alpha + \beta)}(1 - i) \tag{4.6}$$

Por último, a descrença (d) é derivada da crença (c). O cálculo da descrença (d) é alcançado seguindo a Equação 4.7, em que (i) representa a incerteza e (c) a crença em relação às predições de um nó.

$$d = (1 - i) - c = \frac{\beta}{(\alpha + \beta)}(1 - i) \tag{4.7}$$

Após obtidos os cálculos das predições (i, c, d) é possível computar a reputação. A reputação de um nó é calculada a partir das experiências baseadas nas predições computadas diretamente. O cálculo da reputação é realizado levando em consideração o *status* (St) do nó que encaminhou as mensagens de dados da IoT. Como se mencionou anteriormente o St representa como o nó se comporta no encaminhamento de mensagens. No entanto, o St e as predições (i, c, d) computadas são os dados de entrada para o uso da teoria de *Dempster-Shafer*, a fim de detectar e reduzir os falsos alarmes. Um nó decide de acordo com o valor obtido após aplicar a teoria *Dempster-Shafer* se um nó é bom ou um atacante dependendo do valor calculado. Este valor da reputação é um valor continuo dentro dos limites R[0;1], se o valor calculado é maior ou igual a 0,5 considera-se um nó bom, caso contrario, é considerado um nó atacante.

O quadro de discernimento consiste de duas possibilidades relativas à suspeita do nó $n_i : \Omega\{T, \overline{T}\}$, em que T significa que o nó n_i tem boa reputação e o $\overline{T}$ significa que é atacante *sinkhole*. Para Ω se tem três hipóteses: $H = T$ que n_i é bom; hipóteses $\overline{H} = \overline{T}$ que n_i não é bom e a hipótese $U = \Omega$ que representa a indecisão se n_i é bom ou é um atacante. Se o nó Líder (L_1) afirma que o nó membro (m_2) é bom, então a sua atribuição de probabilidades é dada na Equação 4.8, em que c representa a crença do nó n_i.

$$
\begin{aligned}
m_2(H) &= c \\
m_2(\overline{H}) &= 0 \\
m_2(U) &= 1 - c
\end{aligned} \tag{4.8}
$$

No caso em que o nó líder (L_1) afirma que o nó membro (m_2) não é bom, então a sua atribuição de probabilidades prévias será representada pela Equação 4.9, em que c representa a crença do nó n_i.

$$
\begin{aligned}
m_2(H) &= 0 \\
m_2(\overline{H}) &= c \\
m_2(U) &= 1 - c
\end{aligned} \tag{4.9}
$$

Da mesma forma, dadas as probabilidades prévias Equação 4.8 ou a Equação 4.9 para o nó m_2, se construirá suas atribuições básicas de probabilidade. Na Equação 4.10, se constrói as probabilidades para o nó (m_2), em que K representa a normalização das crenças, sendo representado por $K = \sum_{L \cap M = \emptyset} m_1(L)m_2(M)$, em que $m_1(L)$ é obtido do St recebido pelo nó e $m_2(M)$ representa a opinião realizada pelo L_1, onde o resultado da reputação é dado pelo valor de $m_1(H) \oplus m_2(H)$ para m_2 , sendo este um valor continuo entre $0 \leq m_2 \leq 1$, este resultado de m_2 é considerado $m_2 < 0,5$ como nó atacante e com valor de $m_2 \geq 0,5$ representará um nó bom.

$$
\begin{aligned}
m_1(H) \oplus m_2(H) = &\quad \frac{1}{K}[m_1(H)m_2(H) + m_1(H)m_2(U) + m_1(U)m_2(H)] \\
m_1(\overline{H}) \oplus m_2(\overline{H}) = &\quad \frac{1}{K}[m_1(\overline{H})m_2(\overline{H}) + m_1(\overline{H})m_2(U) + m_1(U)m_2(\overline{H})] \\
m_1(U) \oplus m_2(U) = &\quad \frac{1}{K}[m_1(U)m_2(U)],
\end{aligned} \tag{4.10}
$$

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

No *cálculo da confiança do encaminhador de dados da IoT* (C), a confiança representa a honestidade que tem uma entidade em relação a outra. Após o cálculo da reputação entre dois nós, calcula-se a confiança. No cálculo da confiança se considera dois valores (γ, δ), sendo estes calculados seguindo a Equação 4.11 em que u é computado a partir do número de iterações (m) realizadas entre dois nós, um nó observador n_j e um nó encaminhador n_i, sendo este número representado por m: $u = 1 - \frac{1}{m}$, em que u possui

valores entre $0 \leq u \leq 1$ é um fator que permite encontrar a confiança para um nó e R representa a reputação do nó.

$$\gamma = u\gamma + R \quad ; \quad \delta = u\delta + (1 - R) \tag{4.11}$$

A Equação 4.12 representa o cálculo da confiança, em que γ e δ são valores que representam as iterações onde $\gamma, \delta > 0$. O valor da confiança calculado é um valor continuo entre [0,1] com um valor neutro de 0,5. Se o valor obtido é maior que 0,5 até 1 o nó é considerado bom mas se o valor está dentro dos limites de 0 e 0,5 o nó é considerado atacante.

$$C = \mathbf{E}(Beta(\gamma + 1, \delta + 1)) = \frac{\gamma + 1}{\gamma + \delta + 2} \tag{4.12}$$

Com o cálculo da reputação e da confiança dos nós de cada agrupamento da rede, o INTI ajuda a prover segurança e proteção aos dispositivos que compõem a IoT. Além disso, com o uso destes mecanismos, o INTI consegue garantir uma rede segura livre de ataques *sinkhole*.

4.2.4 Isolamento

Após detecção do nó atacante *sinkhole*, o **módulo de isolamento** recebe uma mensagem enviada pelo módulo de detecção. Este módulo tem como objetivo afastar o nó *sinkhole* da rede, isto é, que nenhum nó na função de nó membro, nó associado e nó líder estabeleçam comunicação com o nó *sinkhole*. Este módulo é subdividido em dois componentes: de **alerta à rede sobre o nó atacante** e de **reconstrução do agrupamento do no atacante**.

O componente de *alerta à rede sobre o nó atacante* recebe a mensagem enviada pelo módulo de detecção, esta mensagem consiste do <ID> do nó atacante. Após conhecer o identificador (ID) do nó atacante *sinkhole* detectado, este componente gera e propaga uma mensagem de alarme em *broadcast* para divulgar o ID do nó atacante para os demais nós da rede, a fim de colocar o ID do nó atacante na *blacklist* de cada nó da rede. Além disso, o componente de *reconstrução do agrupamento do nó atacante* gera outra mensagem para reparar o agrupamento afetado. Para isso, o nó que detectou o ataque promove o isolamento do atacante enviando uma mensagem de reconstrução para seus vizinhos.

Um nó atacante *sinkhole* assume três papeis, como nó membro, nó associado ou como nó líder, a fim de interromper a comunicação entre os agrupamentos da rede. No isolamento quando um nó *sinkhole* passa a formar parte de um agrupamento, este será isolado pelo nó líder ao não estabelecer comunicação com o nó *sinkhole*. Além disso, o nó *sinkhole* não será um atacante efetivo por ficar longe do alvo. O isolamento do nó *sinkhole* quando assume a função do nó líder, neste caso o nó associado e os nós membros isolam o nó

sinkhole. Estes nós deixam de transmitir mensagem de dados para seu líder e geram e propagam duas mensagens uma de alarme e a outra de reconstrução para realizar uma nova configuração do agrupamento afetado. No isolamento quando o nó *sinkhole* assume a função de nó associado, o nó *sinkhole* será isolado pelo nó líder. Sendo que o nó líder deixará de transmitir, e propagará uma mensagem de reconstrução para os nós afetados, a fim de formar um novo agrupamento e seguir transmitindo.

4.3 Funcionamento do INTI

Esta seção detalha o funcionamento do sistema INTI na detecção e isolamento de ataques *sinkhole* em uma rede IoT. É apresentado o funcionamento do INTI desde a criação dos agrupamentos na rede até a detecção e isolamento do ataque. Em seguida, a Subseção 4.3.1 detalha a configuração e formação dos agrupamentos, a Subseção 4.3.2 apresenta como acontece a comunicação no sistema INTI. Por último, a Subseção 4.3.3 detalha como o sistema INTI detecta e isola um nó atacante.

4.3.1 Configuração da rede

O funcionamento do sistema INTI tem como base criação de agrupamentos formados por nós membros e nós líderes gerando uma hierarquia na rede. Ademais, da escolha dos nós associados para a conexão entre agrupamentos vizinhos para o encaminhamento das mensagens de dados. Inicialmente a rede consiste em um conjunto P composto por n objetos (nós) identificados por $\{n_1, n_2, n_3, ..., n_i\}$, onde todos os nós começam livres transmitindo e coletando dados de controle. O INTI é executado em cada nó da rede permitindo detectar e isolar um nó *sinkhole*, como ilustrado na Figura 4.10.

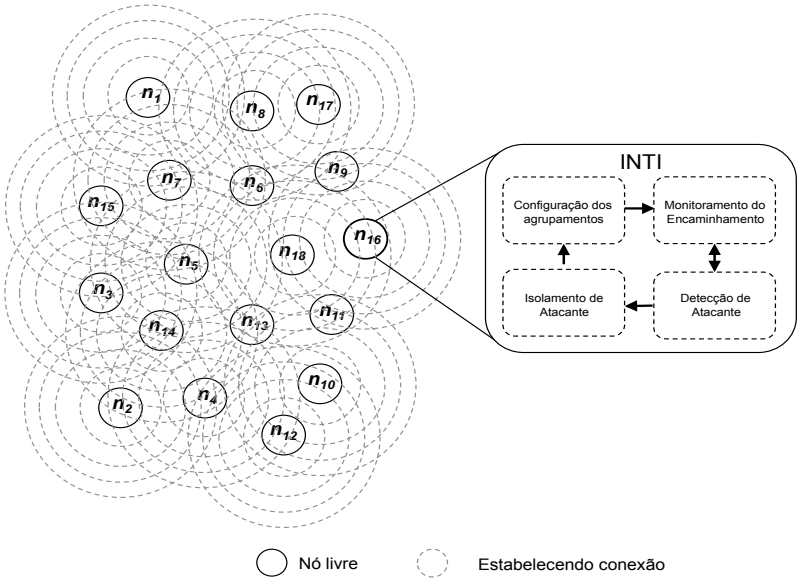

Figura 4.10: Inicialização para a formação dos agrupamentos no INTI

O algoritmo 1 apresenta o funcionamento para a configuração dos agrupamentos. Periodicamente, os nós transmitem mensagens de controle em *broadcast* informando seu identificador, categoria do nó, índice de energia, tipo de operação e a quantidade de vizinhos *(l.2)*. A função *Send* é responsável por transmitir esta mensagem para todos os nós vizinhos. Deve-se notar que o envio periódico destas mensagens insere sempre um tempo aleatório da ordem de milissegundos para evitar transmissões simultâneas, minimizando o número de possíveis colisões *(l.3)*. As variáveis que controlam esse tempo são *interval*, que é o período pré-determinado de envio e *rand()* que serve para adicionar uma variação no tempo de envio das mensagens. A função *EscolherLider (l.6)*, é utilizada para a eleição do nó líder. A informação considerada para a eleição do nó líder é o número de vizinhos. O número é computado através das mensagens de controle que um nó recebeu. Após conhecida a quantidade de vizinhos os nós publicam esta informação para os nós vizinhos *(l.8-10)* a fim de realizar a eleição do nó líder. Para isso, o nó que possui o maior número de vizinhos é escolhido como nó líder, desta forma, este nó muda de categoria, sendo classificado como nó líder *(l.11-15)*. Cada nó da rede cria uma lista de vizinhos (*ListVizh*) baseado nas mensagens de controle recebidas *(l.17-21)*. Se a categoria de um nó transmissor é livre, o nó receptor adiciona a sua lista. Este algoritmo também permite remover um nó da lista quando este falha ou abandona o agrupamento. Esta estratégia é utilizada pois, se a mensagem recebida for de um nó membro, ao se tornar líder, o nó membro será classificado como associado e o novo nó líder consegue estabelecer comunicação. Caso a mensagem for de um nó associado, o novo líder apenas estabelece comunicação com ele.

Algoritmo 1 Configuração dos Agrupamentos

```
1:  procedimento EnviaBeacon
2:      Send(broadcast, beacon, Catg, id, Rank, idLider, Root, IE, Vizh, idMaior)
3:      Timer(EnviaBeacon, interval + rand)
4:  fim procedimento
5:
6:  procedimento EscolherLider
7:      se (Catg ⇔ Livre) então                          ▷ cada n_i publica sua quantidade de vizinhos
8:          se (VizhMsg > Vizh) então                    ▷ atualiza a quantidade de nós vizinhos
9:              Maior ← id                               ▷ armazena o id do nó
10:         fim se
11:         se (id ⇔ MaiorMsg) então        ▷ verifica o id do nó com a maior quantidade de vizinhos
12:             mudaCatg ⇐ Lider                         ▷ nó livre classificado como nó líder
13:         fim se
14:     fim se
15:     se ((CatgMsg ⇔ Associado ∨ Membro) ∧ (Vizh ⇔ 0)) então          ▷ escolha como nó líder
16:         mudaCatg ⇐ Lider
17:     fim se
18:     se (CatgMsg ⇔ Livre) então
19:         insertList[Livre] ← {&ListVizh, idMsg, CatgMsg}      ▷ adiciona o nó na lista Vizinhos
20:     senão
21:         deletList[Livre] ← {&ListVizh, idMsg}                ▷ remove o nó da lista Vizinhos
22:     fim se
23: fim procedimento
```

Com a eleição dos nós líderes e a criação das listas de vizinhos *ListVizh* de cada nó, sendo constantemente atualizada com a troca de mensagens de controle, permitindo-se saber quais nós na vizinhança do nó atual são vistos como possíveis nós membros. Assim, o líder anuncia-se aos nós vizinhos como líder e aguarda a solicitação dos nós livres a fim de criar o agrupamento, como apresentado no Algoritmo 2. Desta forma, cada nó responde enviando uma mensagem de controle para o nó líder para formar parte do agrupamento, sendo estes nós classificados como nós membros e adicionados à lista do nó líder para o controle dos nós pertencentes ao agrupamento *(l.2-8)*. Este algoritmo também serve quando um nó for livre e ele recebe a mensagem de controle do nó líder, o nó livre muda sua classificação para nó membro e passa a comunicar-se com o nó líder.

Algoritmo 2 Processo de Agrupamento

```
1: procedimento CLUSTER
2:     se (Catg ⇔ Lider) ∧ (CatgMsg ⇔ Lider) então        ▷ formação dos agrupamentos
3:         mudarCatg ⇐ Membro
4:         conectRoot ⇐ idMsg
5:         conectLider ⇐ idMsg
6:     fim se
7: fim procedimento
```

A Figura 4.11 mostra a rede após da formação de agrupamentos, a eleição dos nós líderes e classificação dos nós membros. Onde os nós n_1, n_6, n_{14}, n_{10} foram eleitos como nós líderes por possuir a maior quantidade de nós vizinhos. Além disso, os nós n_7, n_5, n_9 desenvolvem a função de nós membros, sendo o nó n_6 seu nó líder. Os nós n_{15}, n_{16}, n_{18} não formam parte da rede, já que eles não pertencem a nenhum agrupamento. A conexão dos nós membros com o nó líder esta denotada pelas setas pretas. Desta maneira, qualquer nó da rede conseguirá transmitir seus dados da IoT para seu líder.

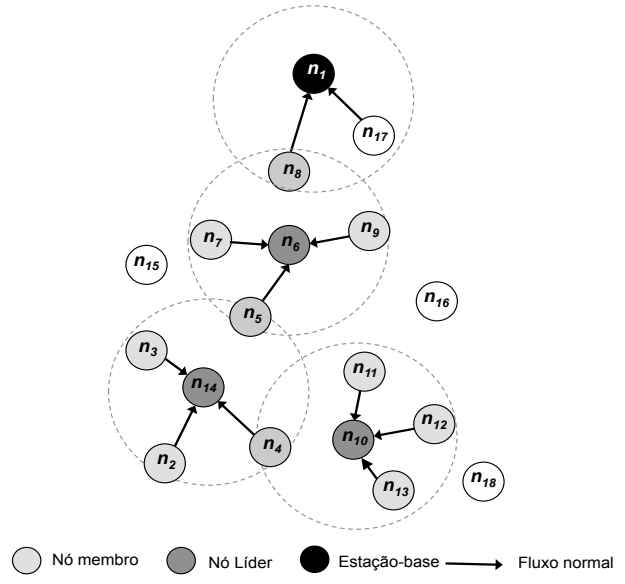

Figura 4.11: Ilustração dos agrupamentos formados no INTI

4.3.2 Comunicação

Uma das funções principais em uma rede é a comunicação entre as partes participantes da rede. Esta rede utiliza comunicação multi-saltos (*multi-hop*) para disseminar as informações coletadas pelos nós membros até o nó destino. Esta comunicação ocorre através dos próprios nós, que funcionam como roteadores para encaminhar os pacotes até o destino. Porém, a comunicação permitirá que os nós da rede IoT possam trocar informações. No Algoritmo 3 a linha *(l.2-6)* apresenta um caso especial realizado quando um nó está no alcance do ponto de coleta, esse nó será classificado como nó associado independentemente da função que está realizando. Um nó membro é classificado como nó associado quando este nó recebeu mais de uma mensagem de controle de diferentes líderes *(l.7-10)*. Para reiniciar o estado de um nó é executada *(l.12)*, a fim que o nó associado volte a ser um nó membro. A função escolhe associado *(l.18)* apresenta a fase de reagrupamento quando um nó associado é afetado por algum problema como falha ou abandono do agrupamento. Neste algoritmo se realiza uma nova escolha do nó associado, a fim de manter a comunicação entre diferentes agrupamentos. No caso em que existam dois nós associados dentro da mesma área comum de dois agrupamentos, é levado em consideração o nó que possua o maior índice de energia (IE). A utilização do índice de energia serve para garantir um maior equilíbrio na utilização da energia dos nós, evitando a exaustação deles.

Algoritmo 3 Determinação dos nós associados

```
1:  procedimento NoViraAssociado
2:      se (CatgMsg ⇔ PtColeta) então                ▷ nós próximos do ponto de coleta
3:          mudarCatg ⇐ Associado
4:          conectRoot ⇐ idMsg
5:          conectLider ⇐ idMsg
6:      fim se
7:      se (Catg ⇔ Membro) então      ▷ nós escolhidos como nó associado só pode ser um nó Membro
8:          se (CatgMsg ⇔ Lider) então                ▷ Msg enviada pelo líder a seus nós Membros
9:              se (idLider ≠ idMsg) então    ▷ verificação do nó que recebeu Msg de diferentes Líderes
10:                 mudarCatg ⇐ Associado
11:             senão
12:                 Reset ⇐ TimerAssociado
13:             fim se
14:         fim se
15:     fim se
16: fim procedimento
17:
18: procedimento EscolheAssociado
19:     se (Catg ⇔ Lider) então          ▷ Msg enviado pelo líder para a escolha de um nó Associado
20:         se (CatgMsg ⇔ Associado) então              ▷ procura a existência de um nó Associado
21:             se (((Rank + 1) < RankMsg) ∧ (RankMsg ≠ id) ∧ (Rank < InfRank) ∧ (RootIE <
    IEMsg)) então                                    ▷ verificação de algum nó Associado
22:                 conectRoot ← {id, IEMsg}
23:             fim se
24:         fim se
25:     fim se
26: fim procedimento
```

A Figura 4.12 ilustra a rede após a escolha dos nós n_4, n_5, n_8 como nós associados e auxiliando no estabelecimento da conexão entre os agrupamentos e colaborando no encaminhamento das mensagens e na comunicação do sistema. Os nós associado e nós líderes formam a hierarquia principal (H. principal) formada pelos nós $n_{10}, n_4, n_{14}, n_5, n_6, n_8$ denotado pelas setas pontilhadas que têm como alvo o ponto de coleta representado por n_1, como mostra a Figura 4.12 (a).

Os nós membros são os nós que não são monitorados devido a que o ataque *sinkhole* não seria efetivo, devido a que o nó atacante não encaminharia nenhum dado de outro nó. Desta forma, qualquer nó da rede conseguirá encaminhar seus dados de IoT para o destino final como ilustrado na Figura 4.12 (b), onde o nó n_4 atuando na função de nó associado encaminha seus próprias mensagens e reencaminha as mensagens do agrupamento que tem como líder o nó n_{10}.

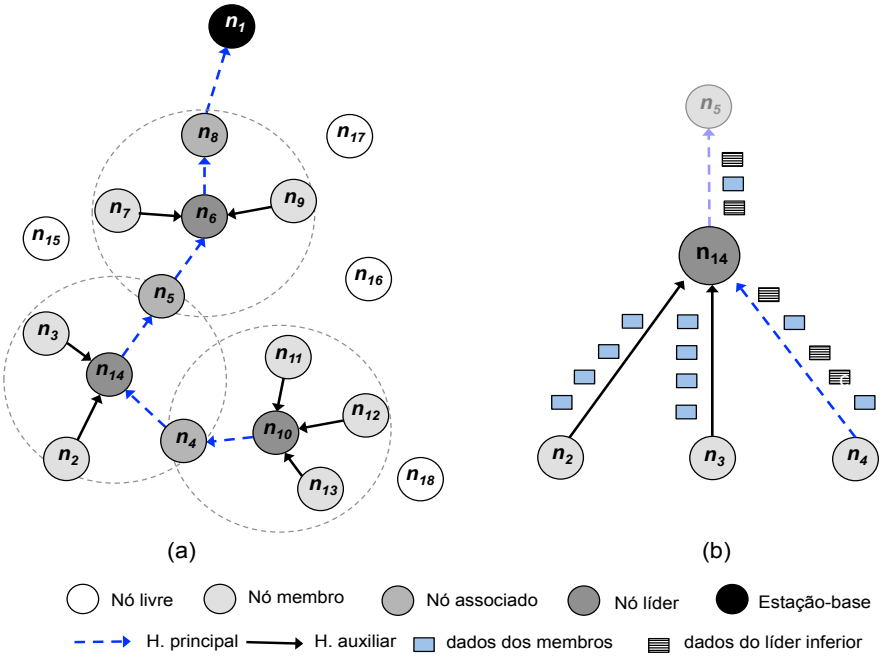

Figura 4.12: Representação da comunicação no INTI

4.3.3 Detecção de ataques sinkhole

Formados os agrupamentos e definidas as funções das entidades da rede, determina-se a ordem do monitoramento dos nós da rede. Esta ordem de monitoramento é que os nós membros e associados monitoram seu líder no encaminhamento de dados. Um nó líder monitora um nó associado que atua como encaminhador de dados de um agrupamento a outro. A detecção de um ataque *sinkhole* é realizada do nó observador para o nó encaminhador da rede.

O Algoritmo 4 detalha o monitoramento do comportamento dos nós encaminhadores através da contagem das mensagens encaminhadas. Cada nó executa esse algoritmo

quando envia uma mensagem de dados para seu nó líder ou para um nó associado. O nó n_i ao identificar seu nó encaminhador inicializa este procedimento monitorando a quantidade das mensagens enviadas, sendo armazenadas na variável *IteRations*. Para isso, cada vez que uma mensagem é transmitida, esta variável é incrementada *(l.3)*. A variável *bta* contabiliza as iterações incorretas do nó encaminhador *(l.4)*. No momento em que o nó encaminhador retransmite a mensagem, o procedimento *RetransmissaoEncaminador* entra em ação e realiza a verificação para certificar que a mensagem retransmitida foi a mesma que enviada pelo nó n_i *(l.11-12)*. Se o resultado for positivo, então a variável beta é decrementada *(l.13)* uma vez que a iteração com o nó encaminhador foi correta. Caso contrario, é enviada uma mensagem *inKlin* formada pela tupla <ID, St> nó encaminhador suspeito para o módulo de detecção, a fim de verificar se nó encaminhador com que o nó se comunica está se comportando de forma adequada *(l.14)*.

Algoritmo 4 Monitoramento do nó encaminhador

```
1:  procedimento MonitoraEncaminhador
2:      se ((Root ≠ 0) ∧ (Rank < InfRank)) então          ▷ determina o nó encaminhador
3:          IteRations[Root] ⇐ IteRations[Root] + 1   ▷ contabiliza as iterações com o nó encaminhador
4:          bta[Root] ⇐ bta[Root] + 1                          ▷ computa a variável beta
5:          Status ⇐ calculaStatus()          ▷ cálculo do status do nó encaminhador
6:      fim se
7:  fim procedimento
8:
9:  procedimento RetransmissaoEncaminhador
10:     se ((idEnc ⇔ Root) ∧ (idOrig ⇔ id)) então
11:         se (Sequencia ⇔ Pacote) então          ▷ verifica a sequencia da Msg enviada
12:             bta[Root] ⇐ bta[Root] − 1                  ▷ atualiza a variável beta
13:             af[Root] ⇐ IteRations[Root] + bta[Root]    ▷ computa a variável alfa
14:             InKlin ⇐ DetecRepConf(id, St)                          ▷ nó suspeito
15:         fim se
16:     fim se
17: fim procedimento
```

Um nó atacante *sinkhole* pode desempenhar três roles como nó líder, nó associado ou nó membro. Quando o nó *sinkhole* desempenha a função de nó líder, este será detectado pelos nós membros e o nó associado. O Algoritmo 5 foi implementado para detectar ataques *sinkhole* dentro da rede, após encontrado alguma suspeita. Neste algoritmo, *DetecRepConf (l.1)*, recebe os valores do <ID, St> do nó encaminhador detectado como nó suspeito para determinar se é um nó bom (normal) ou um nó *sinkhole*. Estes valores são baseados em seu comportamento na transmissão de mensagens. Para isso, o nó que detectou o nó suspeito utiliza suas próprias observações (valores) definidas em *(l.2-4)* no cálculo da reputação. Para este cálculo da reputação *(l.5)* são utilizadas as observações próprias do nó definida por c e o valor da qualificação do nó suspeito (St). Após disso, é também calculado a confiança do nó suspeito *(l.9)*. O sistema INTI considera um nó como atacante quando este possui uma reputação e confiança abaixo de [0,5], por conseguinte este nó não encaminhará as informações enviadas pelos demais nós *(l.10)*.

Algoritmo 5 Detecção de nós atacantes

```
1: procedimento DetecRepConf(id,St)
2:     i ⇐ uncertainty ← {af, bta}                          ▷ cálculo das predições do nó observador
3:     c ⇐ belief ← {af, bta}
4:     d ⇐ disbelief ← {af, bta}
5:     DetecRep ⇐ m ← {c, St}        ▷ calcula a reputação considerando a crença(c) e o status (St) do
   encaminhador
6:     u ⇐ 1 − (1/IteRations[Root]
7:     Gma ⇐ (u ∗ Gma) + DetecRep
8:     Dlta ⇐ (u ∗ Dlta) + (1 − DetecRep)
9:     Trust ⇐ (Gma + 1)/(Gma + Dlta + 2)                   ▷ calcula a confiança do nó suspeito
10:    se (DetecRep > 0.5) ∧ (Trust > 0.5) então            ▷ verificação do nó suspeito
11:        InKlin ⇐ "good"
12:    senão
13:        InKlin ⇐ "sinkhole"
14:    fim se
15:    retorna InKlin                                       ▷ retorna o valor da suspeita
16: fim procedimento
```

Após detectar um nó *sinkhole*, o nó que detectou o nó *sinkhole* promove o isolamento como apresenta no Algoritmo 6. Este algoritmo detalha o isolamento de nós atacantes para o qual gerar uma mensagem de alarme para divulgar o <ID> do nó que ameaça à rede. O procedimento *AlertaRede* definido na *(l.1)* é usado, a fim de colocar <ID> do nó atacante na *blacklist* de cada nó da rede. A *blacklist* é representada por *ListSinkhole (l.3-9)*. Além disso, o nó que detectou o ataque envia uma mensagem de reconstrução para os nós afetados *(l.14)*, a fim de formar um novo agrupamento ou fazer com que os nós se reagrupem em agrupamentos vizinhos*(l.15-16)*.

Algoritmo 6 Isolamento de nós atacantes

```
1: procedimento AlertaRede(InKlin)
2:     se (MsgTipo ⇔ Alarme) então                          ▷ Msg de Alarme
3:         se (IdMsg ⇔ Root) então
4:             insertList[Sinkhole] ← {&ListSinkhole, idAtaq}   ▷ adiciona o nó atacante à blacklist
5:             Send(broadcast, Alarme, id, Atacid)          ▷ divulgação do nó atacante
6:         fim se
7:         se (IdMsg ∈ ListFilhos) então          ▷ divulgação do nó atacante aos nós Membros
8:             insertList[Sinkhole] ← {&ListSinkhole, idAtaq}
9:             Send(broadcast, Alarme, id, Atacid)
10:        fim se
11:    fim se
12: fim procedimento
13:
14: procedimento Reestruturacao
15:    se (InKlin ⇔ Sinkhole) ∧ (Catg ⇔ Lider) então     ▷ Msg de restruturação se Líder é afetado
16:        EscolherLider()
17:    fim se
18:    se (InKlin ⇔ Sinkhole) ∧ (Catg ⇔ Associado) então ▷ Msg de restruturação se o Associado é
   afetado
19:        NoViraAssociado()
20:    fim se
21: fim procedimento
```

A Figura 4.13 ilustra a detecção e isolamento de um nó *sinkhole* dentro da rede P. A Figura 4.13 (a) ilustra quando um nó n_5 atuando como nó associado se torna um nó atacante *sinkhole*, afetando assim aos nós do agrupamento no encaminhamento de mensagens. Esta figura mostra também como os nós vão assumindo diferentes funções, isto é a causa da mobilidade que possuem os nós na rede. A Figura 4.13 (b) mostra como o nó atacante é detectado pelo nó n_{14} e o nó n_6 sendo que o nó n_5 qualificado como atacante. Também observa-se que m_1 representa ao nó observador, m_2 é o nó observado e R representa a reputação calculada pelos nós observadores sendo eles os nós que divulgaram a identidade do nó atacante e propagará a mensagem de reconstrução para o isolamento do nó atacante *sinkhole*, a fim de manter a estabilidade na comunicação dos agrupamentos.

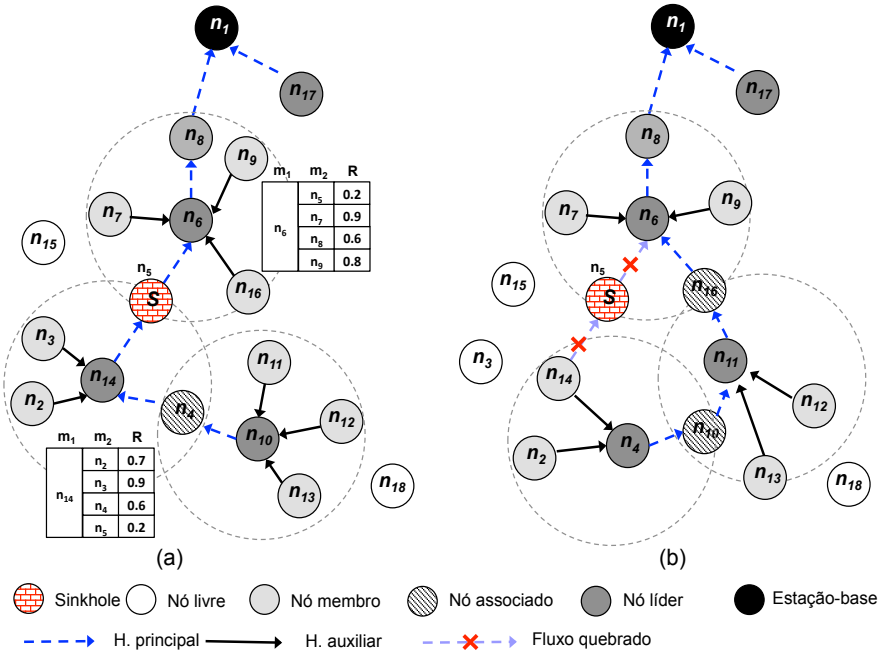

Figura 4.13: Detecção do ataque sinkhole pelo INTI

Como descrito anteriormente, o sistema tem as propriedades de ser **auto-organizado** com o objetivo de coordenar a cooperação dos diversos nós da rede para a detecção de um nó atacante. Este sistema é também **auto-reparável** já que ao ser detectado um nó adversário *sinkhole* os nós realizam o processo de agrupamento ou reagrupamento com a finalidade de seguir transmitindo suas informações.

4.4 Resumo

Este capítulo apresentou a descrição do INTI, um sistema de detecção contra ataques *sinkhole* para a proteção na IoT. O sistema é baseado na reputação e na confiança dos nós que atuam como encaminhadores de mensagens formando parte da rede. O INTI

é composto por quatro módulos: o módulo de configuração dos agrupamentos, para a criação e restruturação dos agrupamentos. O módulo monitoramento do encaminhamento controla e verificar o comportamento do nó encaminhador, a fim de encontrar alguma suspeita. O módulo de detecção de atacante, consiste em determinar se essa suspeita é verdadeira ou falsa detectando assim um ataque *sinkhole*. Por último, o módulo de isolamento de atacante é responsável por avisar e promover a separação do nó atacante da rede. O próximo capítulo apresentará a implementação e os resultados obtidos na validação.

CAPÍTULO 5

AVALIAÇÃO DO SISTEMA INTI

Este capítulo apresenta uma avaliação do sistema INTI na detecção de ataques *sinkhole*, considerando tanto a eficiência no consumo de recursos quanto a eficácia na detecção de nós atacantes. A Seção 5.1 apresenta o ambiente de simulação e os cenários empregados na avaliação. A Seção 5.2 descreve as métricas empregadas na medição da eficiência e da eficácia do INTI e do SVELTE. A Seção 5.3 e a Seção 5.4 apresentam e discutem os resultados da avaliação do INTI. Por fim, a Seção 5.5 mostra uma análise comparativa do sistema INTI e do SVELTE.

5.1 Ambiente e os cenários de simulação

A avaliação dos sistemas INTI e SVELTE é realizada empregando o simulador Cooja [123]. Este simulador é escrito em linguagem Java e foi desenvolvido especificamente para o ambiente IoT. A configuração de Cooja é flexível, de modo que várias partes do simulador pode ser facilmente substituído com uma funcionalidade adicional. Além disso, ele permite a configuração dos recursos de hardware e do software dos dispositivos (nós) e dos periféricos, como por exemplo a capacidade da memória de dados, sendo assim um simulador bastante flexível. O Cooja faz parte do sistema operacional (SO) Contiki [124], que é de código aberto, escrito em linguagem C. Os níveis de simulação do Cooja são ilustrados na Figura 5.1 em comparação com outros simuladores como NS2 [125], TOSSIM [126] e AVRORA [127].

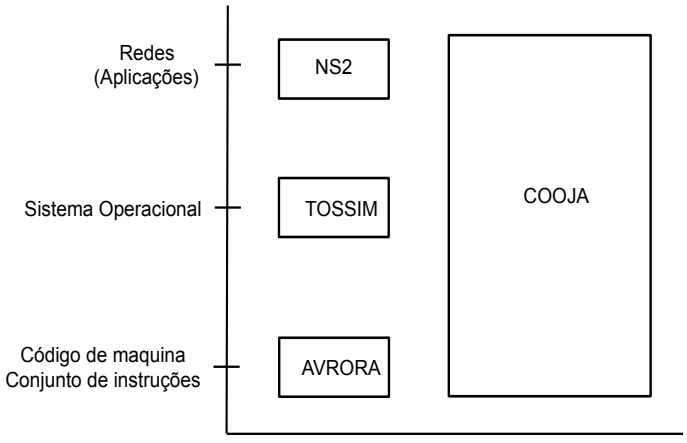

Figura 5.1: Simulação de Cooja em vários níveis

O sistema INTI e o ataque sinkhole foram implementados em linguagem Java e incluídos no simulador Cooja. Esta implementação foi realizada a fim de avaliar a eficácia e a

eficiência do sistema INTI diante detecção dos ataques sinkhole. Além disso, o sistema de detecção SVELTE e o protocolo RPL foram modificados a fim de poder estabelecer uma comparação entre o sistema INTI e o SVELTE.

A eficiência e a eficácia dos sistemas INTI e SVELTE serão avaliadas em ambientes próprios da IoT. O primeiro ambiente constitui um ambiente inteligente (smarthome) com dispositivos fixos. O segundo ambiente simulado corresponde um condomínio onde os usuários utilizam equipamentos sem fio, como celulares (smartphone), notebook, PDA (Ajudante Pessoal Digital) e outros dispositivos inteligentes, sendo estes dispositivos móveis e vulneráveis a ataques sinkhole. Estes cenários representam situações reais da IoT, relacionado à segurança como a troca de mensagens entre os dispositivos (nós) com limitações de recursos, tais como capacidade de processamento, memória, energia, a heterogeneidade dos dispositivos e outros requisitos específicos da IoT.

5.2 Métricas

Na avaliação da eficácia e da eficiência do INTI foram empregadas sete métricas. As métricas da eficácia aferem a quantidade de ataques sinkhole dentro da rede detectados, enquanto as métricas de eficiência medem o consumo de recursos utilizados por ambos sistemas nos cenários utilizados na avaliação. As métricas de eficácia definidas são a taxa de detecção de ataques *sinkhole* (Tx_{det}), a taxa de falsos negativos (Tx_{Fn}), a taxa de falsos positivos (Tx_{Fp}). As métricas de eficiência definidas são a taxa de entrega ($Tx_{Entrega}$), o consumo de energia (E_{gc}), a latência (L_T), e as funções assumidas pelos nós dentro da rede, como **número de líderes, número de associados, número de nós por líder e o número de nós solitários (livres)**. Esta última métrica é aplicada apenas ao sistema INTI, visto que o sistema SVELTE não permite a formação de agrupamentos dos nós. Todas as métricas empregadas são detalhadas a seguir:

A taxa de detecção do ataque sinkhole (Tx_{det}) contabiliza os ataques identificados corretamente pelo sistema INTI. O cálculo desta métrica é alcançada seguindo a Equação 5.1, em que X representa o total de iterações dos nós atacantes e os respectivos resultados obtidos pelo INTI, dado na forma de $X = (d, c)$, onde d é o valor da detecção realizada pelo sistema e c é a autêntica condição do nó $n_i \in P$, sendo P o conjunto de nós que conformam a rede. Esta métrica está determinada entre os valores de 0% e 100%, o valor mais próximo ao 100% denotam uma maior precisão do sistema.

$$T_{det} = \frac{\sum D_i}{|X|} \forall_i \in X \quad \text{onde} \quad D_i = \begin{cases} 1, & \text{se} \quad d_i = c_i, \\ 0, & \text{se} \quad d_i \neq c_i. \end{cases} \tag{5.1}$$

A 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 5.2, 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 5.1.

$$Tx_{Fn} = |X| - T_{det} \tag{5.2}$$

A taxa de falsos positivos (Tx_{Fp}) determina a quantidade de vezes que o sistema detectou um ataque *sinkhole* onde não existia o ataque. A Tx_{Fp} é calculada pela Equação 5.3, 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 a condição real do nó $n_i \in P$, onde $c=1$ significa um nó atacante e $c=0$ significa um nó bom.

$$Tx_{Fp} = \frac{\sum Dp_i}{|Z|} \forall_i \in Z \quad \text{onde} \quad Dp_i = \begin{cases} 1, & \text{se} \quad d_i = c_i, \\ 0, & \text{se} \quad d_i \neq c_i. \end{cases} \tag{5.3}$$

O 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 5.4, em que $\sum_{i=1}^{z} TE_i$ representa a somatória total de energia inicial de todos os nós da rede, e $\sum_{i=1}^{z} TE_r$ é o somatório total da energia restante dos nós. Onde $\sum_{i=1}^{z} n_i = 1$ e $\forall\ P$, n_i é qualquer nó pertencente à rede P, obtendo assim a energia total consumida quando é executado o sistema.

$$E_{gc} = \sum_{i=1}^{z} (TE_i - TE_r) \tag{5.4}$$

A taxa de entrega de pacotes ($Tx_{Entrega}$) determina o total de pacotes de dados recebidos com sucesso. O cálculo da $Tx_{Entrega}$ é apresentado na Equação 5.5, onde ($Tx_{Entrega}$) é obtida dividindo o número de pacotes recebidos pelo número de pacotes enviados pelo nó origem.

$$Tx_{Entrega} = \frac{NpacotesRecibidos}{NpacotesEnviados} X100 \tag{5.5}$$

A latência (L_T) é definida como a quantidade média de tempo entre o início da difusão de um conjunto de dados e sua chegada a um nó interessado em receber os dados. Assim, a latência mede o desempenho de tempo para cada mensagem individual. O cálculo da

L_T é apresentada na Equação 5.6, onde $\sum Tpfinal$ representa a somatória de tempo final e $\sum Tpinicial$ é a somatória de tempo inicial em que se enviou a mensagem.

$$L_T = \sum(Tpfinal) - \sum(Tpinical) \tag{5.6}$$

5.3 Avaliação em um ambiente doméstico

O ambiente doméstico corresponde a um cenário inteligente (*smarthome*), constituído por uma região de $60m$x$60m$. Neste cenário, para cada simulação assume-se uma quantidade de (dispositivos) nós fixos, 30, 40 e 50, que estão distribuídos de forma aleatória nos cômodos do ambiente, como visto na Figura 5.2. Além disso, um dado nó atua como nó destino, para onde os demais nós enviarão seus dados coletados. Os nós que se encontram nas extremidades alternadamente geram um pacote de dados, a cada período de intervalo de 10 segundos(s), e enviam este pacote ao nó destino. Os nós usam o canal sem fio, seguindo o modelo de propagação (*Unit Disk Graph Medium* (UDGM)) podendo assim os nós estabelecer comunicação dentro da rede. O tempo de simulação estabelecido nesta avaliação é de 1500s, e ele foi definido a fim de que os nós possam trocar uma quantidade de pacotes.

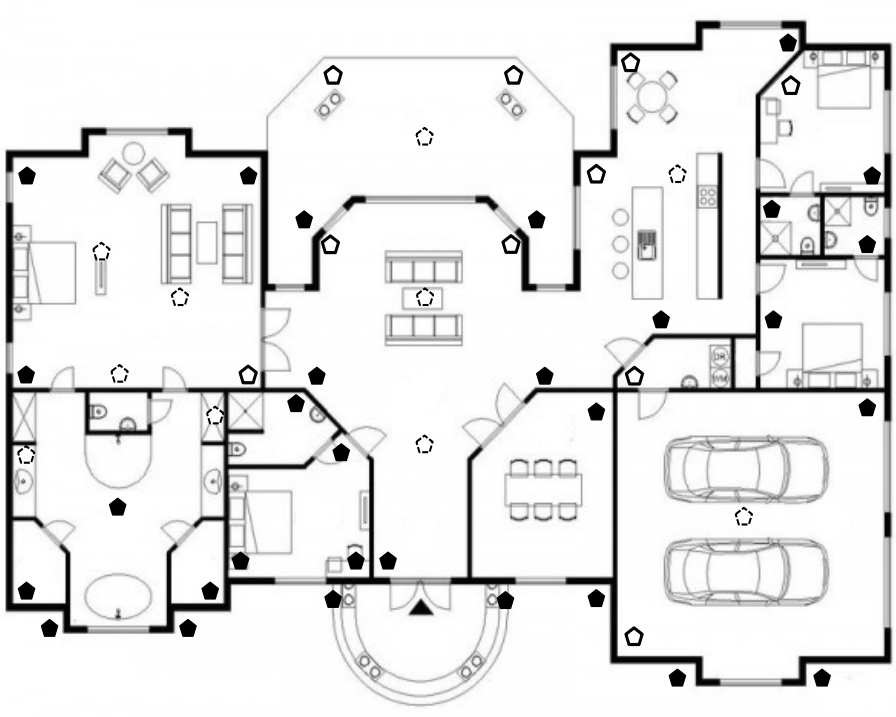

Figura 5.2: Cenário Smarthome

O INTI e o SVELTE utilizam o mesmo protocolo de roteamento, os nós usam o protocolo de transporte UDP, o raio de alcance dos nós varia de 10 metros (m), $20m$, $30m$

e $40m$. Neste cenário são consideradas as percentagens de 20% e o 30% de nós atacantes do total de nós utilizados nas simulações. Os nós atacantes agem de forma maliciosa durante todo o período da simulação e no momento do encaminhamento dos dados. Os resultados apresentados são as médias de 35 simulações e com um intervalo de confiança de 95%. Uma síntese dos parâmetros empregados nas simulações, e a variação dos valores utilizados para cada parâmetro do sistema de detecção INTI são detalhados na Tabela 5.1.

Parâmetro	**Valores**
Tipo de nó sensor	Tmote Sky mote
Número de nós	30, 40 e 50
Tempo de simulação	1500s
Raio de alcance	10m, 20m, 30m e 40m
Área	60x60 metros
Tipo de pacote utilizado	UDP
Tempo para gerar pacote de dados	10s
Padrão	IEEE 802.15.4
Canal sem fio	Unit disk graph Medium (UDGM)
Número de nós atacantes	20% e 30%
Taxa de dados	10^2 kbps

Tabela 5.1: Parâmetros de simulação do cenário

A Figura 5.3 ilustra o cenário visualizado dentro do simulador Cooja. Os dispositivos dos usuários são representados pelos pentágonos regulares que serão os nós da rede, sendo a comunicação representada pelas linhas que unem estes pentágonos regulares (nós). Esta comunicação é estabelecida cada vez que quando um nó encontra-se dentro do alcance de outro nó e vice versa.

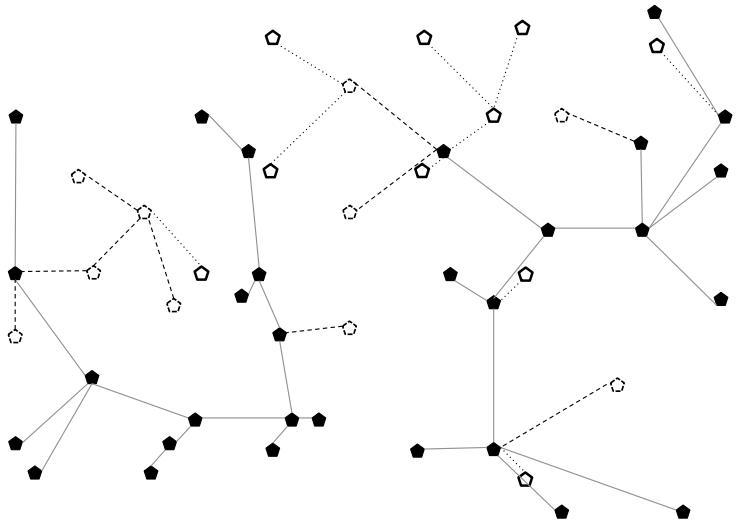

Figura 5.3: Visualização do cenário da simulação no Cooja

5.3.1 Resultados da eficácia

Essa subseção apresenta uma avaliação da eficácia do sistema INTI diante a detecção de ataques sinkhole, considerando as métricas taxa de detecção (Tx_{det}), taxa de falsos negativos (Tx_{Fn}) e taxa de falsos positivos (Tx_{Fp}). Uma comparação da eficácia do INTI e do SVELTE também levou em conta essas métricas.

As taxas de detecção de ataques sinkhole (Tx_{det}) alcançadas pelo INTI são mostradas nos gráficos da Figura 5.4. Os resultados obtidos consideram duas porcentagens de nós atacantes. No gráfico (a) da Figura 5.4, com quantidades de 30, 40 e 50 nós, onde 20% deles são nós atacantes, e com raio de alcance de $10m$, o INTI obteve uma taxa de detecção superior a 90%. Esta taxa de detecção acrescenta quando se aumenta a quantidade nós. No gráfico pode-se observar que quando o tamanho do raio de alcance aumenta para 20 e $30m$, o INTI alcançou também uma taxa de detecção superior a 90%. Isto ocorre porque o INTI identifica corretamente os nós sinkhole, e uma vez identificados estes nós atacantes são isolados da rede no momento da reconstrução da rede. No gráfico (b) da Figura 5.4 com quantidades de 30, 40 e 50 nós, onde 30% deles são nós atacantes, e com diferentes tamanhos de raios de alcance. A taxa de detecção de nós atacantes alcançada pelo INTI apresentou resultados similares como os obtidos no gráfico (a) da Figura 5.4. Portanto, o sistema INTI garanta uma taxa de detecção superior de 90% para diferentes quantidades de nós e para distintos tamanhos de raio de alcance. Além disso, os resultados obtidos pelo sistema INTI mostram uma alta confiabilidade. Isso ocorre devido à eficácia dos mecanismos utilizados pelo sistema INTI diante a detecção de nós atacantes.

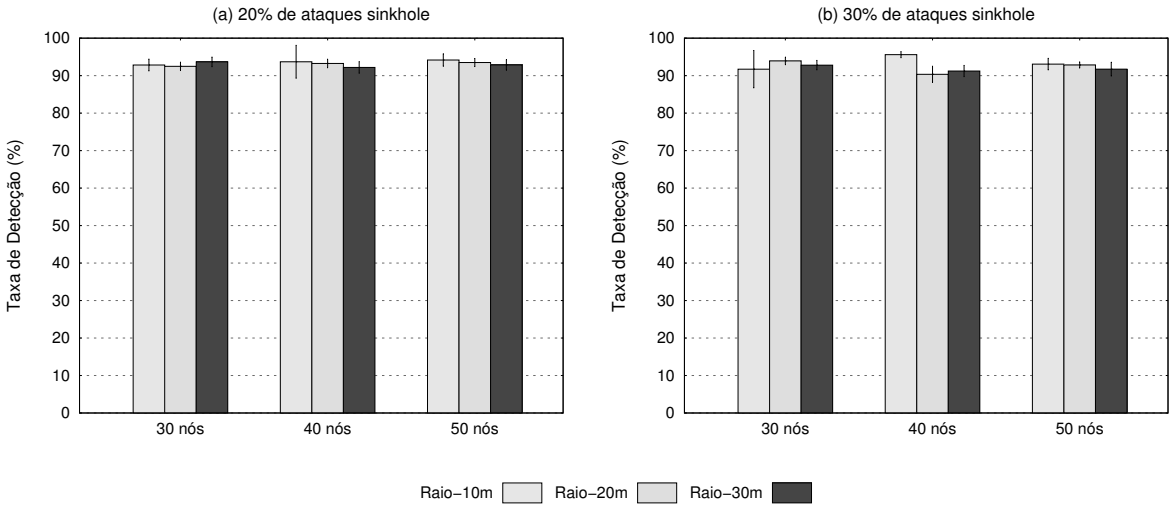

Figura 5.4: Taxa de detecção - Tx_{det} diante de ataques sinkhole

O sistema INTI atingiu uma pequena taxa de falsos negativos (Tx_{Fn}), como visto nos gráficos da Figura 5.5. No gráfico (a) da Figura 5.5, considerando uma quantidade de 30 nós, onde 20% deles são atacantes, e com raio de alcance de $10m$, o sistema INTI alcançou uma taxa de falsos negativos de 7% aumentado até 7.5% quando se usa um raio

$20m$. Ao empregar o raio de $30m$ a taxa de falsos negativos obtida pelo INTI diminui até o 6%. Esta diminuição ocorre devido aos mecanismos empregados no sistema INTI diante a detecção de ataques sinkhole. Para uma quantidade de 40 nós, e com raio de alcance de $10m$, a taxa de falsos negativos obtida pelo INTI é de 6%, quando o tamanho do raio de alcance é de $20m$, esta taxa é de 6.5% aumentando para 8.5% ao utilizar um raio de $30m$. Já com 50 nós, e com raio de alcance de $10m$, o sistema INTI atinge uma taxa de falsos negativos de 6.3% chegando aumentar a medida que aumenta o raio de alcance para 20 e $30m$ obtendo assim taxas de 7% e 7.5%. Consequentemente, a taxa de falsos negativos varia dependendo da quantidade de nós, atacantes e dos raios de alcances usados.

Pode-se observar que, no gráfico com 30 nós, onde 30% deles são atacantes, e com raio de alcance de $10m$, o INTI obteve uma taxa de falsos negativos inferior a 8% descendo até conseguir uma taxa do 5.5% ao usar um raio de $20m$. Isto ocorre devido a efetividade na detecção de ataques empregada pelo sistema INTI. Ao usar um raio de $30m$, o INTI atingiu uma taxa de falsos negativos de 7.5%. Com 40 nós, e com raio de alcance de $10m$, o sistema obteve uma taxa de falsos negativos de 4.7% e ao usar um raio de $20m$ a taxa de falsos negativos aumento para 9.7%. Já com um raio de alcance de $30m$, o sistema obteve uma taxa de falsos negativos de 7%. Para terminar, ao usar 50 nós com raio de $10m$ o sistema INTI atingiu a taxa de falsos negativos de 6%. Quando se usa um raio de $20m$ o resultado se estabiliza alcançando uma taxa de 5.5%. Finalmente, quando o raio de alcance $30m$ aumenta a taxa de falsos negativos se estabiliza em 6.5%, como ilustrado no gráfico (b) da Figura 5.5. Em conclusão, pode-se observar que ambos gráficos com diferentes porcentagens de nós atacantes o INTI obteve uma taxa de falsos negativos inferior a 9.5%, sendo que no uso com 30 e 40 nós, e com raio de alcance de $10m$ os resultados obtido não são confiáveis. Isto é devido à distribuição dos nós dentra da área simulada.

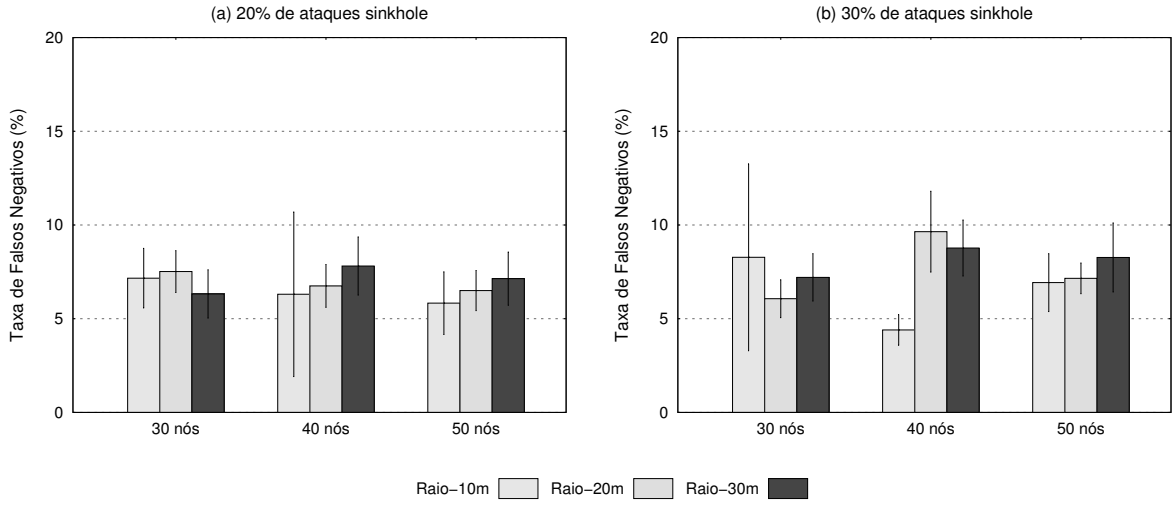

Figura 5.5: Taxa de falsos negativos - Tx_{Fn}

O sistema INTI obteve uma baixa taxa de falsos positivos (Tx_{Fp}), conforme visto nos gráficos da Figura 5.6. No gráfico (a) da Figura 5.6 com quantidade de 30 nós, onde 20% deles são atacantes sinkhole, e um raio de alcance de $10m$, o sistema INTI atingiu uma taxa de falsos positivos inferior a 2.5%. Ao aumentar o raio para $20m$ a taxa de falsos positivos aumentou em 1% sendo de 3.5%. Quando o raio de alcance é de $30m$, o INTI obteve uma taxa de falsos positivos de 3%. Já com 40 nós, e um raio de alcance de $10m$, a taxa de falsos positivos atingida é de 3.5% enquanto o raio de alcance aumenta para $20m$ esta taxa chega atingir o 5%. A taxa de falsos positivos aumenta a medida que o raio de alcance é de $30m$ alcançando o 5.5%. Com a quantidade de 50 nós, e um raio de $10m$, o sistema atinge uma taxa de falsos positivos de 5% aumentando até 7% quando o raio aumenta para $20m$. Ao usar um raio de $30m$ a taxa de falsos positivos diminui atingindo o 6.5%. Neste mesmo cenário com 30 nós, e onde o 30% deles são atacantes e com raio de alcance de $10m$, o sistema obteve a taxa de falsos positivos de 3%. Esta taxa de falsos positivos acrescenta para 4% e 5% ao aumentar o raio de alcance. Com 40 nós e com raio de $10m$, o INTI atinge uma taxa de 4%, ao aumentar o raio para $20m$ a taxa de falsos positivos é de 6.5% logrando aumentar até 10% a medida que se utiliza o raio de $30m$. Já com uma quantidade de 50 nós o sistema INTI mostra uma estabilidade nos resultados obtidos, considerando um raio de $10m$, sendo que o sistema obteve uma taxa de falsos positivos de 4.8%. Com um raio de $20m$ a taxa de falsos positivos diminui a 3.5%. Esta taxa aumenta consideravelmente quando se usa um raio de $30m$ alcançando uma taxa de falsos positivos de 11%, como visto no gráfico (b) da Figura 5.6. Estes resultados indicam que o sistema INTI identifica poucos nós confiáveis como nós sinkhole. Esta detecção equivoca pode ser devido à demora do nó ao encaminhar seus próprios pacotes e os pacotes de outro nó. Sendo que por um momento eles sejam considerados como nós suspeitos até corroborar com sua reputação e confiança.

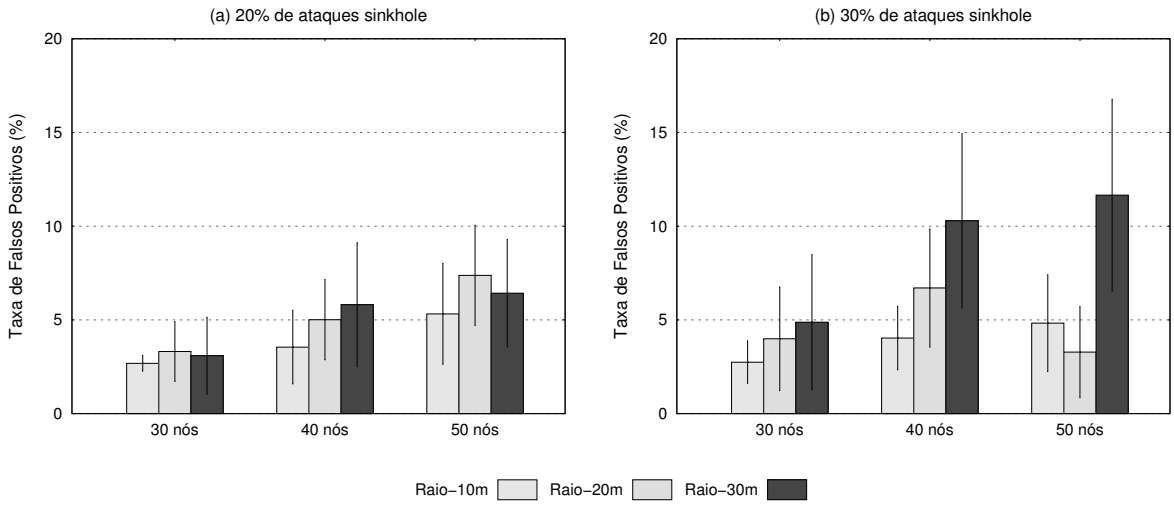

Figura 5.6: Taxa de falsos positivos - Tx_{Fp}

5.3.2 Resultados da eficiência

Essa subseção apresenta a avaliação da eficiência do sistema INTI na detecção de ataques sinkhole. As métricas que quantificam a eficiência são: as funções assumidas pelos nós como **número de associados, número de líderes, número de nós membros e o número de nós livres**, a taxa de entrega ($Tx_{Entrega}$), a latência (L_T) e para terminar o consumo de energia (E_{gc}). Os resultados obtidos pelas métricas utilizadas são apresentados a seguir.

As funções assumidas pelos nós no transcurso do tempo de simulação se pode observar no gráfico da Figura 5.7. Este gráfico mostra quantos nós assumem as diferentes funções desempenhadas dentro da rede. Esta figura apresenta um conjunto de gráficos que permitem determinar quantos nós conseguem-se comunicar com outros nós na rede. Inicialmente à esquerda, nota-se que avaliação com 30 e 40 nós usando o raio de alcance de $10m$. Pode-se ver que a quantidade de nós líderes e associados tem quase a mesma quantidade de 10 nós, sendo que a quantidade de nós membros e livres seja de quase 5 nós. As funções assumidas usando as mesmas quantidades de nós e variando o raio de alcance para 20, 30 e $40m$ a quantidade de nós desempenhando alguma função dentro da rede aumenta de forma proporcional para ambos cenários. Na simulação com 50 nós o crescimento na quantidade das funções assumidas pelos nós é de quase um 25% em comparação dos resultados obtidos na simulação com 30 nós e de um 10% em comparação com os resultados alcançados na simulação com 40 nós. Este aumento ocorre devido ao tamanho do raio de alcance empregado pelos nós dentro da rede podendo existir uma sobreposição de na cobertura da área. Com esta sobreposição a delegação de funções é a mais adequada fazendo com que mais nós se consigam comunicar. Além disso, devemos destacar que neste cenário não foi considerada a mobilidade para os nós.

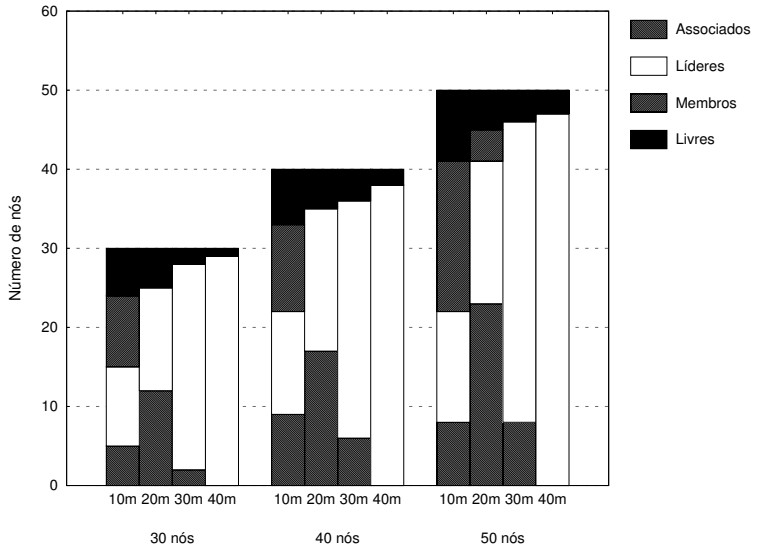

Figura 5.7: Funções assumidas pelos nós

A taxa de entrega ($Tx_{Entrega}$) mostrada no gráfico da Figura 5.8, observa-se que com 30 nós, e com raio de alcance de $10m$, o INTI atingiu a taxa de entrega de 97%, sendo similar à taxa alcançada quando se utilizou o raio de $20m$. Quando se aumenta o raio de alcance para 30 e $40m$, a taxa de entrega aumenta de maneira satisfatória chegando atingir o 100% e de 98%. Estes resultados obtidos são devido aos mecanismos empregados pelo INTI no encaminhamento de dados até alcançar o destino pretendido. Já com 40 nós e com raio de $10m$, o sistema alcançou uma taxa de entrega superior a 85%, enquanto se utiliza um raio de $20m$, o sistema atingi uma taxa de entrega de 95%, a medida que este raio aumenta para $30m$, o resultado da taxa de entrega obtida é similar que quando se utilizou o raio de $20m$, já com raio de alcance de $40m$, o resultado da taxa de entrega melhora alcançando o 100%. Neste mesmo cenário com 50 nós, e com raio de alcance de $10m$ a taxa de entrega obtida pelo sistema INTI é de 88%. Além disso, quando o raio é de $20m$ a taxa de entrega aumenta atingindo a taxa de 95%, já com raio de $30m$, o sistema INTI obteve uma taxa de entrega de 98% sendo o mesmo resultado que se conseguiu quando se aplicou um raio de alcance de $50m$. Entretanto, note-se que nos cenários com 40 e 50 nós com raios de alcance $20m$ e $30m$ apresentam quase uma igualdade. Isto ocorre porque a quantidade de nós e o raio de alcance usado são os adequados para estes cenários.

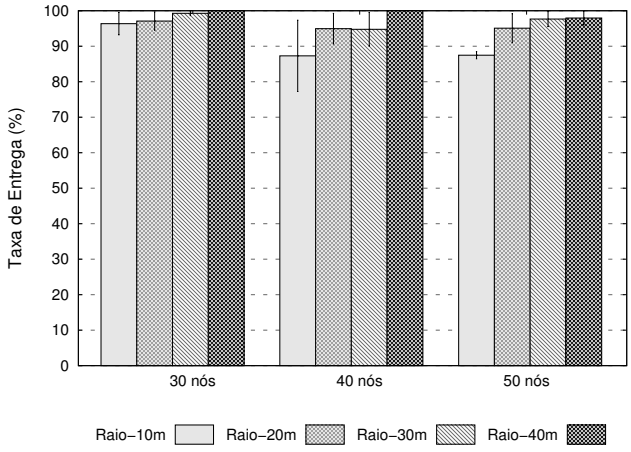

Figura 5.8: Taxa de entrega - $Tx_{Entrega}$

Verificamos que a latência (L_T) dada quando se varia a quantidade de nós da rede como é mostrada na Figura 5.9, diminui a medida que o tamanho do raio de alcance dos nós se amplia. Como pode-se observar inicialmente com a quantidade de 30 nós e com diferentes raios de alcance de 10, 20, 30 e $40m$ a latência é inferior a 69 milissegundos(ms) chegando a diminuir até os $25ms$ a medida que se amplia o raio de alcance dos nós. Com 40 nós e com diferentes tamanhos de raio de alcance a latência obtida é de $88ms$ chegando a diminuir até chegar a $25ms$. Para terminar, com uma quantidade de 50 nós e com um raio de alcance de $10ms$, inicialmente o INTI conseguiu alcançar uma latência de $87ms$ diminuindo até atingir uma latência de $25ms$ usando um raio de $40m$. Ademais, nota-se

que nos resultados obtidos usando 30, 40 e 50 nós com raios de 20, 30 e 40m latência é quase igual. Isto ocorre pois, a quantidade de nós e o raio de alcance são os ideais para este cenário. Nos seguintes gráficos não será considerado o raio de alcance de 40m, devido à área utilizada de 60mx60m, e portanto não representaria um cenário realístico da IoT.

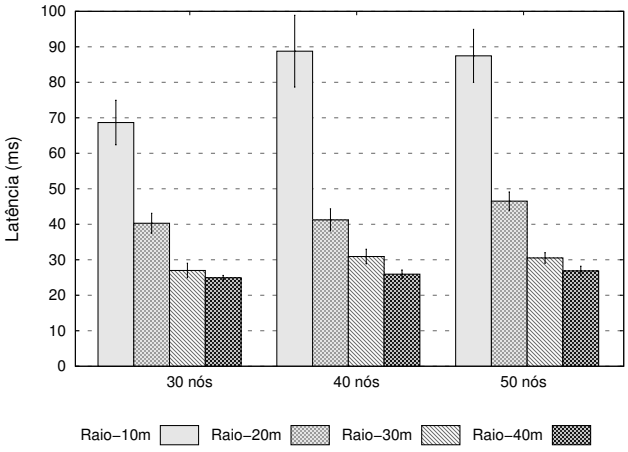

Figura 5.9: Latência -L_T

O consumo de energia (E_{gc}) alcançado pelo sistema INTI é apresentado no gráfico da Figura 5.10. Pode-se observar que a energia consumida pelo INTI é inferior a 30000 milíjoule (mJ). Com o uso de 30 nós o INTI apresenta um consumo de energia de 29000mJ logrando diminuir o consumo de energia até 27000mJ quando se usa uma quantidade de 40 nós. Já com 50 nós o sistema INTI ainda consegue diminuir seu consumo de energia atingindo os 25000mJ. Pode-se determinar que cada vez que aumenta a quantidade de nós dentro da rede o consumo de energia diminui. Isto é devido a que todos os nós da rede utilizam o *duty cycle* (ciclo de trabalho), que permite saber se o hardware dos nós está em estado ativo o desativo permitindo controlar o consumo de energia de cada nó dentro da rede.

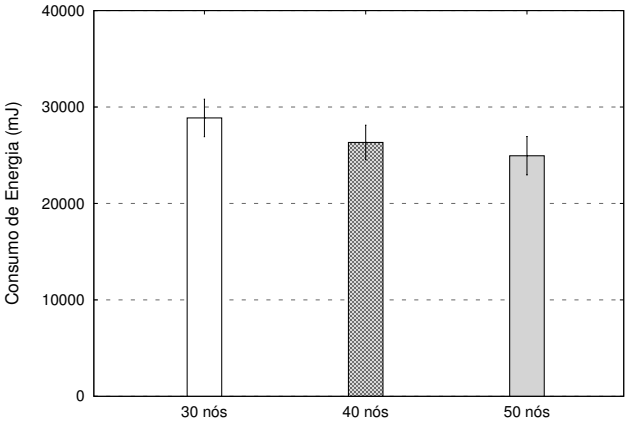

Figura 5.10: Energia (E_{gc}) consumida pelos nós

5.4 Avaliação em um cenário de condomínio

O cenário avaliado corresponde a um condomínio. A avaliação considera tanto a eficácia e a eficiência do INTI diante a detecção de ataques *sinkhole*. Este cenário tem como base o cenário descrito em [128], que representa, em geral, condomínios reais aplicados à IoT. A ideia dos autores é criar um roteamento seguro e robusto entre casas individuais. Considera-se que tais informações enviadas são de caráter informativas, preventivas e cooperativas sobre a segurança da comunidade. Este cenário está constituído por uma área de $100m$x$100m$. Para cada simulação assume-se uma quantidade de nós móveis de 30, 40 e 50, distribuídos de forma aleatória dentro da área especificada, como visto na Figura 5.11.

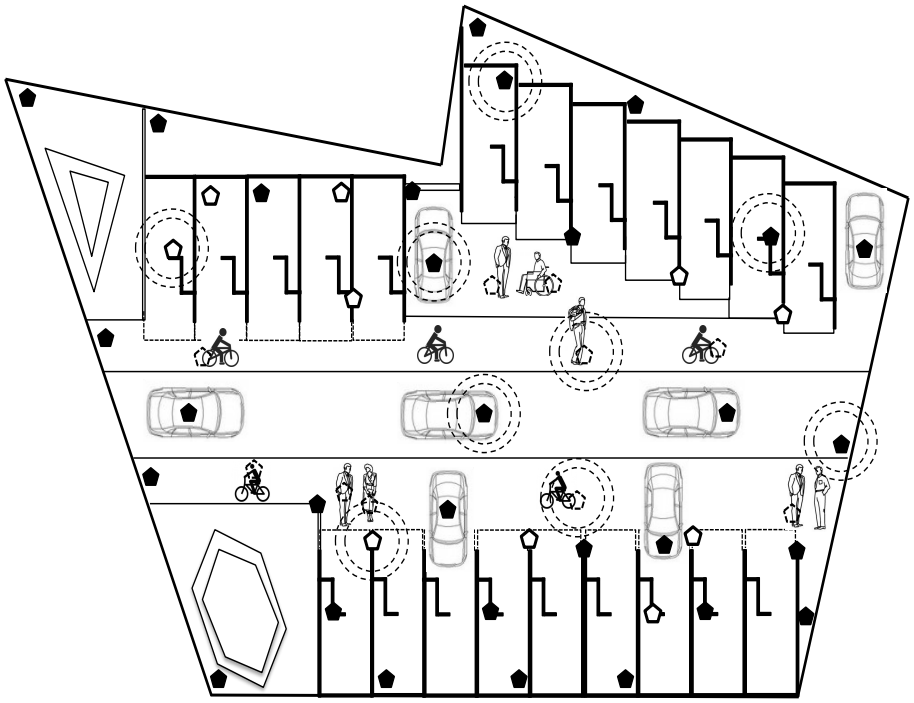

Figura 5.11: Cenário condomínio

Estes nós móveis representam aos usuários que utilizam equipamentos sem fio, como celulares, PDAs, notebooks, e movimentam-se em uma área delimitada, seguindo o padrão de mobilidade *RandomWaypoint*. Sendo este padrão de movimentação mais realístico. Esses usuários podem ser pedestres, corredores, ciclistas e até automóveis. As velocidades médias adotadas por cada usuário estão entre ($0m/s$ até $6.94m/s$), como mostrado na Tabela 5.2. O tempo de simulação estabelecido é de 1500 segundos(s). O protocolo de roteamento empregado pelo INTI é uma modificação do protocolo RPL utilizado pelo sistema SVELTE, sendo que o protocolo de transporte utilizado pelos nós é o UDP. O raio alcance dos nós é de $20m$, $30m$ e $40m$. Neste cenário são consideradas as porcentagens de 20% e o 30% de nós atacantes do total de nós utilizados nas simulações. Os resultados apresentados são as médias de 35 simulações e com um intervalo de confiança de 95%.

Velocidades	Usuário	Pausa
$0m/s$ - $1.39m/s$	pedestres	$30s$
$1.67m/s$ - $4.17m/s$	corredores	$60s$
$4.44m/s$ - $6.94m/s$	ciclistas e automóveis	$90s$

Tabela 5.2: Relação de velocidade máxima e tempo de pausa

Uma sínteses dos parâmetros empregados nas simulações para o cenário de condomínio, e a variação dos valores utilizados para cada parâmetro do sistema de detecção INTI são detalhados na Tabela 5.3.

Parâmetro	Valores
Tipo de nó sensor	Tmote Sky mote
Número de nós	30, 40 e 50
Tempo de simulação	$1500s$
Raio de alcance	$10m$, $20m$, $30m$ e $40m$
Velocidades	$1.39m/s$, $4.17m/s$ e $6.94m/s$
Tempo de pausa do nó	$30s$, $60s$ e $90s$
Área	100x100 metros
Tipo de pacote utilizado	UDP
Tempo para gerar pacote de dados	$10s$
Padrão	IEEE 802.15.4
Canal sem fio	Unit disk graph Medium (UDGM)
Número de nós atacantes	20% e 30%
Taxa de dados	10^2 kbps

Tabela 5.3: Parâmetros de simulação do condomínio

5.4.1 Resultados da eficácia

As métricas para medir a eficácia são as mesmas que da Subeção 5.3.2 como: a taxa de detecção (Tx_{det}), a taxa de falsos negativos (Tx_{Fn}) e taxa de falsos positivos (Tx_{Fp}). Com estas métricas se poderá conhecer a eficácia do sistema INTI diante os ataques sinkhole. Os resultados obtidos a partir destas métricas são mostradas a continuação.

Para a taxa de detecção (Tx_{det}) são apresentados três gráficos como visto na Figura 5.12. No gráfico (a) da Figura 5.12, com 30, 40 e 50 nós, onde 20% deles são nós atacantes sinkhole, e com diferentes tamanhos de raio de alcance como de 20, 30 e $40m$ a taxa de detecção alcançada em geral é superior ao 90% chegando até em alguns casos a 95%. Esta taxa de detecção é obtida devido aos diferentes mecanismos usados no INTI que trabalhando de forma unida permitem obter estes resultados. Já com 30% de nós atacantes sinkhole, e com os mesmos raios de alcances o sistema INTI alcançou uma taxa de detecção superior ao 93% chegando ao 98%. Estes resultados são mostrados no gráfico (b) da Figura 5.12. O terceiro gráfico apresenta a média alcançada pelo sistema INTI diante a detecção de nós atacantes sinkhole. Pode-se observar que em todos os resultados usando diferentes quantidades de 30, 40 e 50 nós, onde o 20% deles são ataques sinkhole,

a taxa de detecção de ataques sinkhole atinge uma taxa superior do 80%. Com as mesmas quantidades de nós, onde o 30% deles são nós atacantes a taxa de detecção é superior do 90%, como ilustrado no gráfico (c) da Figura 5.12.

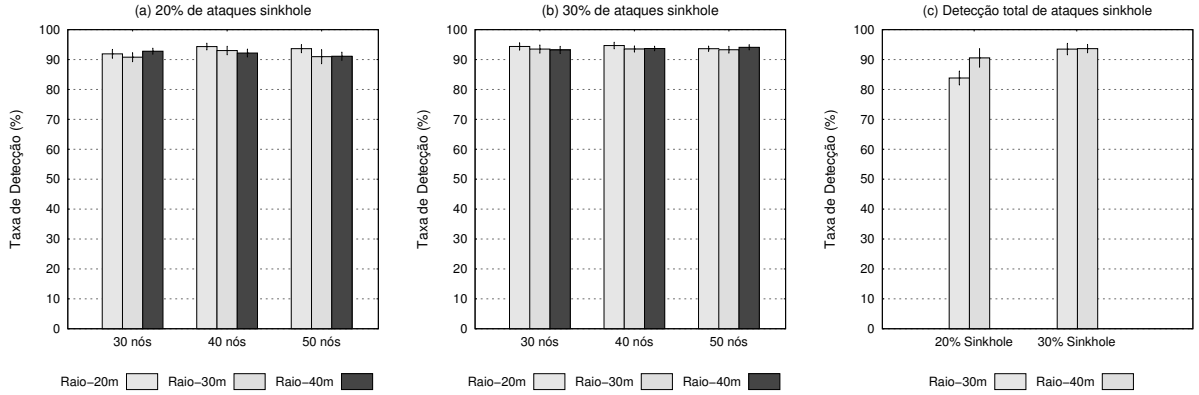

Figura 5.12: Taxa de detecção - Tx_{det} diante de ataques sinkhole

O sistema INTI apresenta uma baixa taxa de falsos negativos (Tx_{Fn}), como mostram os gráficos apresentados na Figura 5.13. No gráfico (a) da Figura 5.13 com 30, 40 e 50 nós, onde 20% deles são nós atacantes, e variando o raio alcance, o sistema INTI obteve uma taxa de falsos negativos inferior do 8%, enquanto a menor taxa de falsos negativos alcançada é de 5.5%. Isto se deve à eficácia dos mecanismo utilizados pelo sistema INTI. Nos resultados apresentados no gráfico (b) da Figura 5.13 com 30% e com os mesmos parâmetros usados no cenário anterior a taxa de falsos negativos alcançada não supera o 7% com uma mínima do 5.3% . Esta baixa nos resultados alcançados pelo sistema INTI é devido à demora na corroboração do status (St) de um nó suspeito esta demora pode acontecer a um gargalo na rede, onde um nó na função de líder deve calcular a reputação e a confiança a partir do status do nó suspeito. Por último, o gráfico (c) da Figura 5.13, apresenta um resumo da media da taxa de falsos negativos obtidos pelo sistema INTI diante os diferentes porcentagens de nós atacantes sinkhole.

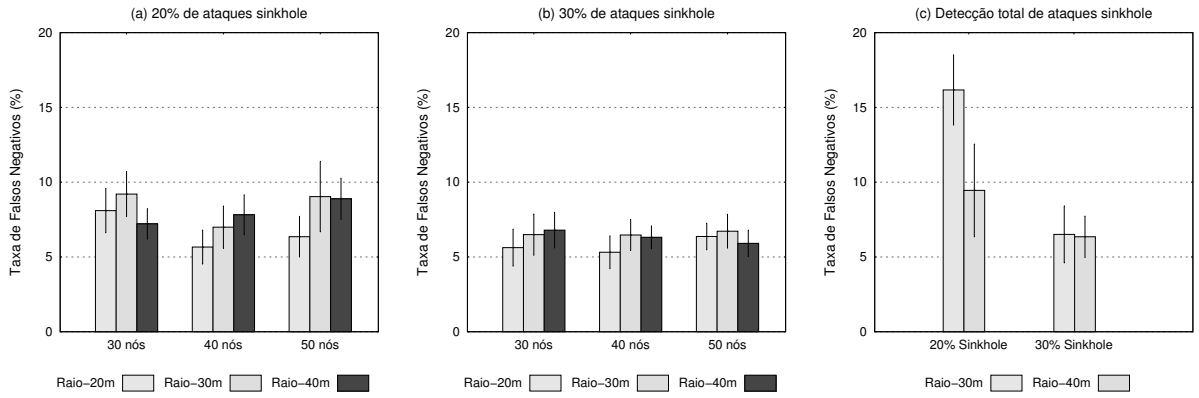

Figura 5.13: Taxa de falsos negativos - Tx_{Fn}

Por outro lado, a taxa de falsos positivos (Tx_{Fp}), conforme mostram os gráficos da Figura 5.14. No gráfico (a) da Figura 5.14, com 30 e 40 nós, onde 20% deles são ataques sinkhole, o sistema INTI atingiu uma taxa de falsos positivos de 4% chegando até o 7%. Já no cenário com 50 nós os resultados obtidos aumentam do 4.5% até o 12%. Isto acontece devido ao atraso no encaminhamento dos pacotes dos agrupamentos formados. No gráfico (b) da Figura 5.14 com 30 nós, onde 30% deles são nós atacantes, e um raio de $10m$ os resultados melhoram sendo que o sistema INTI atingia a taxa de falsos positivos de 4% e ao aumentar o raio para $20m$ a taxa de falsos positivos é de 10%. Isto pode ser devido à mobilidade que apresentam os nós. Já nos cenários com 40 e 50 nós os resultados melhoram chegando ao 6% e diminuindo até 3%. Enquanto o gráfico (c) ilustrado na Figura 5.14 apresenta a média de ambos cenários. A taxa de falsos positivos com 20% de nós atacantes sinkhole e considerando raios de alcance de 30 e $40m$ os resultados chegam de 9.5% até 13%. Já no cenário com 30% de nós sinkhole, e os mesmos raios de alcance, a taxa de falsos positivos é menor a 6%. Isso indica que o INTI identifica poucos nós confiáveis como atacantes. Essa detecção equivocada pode acontecer quando alguns nós atrasam-se no encaminhamento dos pacotes. Assim, momentaneamente eles são considerados sinkhole, porém quando acontece a movimentação e as interações entre os nós, eles são identificados como nós bons.

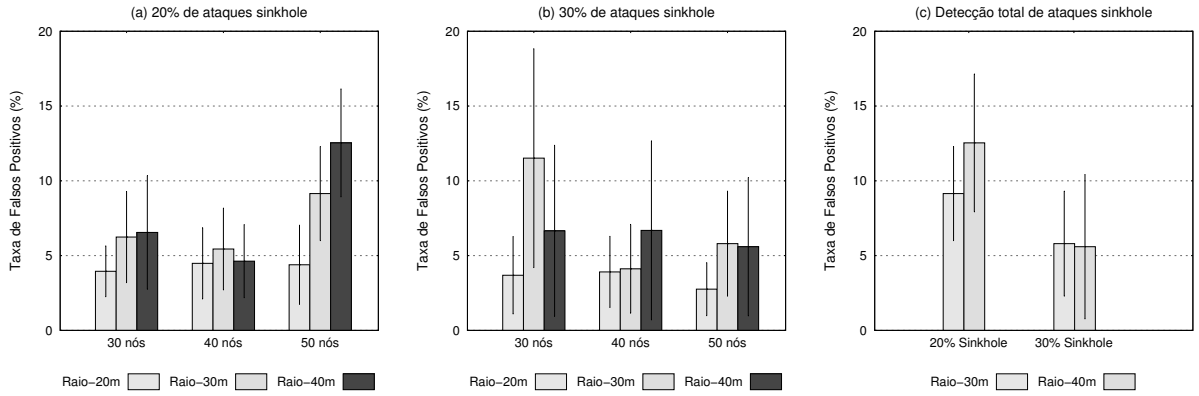

Figura 5.14: Taxa de falsos positivos - Tx_{Fp}

5.4.2 Resultados da eficiência

Essa subseção apresenta a avaliação da eficiência do INTI aplicado em um cenário realístico da IoT. Este cenário esta composto por dispositivos (nós) móveis. As métricas para medir a eficiência são as mesmas que as descritas na Subeção 5.3.2 como: as funções assumidas pelos nós dentro da rede, a taxa de entrega ($Tx_{Entrega}$), a latência (L_T) e o consumo de energia (E_{gc}). A seguir são descritas as medições obtidas pelas métricas.

A seguir são apresentados um conjunto de gráficos em uma só figura mostrando a quantidade do número de nós associados, número de nós líderes, número de nós membros

e o número de nós livres registrados durante a simulação toda. Os resultados com 30 nós e com raio de $10m$ o sistema INTI só consegue formar os agrupamentos mas grande quantidade de nós ficam livres movimentando-se dentro da área determinada. Isso acontece devido à distribuição aleatória dos nós e a pouca quantidade de nós utilizados para a área especificada. Quando se aumenta o tamanho do raio de alcance para 20, 30 e $40m$ esta quantidade de nós livres diminui. Ao aumentar a quantidade a 40 nós pode-se observar que a quantidade de nós livres é de 13 nós diminuindo ao aumentar o tamanho do raio de alcance até alcançar uma quantidade inferior de 7 nós. Entretanto, com 50 nós e variando o parâmetro do raio o número de nós livres diminui, sendo que o número de nós associado, de nós líderes e de nós membros aumente de forma proporcional. Isto se deve a que a quantidade de nós e o raio utilizado são os adequados para a área utilizada, como visto na Figura 5.15.

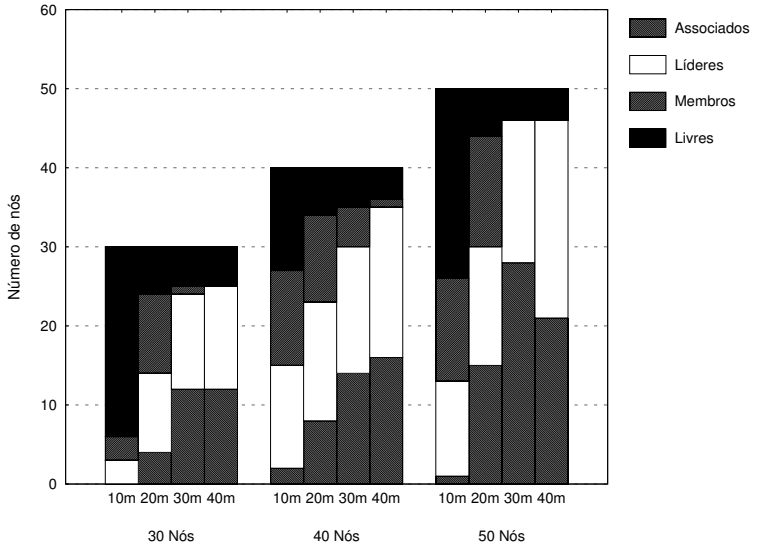

Figura 5.15: Funções assumidas pelos nós

O sistema INTI atingiu uma taxa de entrega ($Tx_{Entrega}$) superior a 80% no cenário com nós móveis. No resultado obtido com 30 nós, e com raio de alcance de $10m$, o sistema INTI obteve uma taxa de entrega de 81%. Quando o raio aumenta a $20m$, o sistema INTI alcançou uma taxa de entrega de 98%. Neste mesmo cenário quando o raio aumenta para $30m$, o INTI conseguiu uma taxa de entrega de 93%. Já com o raio de $40m$, o sistema atingiu a taxa de 95%. Note-se que com 40 nós os resultados obtidos são similares aos resultados obtidos que com 30 nós. Onde usando um raio de $10m$ a taxa de entrega é de 83%, quando aumenta o raio para $20m$ a taxa de entrega é de 90%. Com raios de 30 e $40m$ a taxa de entrega chega até 98%. Por último, com uma quantidade de 50 nós, o INTI obteve uma taxa de entrega mínima de 81% com o raio de $10m$ e máximo de 98% com o raio de $40m$, como visto no gráfico da Figura 5.16. Isto é devido à técnica de agrupamentos utilizada pelo sistema INTI no encaminhamento de dados.

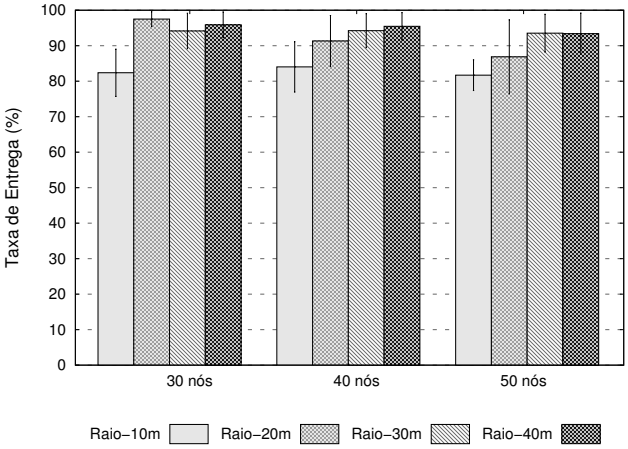

Figura 5.16: Taxa de entrega - $Tx_{Entrega}$

A latência (L_T) mostrada os resultados atingidos com 30 nós e com raio de alcance de $10m$ é inferior a 22 milissegundos (ms), sendo que para o raio de $20m$ o tempo aumente a $53(ms)$. Quando se usa um raio de $30m$ o tempo da latência alcançada pelo INTI diminui até $51(ms)$ diminuindo o tempo até obter $35(ms)$ quando se usa um raio de $40m$. Com a quantidade de 40 nós o tempo da latência alcança o $81ms$ chegando a diminuir até obter um tempo de $38ms$. Para 50 nós, e com raio de alcance de $10m$ o tempo da latência obtida é de $22ms$ aumentado quando se amplia o raio para $20m$ obtendo assim um tempo de latência de $78ms$ para depois diminuir até $49ms$ e $39ms$ a medida que se utiliza os raios de alcance de 30 e $40m$, como é ilustrado no gráfico da Figura 5.17. Esta diferença acontece devido à técnica empregada pelos nós da rede e ao tempo em que a rede demora para definir as rotas de extremo a extremo para a transmissão das mensagens dos nós. Entretanto, os resultados obtidos pelo sistema INTI pode-se notar que quando o raio de alcance aumenta o tempo da latência diminui fazendo mais rápida a comunicação entre os diferentes nós da rede.

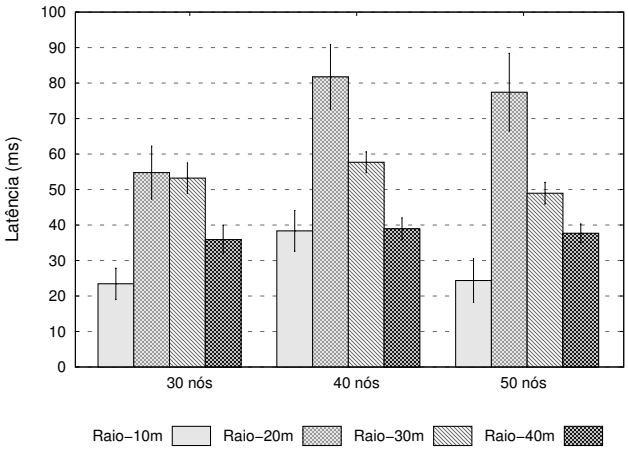

Figura 5.17: Latência - L_T

Nas simulações realizadas, considerou-se o consumo de energia (E_{gc}) nas seguintes situações: recepção, transmissão e verificação de mensagens feitas pelos nós da rede. Entende-se por recepção o processamento completo da mensagem que chega ao nó. Entende-se por verificação a leitura e verificação do cabeçalho da mensagem, que é desprezada caso não seja endereçada ao nó que a recebe. Fazendo isso, pode-se reduzir o consumo de energia dos nós, aumentando seu tempo de vida na rede. O consumo de energia(E_{gc}) dos nós durante toda a simulação é ilustrado no gráfico da Figura 5.18. Pode-se observar que com 30 nós móveis, o consumo de energia do sistema INTI alcança 30000 milíjoule(mJ), já quando a quantidade de nós é aumentada para 40 nós móveis o consumo de energia diminui chegando a $29000mJ$. Por último, com 50 nós móveis o consumo de energia do INTI alcança $28000mJ$. Pode-se observar que a razão aumenta a quantidade de nós móveis dentro da rede o consumo de energia diminui, isto é devido a que todos os nós da rede utilizam o *duty cycle* (ciclo de trabalho), que permite saber se o hardware dos nós esta em estado ativo o desativo permitindo controlar o consumo de energia.

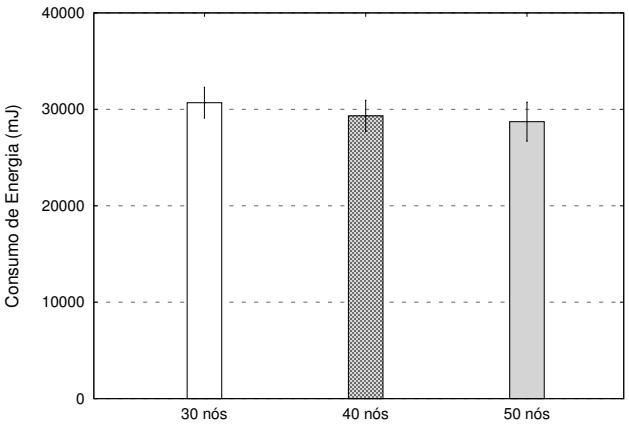

Figura 5.18: Energia -E_{gc} consumida pelos nós

5.5 Comparação do INTI com o SVELTE

Esta seção apresenta os resultados da avaliação dos sistemas de detecção de intrusão (IDS) INTI e SVELTE quanto à eficácia e a eficiência na detecção de ataques sinkhole. O cenário utilizado é similar ao cenário apresentado na seção 5.4 com a única variação na quantidade de nós utilizados. Para este cenário foram utilizados 30 nós. Isto é devido à limitação que presenta o sistema SVELTE como estourar o buffer, a memória. Além disso, foram utilizadas as mesmas métricas descritas na Seção 5.2.

5.5.1 Resultados da eficácia

A taxa de detecção (Tx_{det}) alcançada pelos sistemas INTI e SVELTE diante de ataques *sinkhole* são avaliados em um cenário fixo e móvel como é ilustrado no gráfico da Fi-

gura 5.19. No cenário fixo, o INTI e o SVELTE obtiveram praticamente uma igualdade na detecção de ataques *sinkhole*, como ilustra o gráfico (a) da Figura 5.19. No sistema INTI, a taxa de detecção é de 92%, e isso se deve à característica do INTI, em que para cada nó a reputação e confiança são atualizadas de maneira constante. Desta forma, a taxa de detecção se mantém com o aumento de ataques *sinkhole*. No SVELTE, a taxa de detecção obtida é em média de 90%. 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 o gráfico (b) da Figura 5.19 apresenta a taxa de detecção alcançada pelo sistema SVELTE que diminuiu para 24% e a do INTI é superior a 70%. Esse incremento na taxa de detecção entre ambos sistemas se deve ao fato de que o SVELTE não permite mobilidade dos nós, sendo uns dos pontos fracos. Portanto, o INTI supera ao SVELTE na taxa de detecção diante ataques sinkhole tanto em um cenário com dispositivos fixos como em um cenário com dispositivos móveis.

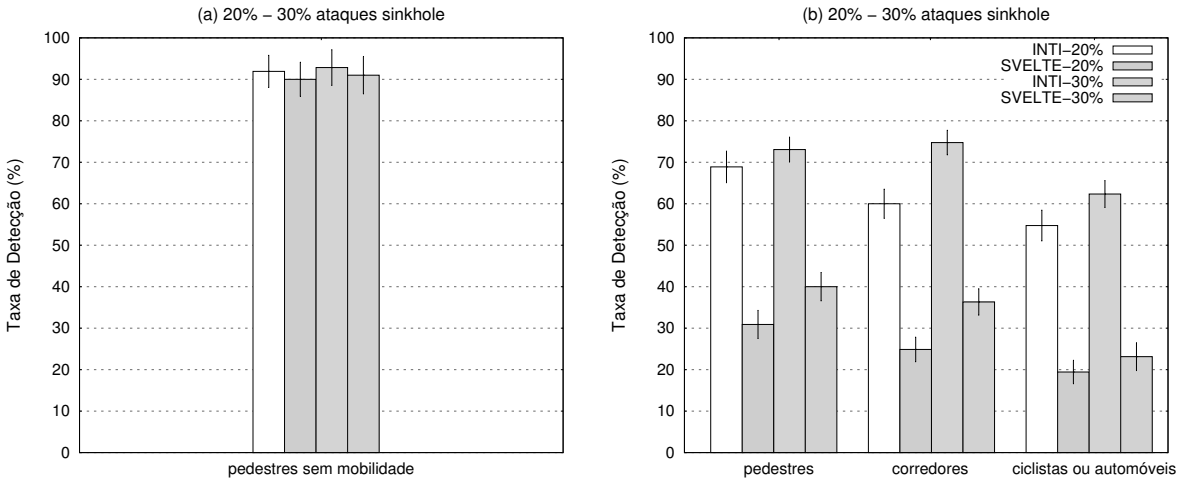

Figura 5.19: Taxa de detecção - Tx_{det} diante de ataques sinkhole

Os resultados da taxa de falsos positivos (Tx_{Fp}) obtidos por ambos sistemas na detecção de ataques *sinkhole* são mostrados nos gráficos da Figura 5.20. No gráfico (a) da Figura 5.20 ilustra um cenário com nós (pedestres) fixos e com o 20 e 30% de nós atacantes sinkhole como pode-se observar o sistema INTI alcançou uma taxa de falsos positivos inferior a 3%. Enquanto o SVELTE alcançou uma taxa de falsos positivos em média de 4%. No cenário com nós móveis como (pedestres, corredores, ciclistas ou automóveis), os resultados são apresentados no gráfico (b) da Figura 5.20, neste gráfico a taxa de falsos positivos obtida pelo INTI é inferior a 30%, sendo que a taxa de falsos positivos alcançada pelo sistema SVELTE é de aproximadamente 39%. 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 nós bons.

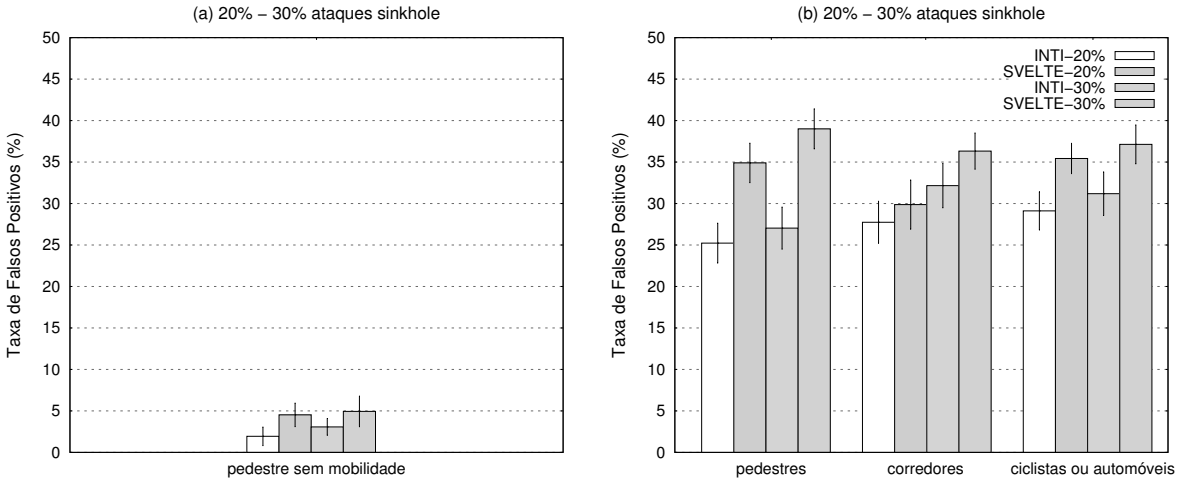

Figura 5.20: Taxa de falsos positivos - Tx_{Fp}

A taxa de falsos negativos (Tx_{Fn}) obtidos pelo INTI em um cenário com nós (pedestres) fixos e com 20 e 30% de nós atacantes sinkhole a taxa de falsos negativos é de 8%, como ilustrado no gráfico (a) da Figura 5.21. 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 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 móvel com nós que representam (pedestres, corredores, ciclistas ou automóveis) e com 20 e 30% de nós atacantes sinkhole a taxa de falsos negativos obtida pelo sistema INTI é de 28% e a taxa de falsos negativos alcançada pelo sistema SVELTE é de 38%, conforme apresentado no gráfico (b) da Figura 5.21. Esse incremento da taxa de falsos negativos acontece pela dinamicidade dos nós da rede.

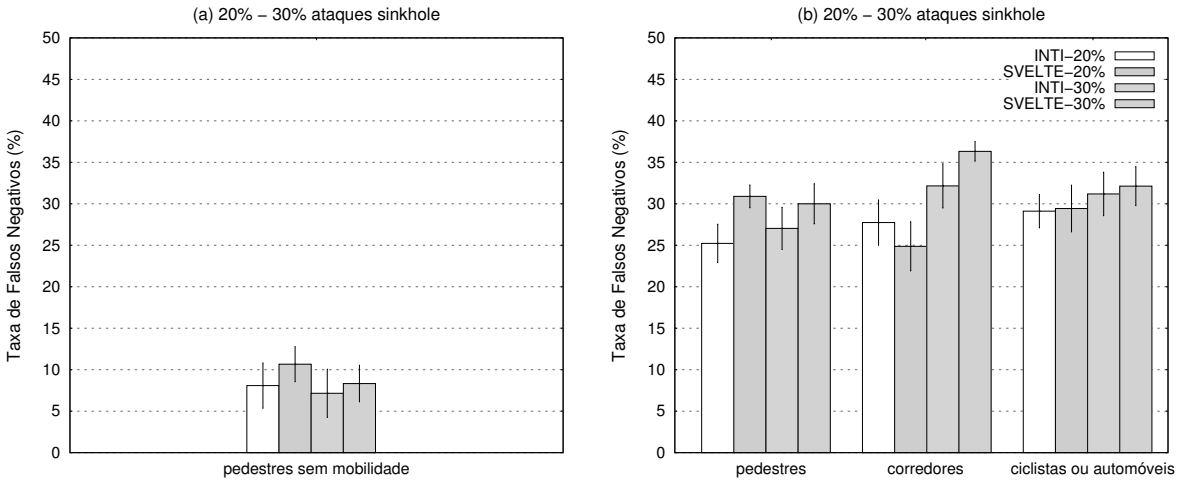

Figura 5.21: Taxa de falsos negativos - Tx_{Fn}

5.5.2 Resultados da eficiência

A taxa de entrega ($Tx_{Entrega}$), como apresentam os gráficos na Figura 5.22. No cenário fixo, o sistema SVELTE apresenta uma maior taxa de entrega alcança o 99% na entrega de dados da IoT, superando os 95% alcançados pelo sistema INTI, como ilustrado no gráfico (a) da Figura 5.22. 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 incremento da quantidade de nós a taxa de entrega aumenta. O gráfico (b) da Figura 5.22 apresenta só a avaliação do sistema INTI, já que o sistema SVELTE não permite a mobilidade dos nós. Este gráfico considera diferentes velocidades como foram definidas na Tabela 5.2. Como pode-se apreciar o sistema INTI no começo possui uma taxa de entrega superior a 55% mas conforme aumenta a quantidade de nós e a velocidade o INTI aumenta conseguindo alcançar uma taxa de entrega superior a 75%.

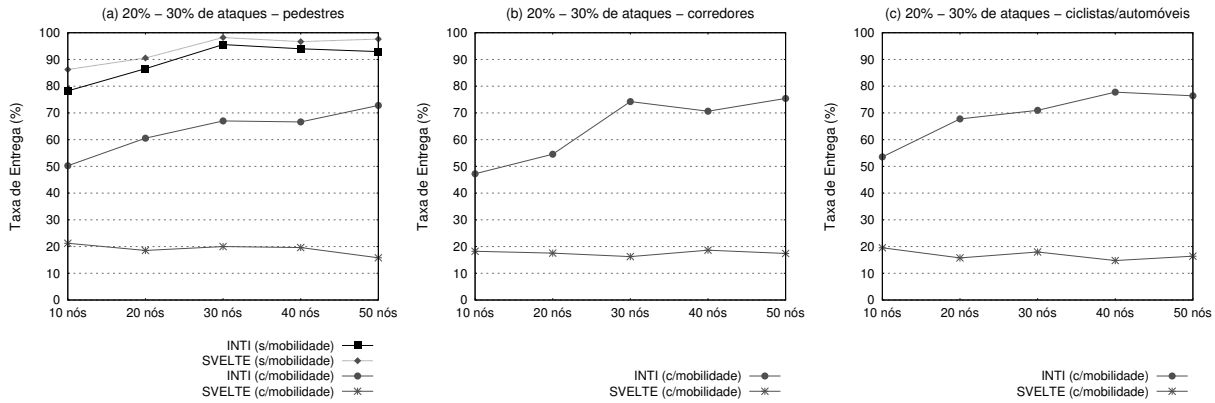

Figura 5.22: Taxa de entrega - $Tx_{Entrega}$

A métrica do consumo de energia (E_{gc}), como mostram os gráficos da Figura 5.23. No cenário fixo, o INTI apresenta um consumo de energia de $25000mJ$ menor do que o consumo de energia produzido pelo sistema SVELT, sendo este de $67000mJ$, como pode-se observar no gráfico (a) da Figura 5.23. O consumo de energia em um cenário móvel aumenta para para ambos sistemas. Isto é devido à mobilidade realizada pelos nos da rede. Neste cenário o sistema INTI obtém quase o mesmo consumo de energia que em um cenário fixo. Isto se deve à técnica usada pelo INTI permitindo a formação de agrupamentos e à configuração do *Duty cycle* dos nós, o qual se encarga de ligar e desligar o raio, a fim de diminuir o consumo de energia. É interessante observar que o consumo de energia do SVELTE em um cenário móvel aumentou para $75000mJ$. Este incremento é devido à formação da topologia da rede no SVELTE, conforme mostrada no gráfico (b) da Figura 5.23.

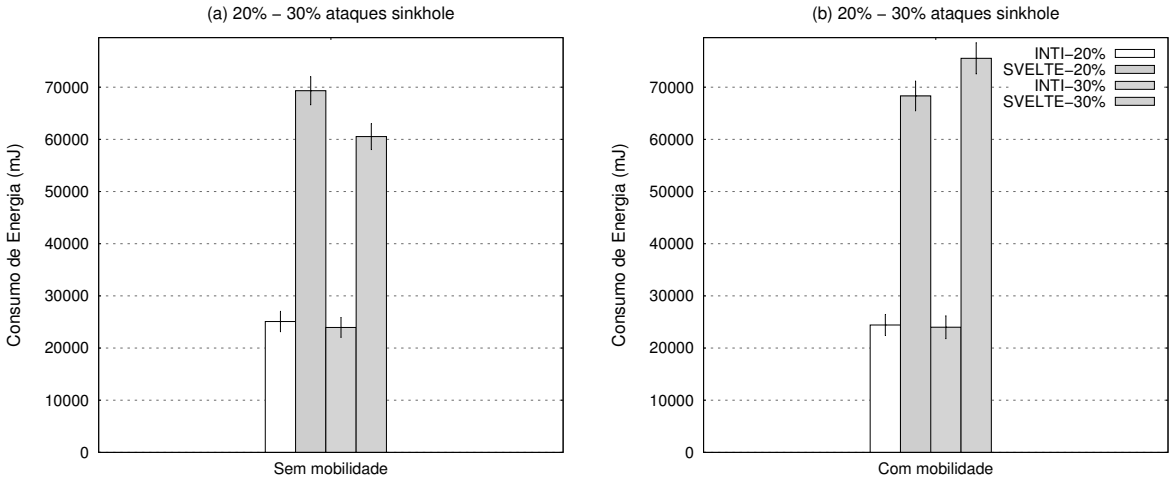

Figura 5.23: Consumo de energia -E_{gc}

5.6 Resumo

Este capítulo apresentou a avaliação da eficácia e da eficiência do sistema INTI, e uma comparação com o sistema SVELTE diante da detecção de ataques *sinkhole*. Foram empregados cenários realísticos da IoT com diferentes quantidades de nós atacantes móveis e diferentes velocidades. Os resultados mostraram que o INTI é mais eficaz do que o sistema SVELTE.

CAPÍTULO 6

CONCLUSÃO

A Internet das Coisas (IoT) é caracterizada por conectar um grande número de objetos heterogêneos fixos ou móveis que possuem características de baixo consumo de energia, armazenamento, processamentos sendo estas características limitadas. Essas características tornam a IoT altamente vulnerável aos ataques *sinkhole*, influindo no desempenho da IoT. Esses ataques são considerados uns dos mais destrutivos nas redes sem fio. Estes ataques tentam atrair o tráfego de uma certa área com o objetivo de prejudicar o destino de receber dados completos e corretos.

Diversos trabalhos encontrados na literatura apresentam métodos ou esquemas que quantificam o impacto de ataques *sinkhole* sobre redes RSSF, MANETs e VANETs. No entanto, as soluções existentes geram outros problemas para a rede denominados como efeitos adversos, como elevadas taxas de falsos positivos e negativos, elevado consumo de energia, entre outros. Dentro deste escopo, poucas pesquisas têm sido desenvolvidas para a proteção e a segurança da IoT na transmissão de informação, visto que trata-se de um novo modelo de rede. Além disso, os trabalhos existentes são inadequados para um funcionamento dinâmico porque não consideram a mobilidade dos dispositivos, sendo isso fundamental para seu uso por pessoas e objetos.

O sistema INTI (***I**ntrusion Detection Si**N**khole At**T**tacks 6LoWPAN Internet of Th**I**ngs*) foi proposto com o objetivo de detectar e isolar ataques *sinkhole* na IoT. Inspirado no comportamento dos nós na transmissão de mensagens de dados, este sistema considera inicialmente que todos os nós começam livres transmitindo e coletando mensagens de controle a fim de criar e configurar os agrupamentos. A partir do momento que os nós começam a trocar mensagens de dados, alguns nós desempenham a função de *watchdogs* controlando e verificando o encaminhamento das mensagens de dados como definido no módulo de monitoramento. Este módulo, quando detecta alguma suspeita, avisa para o módulo de detecção o qual confirma se a suspeita é verdadeira o falsa. Para isso, este módulo calcula a reputação e confiança do nó suspeito. Confirmada a suspeita o nó é considerado um atacante *sinkhole*, em seguida procede-se a seu isolamento. O módulo de isolamento consiste em anunciar à rede sobre o atacante e promover uma reconstrução do agrupamento afetado a fim de manter a estabilidade na comunicação da rede. O INTI combinou o uso de *watchdogs*, reputação e confiança para a detecção de ataques *sinkhole*, por meio da análise do comportamento dos dispositivos no encaminhamento de mensagens.

O sistema INTI foi implementado no simulador Cooja que faz parte do sistema opera-

cional Contiki. O INTI foi avaliado diante da presença de nós atacantes *sinkhole*. Ele foi comparado com o sistema de detecção de intrusão SVELTE, que é um sistema de detecção para a IoT. O SVELTE também foi implementado no simulador Cooja. Para avaliar o desempenho e a eficiência de ambos sistemas, se utilizou um ambiente com dispositivos fixos que representa um cenário *smarthome* e outro ambiente com dispositivos móveis que representa um cenário como um condomínio. Ambos cenários representam ambientes da IoT realísticos. No cenário do condomínio, os nós representam usuários que utilizam equipamentos sem fio, como celulares, PDAs, notebooks, e movimentam-se em um área delimitada. Os resultados obtidos avaliaram o desempenho e a eficiência do sistema INTI apresentando um bom desempenho com elevada taxa na detecção de ataques *sinkhole* aplicando um baixo consumo de energia. Ademais, o sistema INTI alcançou uma boa eficiência com baixas taxas de falsos positivos e falsos negativos, e ao mesmo tempo reduzindo os efeitos adversos como elevadas taxas de falsos positivos e negativos, consumos de energia, entre outras.

Quando comparado ao sistema SVELTE, o INTI apresentou resultados sempre superiores devido à maneira adaptativa e dinâmica com a qual opera, como a formação dos agrupamentos, rotas, o monitoramento do nó encaminhador e a detecção de alguma suspeita, sendo estas reparadas e calculadas através do envio de mensagens de controle. Em contrapartida o sistema SVELTE é inadequado para um funcionamento dinâmico porque não considera a mobilidade dos dispositivos, sendo essa característica fundamental para seu uso por pessoas e objetos.

Desta forma, podemos concluir que o objetivo principal deste trabalho, que foi a detecção da presença de ataques *sinkhole* na IoT, foi atingido. Este objetivo foi alcançado pelo cálculo do comportamento do nó na transmissão das mensagens de dados combinando o uso de *watchdog*, reputação e confiança. Estes três mecanismos foram utilizados para uma ótima detecção e isolamento dos ataques *sinkhole*, tornando assim um sistema eficiente e eficaz na detecção ataques *sinkhole* na Internet das coisas (IoT). Finalmente, a realização deste trabalho foi de significativa importância, pois possibilitou o aprofundamento nesta área de pesquisa que vem crescendo de maneira intensa.

6.1 Trabalhos futuros

Os resultados obtidos e as conclusões deste trabalho abrem as possibilidades de alguns desdobramentos em trabalhos futuros. Uma das possibilidades que se coloca é a implementação real do Sistema de detecção de intrusão INTI. Assim, qualquer sistema de detecção para a IoT poderia ser testado em uma rede real, para assim realmente comprovar sua eficácia e sua eficiência.

Como outra propostas para trabalhos futuros, tem-se a análise de custo computacional a razão da eficácia e da eficiência fornecida pelo sistema INTI diante da detecção de

ataques *sinkhole*, permitindo conhecer a qualidade da solução empregada. Embora o uso de uma abordagem baseada no comportamento dos nós calculando a reputação e confiança possibilite a detecção e isolamento dos ataques *sinkhole*, ainda é possível a existência de outros tipos de ataques que acontecem na IoT como o ataque *selective forwarding* ou *sybil*. Sendo que o ataque *selective forwarding* atua de forma parecida com o ataque *sinkhole*.

Devido à quantidade de objetos conectados uns com outros trocando informações, isto gerará grandes quantidades de dados provocando uma sobrecarga de informação causando inclusive em alguns casos gargalos na comunicação. Por esta razão, pretende-se avaliar a sobrecarga que pode causar o INTI na IoT. Além disso, outra possibilidade para trabalhos futuros seria o desenvolvimento de um protocolo de segurança para a IoT capaz de oferecer certo grau de flexibilidade com relação à escolha dos mecanismos e serviços de segurança a serem utilizados. Dentro do estudo realizado e diante dos resultados apresentados, outro trabalho futuro que surge é a implementação de um método de localização do dispositivo (nó) atacante sinkhole dentro do ambiente da IoT, a fim de corroborar com a detecção e o isolamento realizado pelo sistema INTI

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Charith Perera, Peter Christen Arkady Zaslavsky, and Dimitrios Georgakopoulos. Context aware computing for the internet of things: A survey. In *IEEE Communications survey and tutorials, accepted for publication*, pages 69–71. IEEE, Janeiro 2013.

[2] Future Internet X-ETP Group. Future internet strategic research agenda. In *X-ETP Future Internet Research Agenda*, pages 69–71. European Future Internet, Janeiro 2010.

[3] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. volume 54, pages 2787–2805, Catania, Itália, Outubro 2010. Elservier Science Publishers B. V.

[4] Rolf H. Weber. Internet of things - new security and privacy challenges. volume 26, pages 23–30. Elservier, 2010.

[5] Hua-Dong. Ma. Internet of things: Objectives and scientific challenges. In *Journal of Computer Science and Technology*, volume 26, pages 919–924, China, 2011. Springer USA.

[6] Nima Bari, Ganapathy Mani, and Simon Berkovich. Internet of things as a methodological concept. In *Computing for Geospatial Research and Application, 2013 Fourth International Conference on*, pages 48–55. IEEE, 2013.

[7] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo. A survey on facilities for experimental internet of things research. volume 49, pages 58–67, Guildford, Inglaterra, Setembro 2011. IEEE Computer Society.

[8] Sundmaeker and Harald. *Vision and Challenges for Realising the Internet of Things*, pages 9–79. European Commission, Bruxelas, Bélgica, 2010.

[9] Chen and Yen-Kuang. Challenges and opportunities of internet of things. In *Design Automation Conference (ASP-DAC), 2012 17th Asia and Pacífico do Sul*, pages 383–388, Sydney, Austrália, 2012. IEEE Computer Society.

[10] Stephen Kent. IP authentication header. Technical report, Network Working Group, USA, Dezembro 2005.

[11] IEEE 802 Working Group. Standard for part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area

networks (LR-WPANs). Technical report, ANSI/IEEE 802.15, USA, Dezembro 2008.

[12] Debasis Bandyopadhyay and Jaydip Sen. Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1):49–69, 2011.

[13] Linus Wallgren, Shahid Raza, and Thiemo Voigt. Routing attacks and countermeasures in the rpl-based internet of things. *International Journal of Distributed Sensor Networks*, 2013, 2013.

[14] M.A. Rassam, A. Zainal, M.A. Maarof, and M. Al-Shaboti. A sinkhole attack detection scheme in mintroute wireless sensor network. In *Telecommunication Technologies (ISTT), 2012 International Symposium on*, pages 71–75, Kuala Lumpur, Málasia, 2012. IEEE Tecnology.

[15] Ting Zhang Peng Xiao Hong Yu, Jingsha He and Yuqiang Zhang. Enabling end-to-end secure communication between wireless sensor networks and the internet. In *in: Proceedings of IEEE INFOCOM*, pages 515–540, Nova Iorque, NY, USA, 2012. Springer.

[16] Sandeep Kumar Pedro Moreno-Sanchez Francisco Vidal-Meca Oscar Garcia-Morchon, Sye Loong Keoh and Jan Henrik Ziegeldorf. Securing the IP-based internet of things with hip and DTLS. In *Proceedings of the sixth ACM conference on Security and privacy in Wireless and Mobile Networks. ACM, 2013*, pages 119–124, Nova Iorque, NY, USA, 2013. ACM Security and privacy.

[17] Farshid Keynia Rouhi Rahimeh and Mehran Amiri. Improving the intrusion detection systems performance by correlation as a sample selection method. In *International Journal of computer Applications (IJCA13)*, pages 33–38, USA, Maio 2013. Science and Education Publishing.

[18] Phillip A. Porras and Peter G. Neumann. Emerald: Event monitoring enabling response to anomalous live disturbances. In *Proceedings of the 20th national information systems security conference*, pages 353–365, 1997.

[19] Rodrigo Roman, Pablo Najera, and Javier Lopez. Securing the internet of things. volume 44, pages 51–58. IEEE, 2011.

[20] Bounpadith Kannhavong, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. A study of a routing attack in OLSR-based mobile ad hoc networks. volume 20, pages 1245–1261. Wiley Online Library, 2007.

[21] David Martins and Hervé Guyennet. Wireless sensor network attacks and security mechanisms : A short survey . In *Network-Based Information Systems (NBiS), 2010 13th International Conference on*, pages 313–320. IEEE, 2010.

[22] Thanassis Giannetsos Krontiris and Tassos Dimitriou. Intrusion detection of sinkhole attacks in wireless sensor networks. In *in Proceedings of the 3rd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (AlgoSensors 07)*, pages 150–161, Wroclaw, Polónia, 2007. Springer.

[23] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In *Proceedings of the 1st IEEE International Workshop SNPA2003*, volume 1, pages 293–315, Califórnia, CA, USA, 2003. Elsevier Science Publishers B. V.

[24] Mohammad Sayad Haghighi and Kamal. Mohamedpour. Securing wireless sensor networks against broadcast attacks. In *Telecommunications, 2008. IST 2008. International Symposium on*, pages 49–54. IEEE, 2008.

[25] Nouha Laroussi. Secure routing in wireless sensor networks. Dissertação de mestrado, The University Stax, Tunísia, 2012.

[26] P. Samundiswary, D. Sathian, and P. Dananjayan. Secured greedy perimeter stateless routing for wireless sensor networks. volume 1, pages 9–20. IEEE, 2010.

[27] Ambika N. and Dr. G.T.Raju. TMW - Time-Endorsement by mobile agent in wireless sensor network. In *The Research Bulletin of Jordan ACM*, pages 114–117, USA, 2011. ACM.

[28] Manoj Kumar Kumar, Neeraj and R. B. Patel. A secure and energy efficient data dissemination protocol for wireless sensor networks. volume 15, pages 490–500, Índia, Novembro 2013.

[29] Swimpy Pahuja and Anita Singhrova. Preventive alternate path routing algorithm against intrusion in sensor area network. In *International Journal of Computer Theory and Engineering*, pages 188–191, Índia, 2013. IEEE Computer Society.

[30] Soo Young Moon and Tae Ho Cho. Intrusion detection scheme against sinkhole attacks in directed diffusion based sensor networks. In *International Journal of Computer Science and Network Security*, pages 118–122, Coreia, 2009. IEEE Computer Society.

[31] Kuang Xiaohui Liu Qiang. Jin Qi, Tang Hong. Detection and defence of sinkhole attack in wireless sensor network. In *Communication Technology (ICCT), 2012*

IEEE 14th International Conference on, pages 809–813, Chengdu, China, 2012. IEEE Security.

[32] K. C. Naveen Sheela, D. and G. Mahadevan. A non cryptographic method of sinkhole attack detection in wireless sensor networks. In *Recent Trends in Information Technology (ICRTIT), 2011 International Conference on*, pages 527–532, Tamil Nadu, Chennai, 2011. IEEE Security.

[33] Matthew Keally, Gang Zhou, and Guoliang Xing. Watchdog: Confident event detection in heterogeneous sensor networks. In *Real-Time and Embedded Technology and Applications Symposium (RTAS), 2010 16th IEEE*, pages 279–288. IEEE, 2010.

[34] Shahid Raza, Linus Wallgren, and Thiemo Voigt. Svelte: Real-time intrusion detection in the internet of things. pages 2661 – 2674, USA, 2013. Elservier.

[35] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A Spirito, and Mark Vinkovits. Denial-of-service detection in 6lowpan based internet of things. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on*, pages 600–607. IEEE, 2013.

[36] Caiming Liu, Jin Yang, Yan Zhang, Run Chen, and Jinquan Zeng. Research on immunity-based intrusion detection technology for the internet of things. In *Natural Computation (ICNC), 2011 Seventh International Conference on*, volume 1, pages 212–216. IEEE, 2011.

[37] Paolo Bellavista, Giuseppe Cardone, Antonio Corradi, and Luca Foschini. Convergence of MANET and WSN in IoT urban scenarios. volume 13, pages 3558–3567. IEEE, 2013.

[38] Ismail Butun, S. Morgera, and Ravi Sankar. A survey of intrusion detection systems in wireless sensor networks. IEEE, 2013.

[39] Sonja Buchegger and Jean-Yves Le Boudec. A robust reputation system for peer-to-peer and mobile ad hoc networks. In *Security of Ad Hoc and Sensor Networks, SASN*, pages 66–77, Massachusetts, MA, USA, 2004. EPFL.

[40] Runfang Zhou and Kai Hwang. A robust and scalable reputation system for trusted peer-to-peer computing. pages 460–473, Coreia, 2007. IEEE Computer Society.

[41] Hosein Marzi and Mengdu Li. An enhanced bio-inspired trust and reputation model for wireless sensor network. *Procedia Computer Science*, 19:1159–1166, 2013.

[42] Bo Zhang, Xiaosheng Pan, and Tao Pan Yang Xiang. Belief and reputation based recommended trust computation in wireless sensor networks. In *IFSA*, pages 26–33, China, 2013. Sensor and Transducers.

[43] A. Boukerche and Xu Li. An agent-based trust and reputation management scheme for wireless sensor networks. In *Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE*, page 5, Otawa, Canadá, 2005. IEEE Computer Society.

[44] Sean Dodson. The internet of things. volume 9, 2003.

[45] K. Elissa. Appendix F: the internet of things (background). In *Disruptive Technologies: Global Trends 2025. SRI Consulting Business Intelligence. Retrieved 30 May 2010*, Maio 2010.

[46] Kevin Ashton. Internet of things. volume 1, pages 1–1, Nova Iorque, NY, USA, Junho 2009. RFID Journal.

[47] Edmundo W. Schuster, Stuart J. Allen, and David L. Brock. *Global RFID [Electronic Resource]: The Value of the EPCglobal Network for Supply Chain Management*, pages 16–33. Springer-Verlag, Nova Iorque, NY, USA, 2006.

[48] Benjamin Fabian and Oliver Günther. Security challenges of the EPCglobal network. volume 52, pages 121–125. ACM, 2009.

[49] Liu Chunli. Intelligent transportation based on the internet of things. In *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on*, pages 360–362, Cangzhou, Hebei, China, 2012. IEEE Computer Society.

[50] Margery Conner. Sensors empower the "Internet of things". In *EDN (Electrical Design News)*, volume 55, page 32, 2010.

[51] Lu Tan and Neng Wang. Future internet: The internet of things. In *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, pages 376–380, Chengdu, China, 2010.

[52] Li-Fen Chen, Hong-Yuan Mark Liao, Ming-Tat Ko, Ja-Chen Lin, and Gwo-Jong Yu. A new LDA based face recognition system which can solve the small sample size problem. In *Proceedings of the 2000 International Conference on Dependable Systems and Networks (DSN '00)*, pages 1713–1726, Taiwan, China, Outubro 2000. IEEE Computer Society.

[53] Stephen E. Deering. Internet protocol, version 6 (IPv6). Technical report, Network Working Group, Rockland, Maine, USA, Dezembro 1998.

[54] Bo Yan and Guangwen Huang. Supply chain information transmission based on RFID and internet of things. In *Computing, Communication, Control, and Management, 2009. CCCM 2009. ISECS International Colloquium on*, volume 4, pages 166–169. IEEE, 2009.

[55] Miao Yun and Bu Yuxin. Research on the architecture and key technology of internet of things (IoT) applied on smart grid. In *Advances in Energy Engineering (ICAEE), 2010 International Conference on*, pages 69–72. IEEE, 2010.

[56] Craig Partridge. Realizing the future of wireless data communications. volume 54, pages 62–68. ACM, 2011.

[57] Biswanath Mukherjee Jennifer Yick and Dipak Ghosal. Wireless sensor network survey. pages 2292 – 2330, Califórnia, CA, USA, Agosto 2008.

[58] Linnyer Beatrys Ruiz, Fabricio A Silva, Thais Regina M Braga, José Marcos S Nogueira, and Antonio Alfredo Ferreira Loureiro. On impact of management in wireless sensors networks. In *Network Operations and Management Symposium, 2004. NOMS 2004. IEEE/IFIP*, volume 1, pages 657–670. IEEE, 2004.

[59] Linnyer Beatrys Ruiz. *Maná: uma arquitetura para gerenciamento de redes de sensores sem fio.* PhD thesis, Universidade Federal de Minas Gerais, 2003.

[60] Antonio AF Loureiro, José Marcos S Nogueira, Linnyer Beatrys Ruiz, Raquel Aparecida de Freitas Mini, Eduardo Freire Nakamura, and Carlos Maurıcio Seródio Figueiredo. Redes de sensores sem fio. In *Simpósio Brasileiro de Redes de Computadores (SBRC)*, pages 179–226, 2003.

[61] Archana Bharathidasan and Vijay Anand Sai Ponduru. Sensor networks: An overview. pages 1–24, Califórnia, CA, USA, 2002. Department of Computer Science, University of California.

[62] J. Agre and L. Clare. An integrated architecture for cooperative sensing networks. pages 106–108, Califórnia, CA, USA, 2000. IEEE Computer Society.

[63] Garnett T. Chandrakasan A. P. Bhardwaj, M. Upper bounds on the lifetime of sensor networks. In *Proceedings of the IEEE International Conference on Communications (ICC 01). IEEE International Conference on*, pages 785–790, Massachusetts, MA, USA, 2001. IEEE Computer Society.

[64] Ian F. Akyildiz. Wireless sensor networks: A survey. volume 28, pages 393–422, Georgia, GA, USA, Março 2002. Elservier.

[65] Hossein Jadidoleslamy. A hierarchical intrusion detection architecture for wireless sensor networks. volume 3, 2011.

[66] Chris M. Roberts. Radio frequency identification (RFID). In *journal Computers & Security*, volume 25, pages 18–26. Elsevier, 2006.

[67] Royal Air Force. "History: 1940". `http://www.raf.mod.uk/history/line1940.html`.

[68] A. M. Das H. Bhargava A. Campbell F. Thorton, B. Haines and J. Kleinschmidt. *RFID Security*, pages 1–50. SYNGRESS, Rockland, Maine, USA, 2006.

[69] Mathieu Bouet and Aldri L. Dos Santos. RFID tags: Positioning principles and localization techniques. In *Wireless Days, 2008. WD'08. 1st IFIP*, pages 1–5. IEEE, 2008.

[70] Kazuo Takaragi, Rei Itsuki, Tsuneo Satoh, Mitsuo Usami, and Ryo Imura. An ultra small individual recognition security chip. volume 21, pages 43–49. IEEE Computer Society, 2001.

[71] Melanie R. Rieback Mitrokotsa, Aikaterini and Andrew S. Tanenbaum. Classification of RFID attacks. In *Journal Information Systems Frontiers*, volume 12, pages 1–14, Amsterdam, Holanda, 2010. Department of Computer Science, Vrije Universiteit.

[72] Benjamin. Khoo. RFID- from tracking to the internet of things: A review of developments. In *Proceedings of the 2010 IEEE/ACM Int'L Conference on Green Computing and Communications & Int'L Conference on Cyber, Physical and Social Computing.*, pages 533–538, Washington, DC, USA, 2010. IEEE Computer Society.

[73] S.L. Garfinkel, A. Juels, and R. Pappu. RFID privacy: An overview of problems and proposed solutions. pages 34–43, Viena, Áustria, 2005. Security Privacy, IEEE.

[74] Juels and Ari. RFID security and privacy: A research survey. In *Selected Areas in Communications, IEEE Journal on*, pages 381–394, Bedford, MA, USA, 2006. Security Privacy, IEEE.

[75] Salvatore Bocchetti. Security and privacy in RFID protocols. Master's thesis, University of Naples Federico II, Itália, Julho 2006.

[76] Jiajun Jim Chen and Carl Adams. Short-range wireless technologies with mobile payments systems. In *Proceedings of the 6th international conference on Electronic commerce(ICEC 04)*, pages 649–656, Nova Iorque, NY, USA, 2004. ACM Security and privacy.

[77] Juan C. Augusto Cook, Diane J. and Vikramaditya R. Jakkula. Ambient intelligence: Technologies, applications, and opportunities. volume 5, pages 277–298, Washington, WA, USA, 2009. Elsevier Science Publishers B. V.

[78] Eui-ho Suh Hong, Jong-yi and Sung-Jin Kim. Context-aware systems: A literature review and classification. volume 36, pages 8509–8522, USA, 2008. Elsevier Science Publishers B. V.

[79] Irene Luque Ruiz Miraz, Guillermo Matas and M. A. Gómez-Nieto. How NFC can be used for the compliance of european higher education area guidelines in european universities. In *Near Field Communication, 2009. NFC'09. First International Workshop on*, pages 3–8, Hagenberg, Áustria, 2009. IEEE.

[80] Gerald Madlmayr. NFC devices: Security and privacy. In *Availability, Reliability and Security ARES 08. Third International Conference on.*, pages 642–647, Barcelona, Espanha, 2008. IEEE Computer Society.

[81] Anass Rghioui, Mohammed Bouhorma, and Abderrahim Benslimane. Analytical study of security aspects in 6lowpan networks. In *Information and Communication Technology for the Muslim World (ICT4M), 2013 5th International Conference on*, pages 1–5. IEEE, 2013.

[82] Olfa Gaddour and Anis Koubâa. RPL in a nutshell: A survey. volume 56, pages 3163–3178. Elsevier, 2012.

[83] Z. Shelby, K. Hartke, C. Bormann, and B. Frank. Constrained application protocol (CoAP), draft-ietf-core-coap-13. 2012.

[84] Rathanakar Acharya and K. Asha. Data integrity and intrusion detection in wireless sensor networks. In *Proceedings of 16th IEEE International Conference (ICON)*, pages 1–5, Delhi, Índia, 2008. IEEE Computer Society.

[85] Dave Evans. The internet of things how the next evolution of the internet is changing everything. Technical report, Cisco Internet Business Solutions Group (IBSG), USA, Abril 2011.

[86] Emerson B. M2M: the internet of 50 billion devices, Win-Win, editorial, Huawei. Technical report, WinWin Magazine, USA, Abril 2010.

[87] G. Montenegro Kushalnagar, N. and C. Schumacher. *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement and Goals, IETF RFC 4919*, pages 1–50. RFC4919, USA, 2009.

[88] Gabriel Montenegro, Nandakishore Kushalnagar, J Hui, and D Culler. Transmission of IPv6 packets over IEEE 802.15. 4 networks. volume 4944, 2007.

[89] Rodrigo Roman and Javier López. Integrating wireless sensor networks and the internet: A security analysis. In *Journal Internet Research*, pages 246–259, Málaga, Espanha, 2009. Emerald Group Publishing Limited.

[90] Jesús Ayuso, Leandro Marin, Antonio J. Jara, and Antonio F Gómez Skarmeta. Optimization of public key cryptography (RSA and ECC) for 16-bits devices based on 6LoWPAN. In *1st International Workshop on the Security of the Internet of Things, Tóquio, Japão*, 2010.

[91] W. Haddad S. Chakrabarti J. Laganier. S. Park, K. Kim. IPv6 over low power wpan security analysis. Technical report, USA, Março 2011.

[92] Jin Qi, Tang Hong, Kuang Xiaohui, and Liu Qiang. Detection and defence of sinkhole attack in wireless sensor network. In *Communication Technology (ICCT), 2012 IEEE 14th International Conference on*, pages 809–813. IEEE, 2012.

[93] NK. Sreelaja and GA. Vijayalakshmi Pai. Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks. volume 19, pages 68–79. Elservier, 2014.

[94] Abhishek Pandey and RC. Tripathi. A survey on wireless sensor networks security. In *International Journal of Computer Applications*, volume 3, pages 43–49, Outubro 2010.

[95] Manjot Kaur and Anand. Nayyar. A comprehensive review of mobile adhoc networks (MANETs). volume 2, pages 197–210, 2013.

[96] Ilker Onat and Ali Miri. An intrusion detection system for wireless sensor networks. In *Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob'2005), IEEE International Conference on*, volume 3, pages 253–259. IEEE, 2005.

[97] Joseph Migga Kizza. *Guide to Computer Network Security*. Springer, 2005.

[98] Djamel Djenouri, L. Khelladi, and N. Badache. A survey of security issues in mobile ad hoc networks. volume 7, pages 2–28, 2005.

[99] Muhammad Shoaib Siddiqui and Choong Seon Hong. Security issues in wireless mesh networks. In *Multimedia and Ubiquitous Engineering, 2007. MUE'07. International Conference on*, pages 717–722. IEEE, 2007.

[100] Lília de Sá Silva, Adriana C Ferrari dos Santos, Thiago Dias Mancilha, José Demísio Simões da Silva, and Antonio Montes. Detecting attack signatures in the real network traffic with annida. volume 34, pages 2326–2333. Elsevier, 2008.

[101] Christopher Kruegel and Giovanni Vigna. Anomaly detection of web-based attacks. In *Proceedings of the 10th ACM conference on Computer and communications security*, pages 251–261. ACM, 2003.

[102] KQ Yan, SC Wang, SS Wang, and CW Liu. Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network. In *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, volume 1, pages 114–118. IEEE, 2010.

[103] Hichem Sedjelmaci and Mohamed Feham. Novel hybrid intrusion detection system for clustered wireless sensor network. In *International Journal of Network Security & Its Applications*, volume 3, 2011.

[104] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi. Detection and mitigation of sinkhole attacks in wireless sensor networks. volume 80, pages 644–653. Elservier, 2014.

[105] Omar Abdel Wahab, Hadi Otrok, and Azzam Mourad. A cooperative watchdog model based on dempster–shafer for detecting misbehaving vehicles. *Computer Communications*, 41:43–54, 2014.

[106] Jaleel Shaheen, Diethelm Ostry, Vijay Sivaraman, and Sanjay. Jha. Confidential and secure broadcast in wireless sensor networks. In *Personal, Indoor and Mobile Radio Communications*, pages 1–5, Atenas, Grécia, 2007. IEEE Computer Society.

[107] Saurabh Ganeriwal, Laura K Balzano, and Mani B Srivastava. Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 4(3):15, 2008.

[108] Carlos R Perez-Toro, Rajesh Krishna Panta, and Saurabh Bagchi. Rdas: reputation-based resilient data aggregation in sensor network. In *Sensor Mesh and Ad Hoc Communications and Networks (SECON), 2010 7th Annual IEEE Communications Society Conference on*, pages 1–9. IEEE, 2010.

[109] European project. "Enabling the business-based internet of things and services". `http://www.ebbits-project.eu/news.php`, 2013.

[110] Ossama Younis and Sonia Fahmy. Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. volume 3, pages 366–379. IEEE, 2004.

[111] Wendi B. Heinzelman, Anantha P. Chandrakasan, and Hari Balakrishnan. An application-specific protocol architecture for wireless microsensor networks. volume 1, pages 660–670. IEEE, 2002.

[112] AKM Muzahidul Islam, Shahrum Shah Abdullah, K Wada, J Uchida, and Wei Chen. An efficient routing protocol on a dynamic cluster-based sensor network. In

Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), 2011 Sixth International ICST Conference on, pages 161–165. IEEE, 2011.

[113] Matthias R. Brust, Hannes Frey, and Steffen Rothkugel. Dynamic multi-hop clustering for mobile hybrid wireless networks. In *Proceedings of the 2nd international conference on Ubiquitous information management and communication*, pages 130–135. ACM, 2008.

[114] M. Adjih C. Saidane L.A. Korbi, I.E. Ben Brahim. Mobility enhanced RPL for wireless sensor networks. In *Network of the Future (NOF), 2012 Third International Conference*, pages 21–23. IEEE, 2012.

[115] Bogdan Pavković, Fabrice Theoleyre, and Andrzej Duda. Multipath opportunistic RPL routing over IEEE 802.15. 4. In *Proceedings of the 14th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems*, pages 179–186. ACM, 2011.

[116] Padma Priyadarshini Samundiswary and P. Dananjayan. Detection of sinkhole attacks for mobile nodes in heterogeneous sensor networks with mobile sinks. pages 127–133. IEEE Computer Society, 2010.

[117] Ameer Ahmed Abbasi and Mohamed Younis. A survey on clustering algorithms for wireless sensor networks. volume 30, pages 2826–2841, Arábia Saudita, 2007. Elsevier Science Publishers B. V.

[118] Dali Wei and H. Anthony Chan. Clustering ad hoc networks: Schemes and classifications. In *Sensor and Ad Hoc Communications and Networks, 2006. SECON'06. 2006 3rd Annual*, pages 920–926, Reston, VA, USA, 2006. IEEE Computer Society.

[119] Mohammad Momani, Subhash Challa, and Rami. Alhmouz. Bayesian fusion algorithm for inferring trust in wireless sensor networks. volume 5, pages 815–822, 2010.

[120] Feng Li and Jie Wu. Mobility reduces uncertainty in MANETs. In *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pages 1946–1954. IEEE Computer Society, 2007.

[121] Andrew Whitby, Audun Jøsang, and Jadwiga Indulska. Filtering out unfair ratings in bayesian reputation systems. In *Proc. 7th Int. Workshop on Trust in Agent Societies*, 2004.

[122] Michael G. Solomon and Mike Chapple. *Information Security Illuminated*, pages 303–325. Jones and Bartlett Publishers, 2005.

[123] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt. Cross-level sensor network simulation with cooja. In *Local Computer Networks, Proceedings 2006 31st IEEE Conference on*, pages 641–648, Nov 2006.

[124] Adam Dunkels, Bjorn Gronvall, and Thiemo Voigt. Contiki-a lightweight and flexible operating system for tiny networked sensors. In *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*, pages 455–462. IEEE, 2004.

[125] Georg Wittenburg and Jochen Schiller. Running real-world software on simulated wireless sensor nodes. In *Proceedings of the ACM Workshop on Real-World Wireless Sensor Networks-REALWSN 06*, pages 7–11, 2006.

[126] Philip Levis, Nelson Lee, Matt Welsh, and David Culler. Tossim: Accurate and scalable simulation of entire tinyos applications. In *Proceedings of the 1st international conference on Embedded networked sensor systems*, pages 126–137. ACM, 2003.

[127] Ben L. Titzer, Daniel K. Lee, and Jens Palsberg. Avrora: Scalable sensor network simulation with precise timing. In *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks*, IPSN '05, Piscataway, NJ, USA, 2005. IEEE Press.

[128] Xu Li, Rongxing Lu, Xiaohui Liang, Xuemin Shen, Jiming Chen, and Xiaodong Lin. Smart community: an internet of things application. *Communications Magazine, IEEE*, 49(11):68–75, 2011.

ANEXO

Este anexo apresenta os resultados preliminares sobre o INTI considerando dados sintéticos aplicados aos cenários reais da IoT. Neste anexo foram empregados os mesmos parâmetros usados nas simulações apresentadas no Capítulo 5 com a única alteração nas áreas de $40m$x$40m$ para o cenário *smarthome* e de $80m$x$80m$ para o cenário de um condomínio. O uso destas áreas teve como objetivo conhecer a variação nos resultados obtidos. Além disso, as métricas empregadas são as mesmas definidas no Capítulo 5.

1. Eficiência no cenário *smarthome*

1.1 Funções assumidas pelos nós

Nesta avaliação, temos como referência a quantidade de nós associados, nós líderes, nós membros e nós livres calculados durante toda a simulação. Observa-se que com 30 nós e raio de $10m$, que a quantidade de nós que assumem uma função dentro da rede é de 35 nós ficando 5 nós livres. Quando o raio de alcance do nó aumenta para $20m$, a quantidade de nós líderes obtida é de quase 19 nós, conseguindo assim diminuir o número de nós membros e nós livres. Isto acontece porque há a sobreposição do raio de alcance de alguns nós. Além disso, quando os raios são de 30 e $40m$, essa sobreposição também aumenta. Estes resultados também são observados com 40 e 50 nós, como mostrado no gráfico da Figura 1.

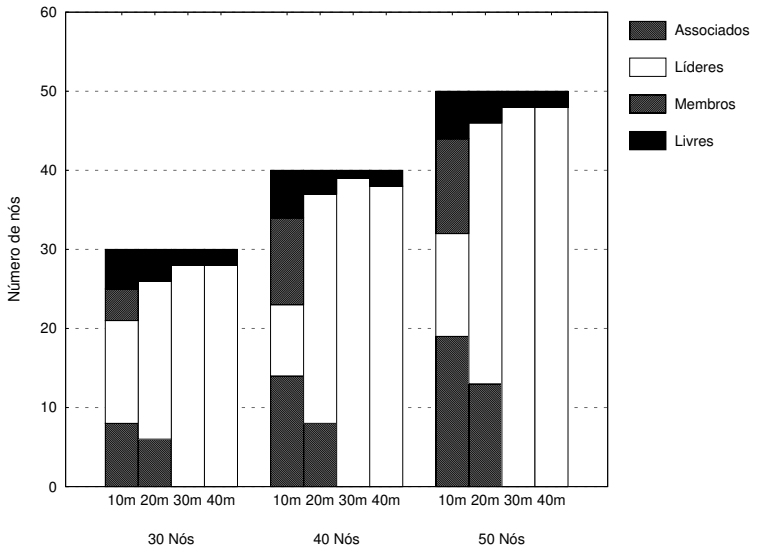

Figura 1: Funções assumidas pelos nós

1.2 Taxa de entrega

O sistema de detecção de intrusão INTI mostrou uma elevada taxa de entrega ($Tx_{Entrega}$), como visto no gráfico da Figura 2. Este gráfico apresenta três cenários variando os parâmetros como a quantidade de nós e o raio de alcance respetivamente. Inicialmente a taxa de entrega com 30 nós e com raio de 10 e 20m é superior a 90% e inferior de 98%. Para os raios de alcance de 30 e 40m a taxa de entrega atingida pelo sistema INTI é de 100%. No cenário com 40 nós e com raio de 10 e 20m a taxa de entrega alcançada superior a 90% e inferior de 99%. Quando o raio de alcance é aumentado para 30 e 40m a taxa de entrega obtida é de 100%. Por fim, com 50 nós com 10 e 20m a taxa de entrega é superior a 92% e inferior de 94%, e usando raios de 30 e 40m a taxa de entrega obtida é de 100%.

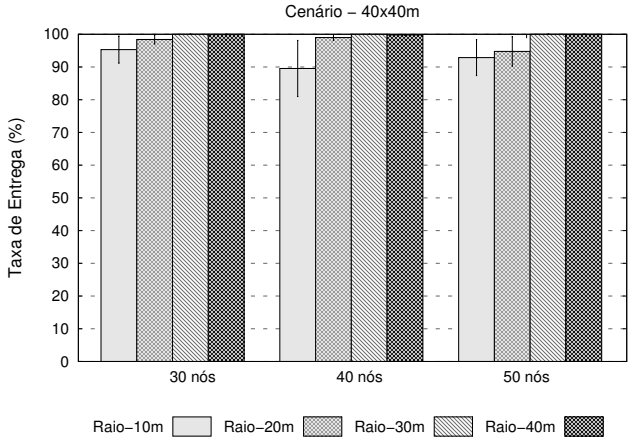

Figura 2: Taxa de entrega - $Tx_{Entrega}$

1.3 Latência

A latência -(L_T) alcançada pelo sistema INTI fazendo uso do raio de 10m é de 59ms chegando até um tempo de 88ms no pior dos casos, como ilustrado no gráfico da Figura 3. Este resultado elevado deve-se ao pequeno raio de alcance empregado pelos nós da rede. Contudo, a latência tende a diminuir quando os nós aumentam seu raio de alcance para 20, 30 e 40m atingindo até um tempo de 27ms. Com 40 nós e com um raio de alcance de 10m, a latência alcançada foi de 82ms, sendo menor quando com os raios de alcance de 20, 30 e 40m obtendo uma latência de 33ms. Já com 50 nós e raio de alcance de 10m, o INTI alcança apresenta um tempo de 90ms para em seguida diminuir este tempo e alcançar latências menores do que 37ms.

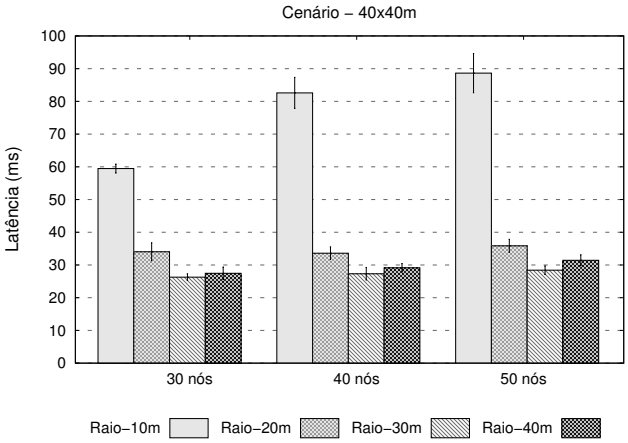

Figura 3: Latência -L_T

2. Eficiência no cenário condomínio

2.1 Funções assumidas pelos nós

Quando altera-se o parâmetro da área de 40x40m para 80x80m, a quantidade de nós que desempenham alguma função dentro da rede é apresentada na Figura 4. Percebe-se que o número de nós que desempenham alguma função dentro da rede aumenta de maneira proporcional para as três quantidades de nós. Nota-se, contudo, que a quantidade de nós livres tende a diminuir, sendo favorável para a rede conseguindo que mais nós consigam se comunicar. O comportamento observado para a quantidade de funções é que quanto maior o parâmetro de raio maior é comunicação e menor quantidade de nós livres.

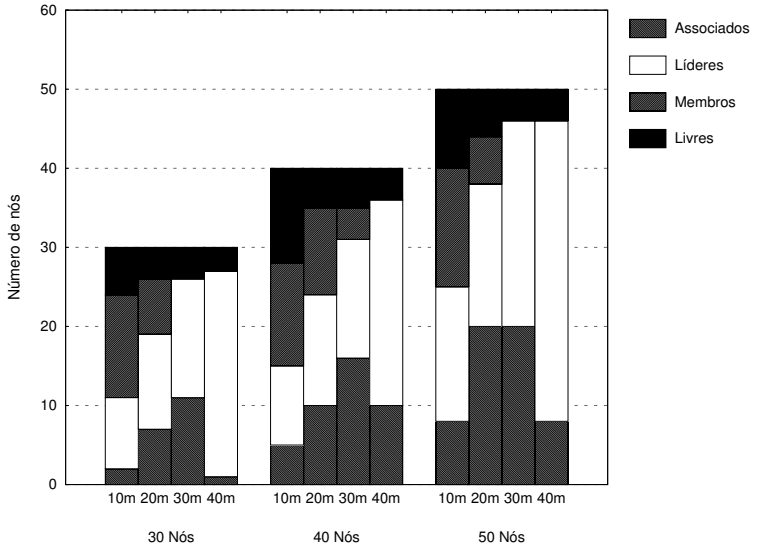

Figura 4: Funções assumidas pelos nós

2.2 Taxa de entrega

A taxa de entrega ($Tx_{Entrega}$) obtida pelo INTI em um cenário com área 80x80m é mostrada no gráfico da Figura 5. Observa-se que os resultados mostram uma elevada taxa de entrega em todas as simulações. Com 30 nós e com raio de alcance 10m, a taxa tem uma mínima de 69% chegando a diminuir até o 61% com 40 nós para logo melhorar até alcançar um 87% com 50 nós. Com 30 nós e um raio de alcance de 20m, a taxa de entrega obtida é de 92%, já no com 40 nós a taxa diminui até 78% para logo com 50 nós a taxa de entrega aumenta para 92%. Finalmente, com nós com raio de alcance de 30 e 40m, se consegue alcançar uma taxa de entrega superior ao 92% alcançando o 98%. Esta elevada taxa de entrega acontece devido à formação de agrupamentos utilizada pelo sistema INTI.

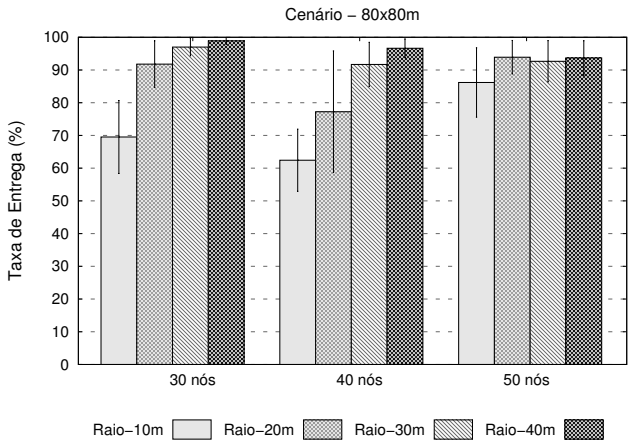

Figura 5: Taxa de entrega - $Tx_{Entrega}$

2.3 Latência

Para finalizar são apresentados os resultados obtidos pela latência (L_T) alcançada pelo sistema INTI no cenário de 80x80m com a quantidade de 30, 40 e 50 nós sobre diferentes raios de alcances, como raios de 10, 20, 30 e 40m, como mostrado no gráfico da Figura 6. Os resultados com 30 nós e diferentes tamanhos de raios de alcances apresentam uma pequena variação da latência chegando a obter uma latência inferior de 60 milissegundos (ms) com uma mínima de 28ms, fazendo uso do raio de alcance de 40m. Já com 40 nós e também diferentes raios de alcance, o sistema INTI obteve uma latência inferior a 60ms quase igual à latência alcançada com 40 nós.

Já com 50 nós e um raio de alcance de $10m$, a latência aumenta consideravelmente gastando até $92ms$. Isto acontece porque os nós se encontram muito distantes entre si. Desta forma, a medida que aumenta o raio de alcance para 20, 30 e $40m$, a latência melhora obter um tempo de uns $32ms$.

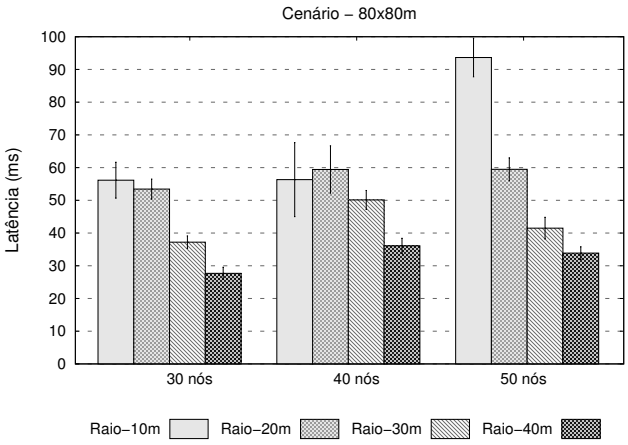

Figura 6: Latência -L_T