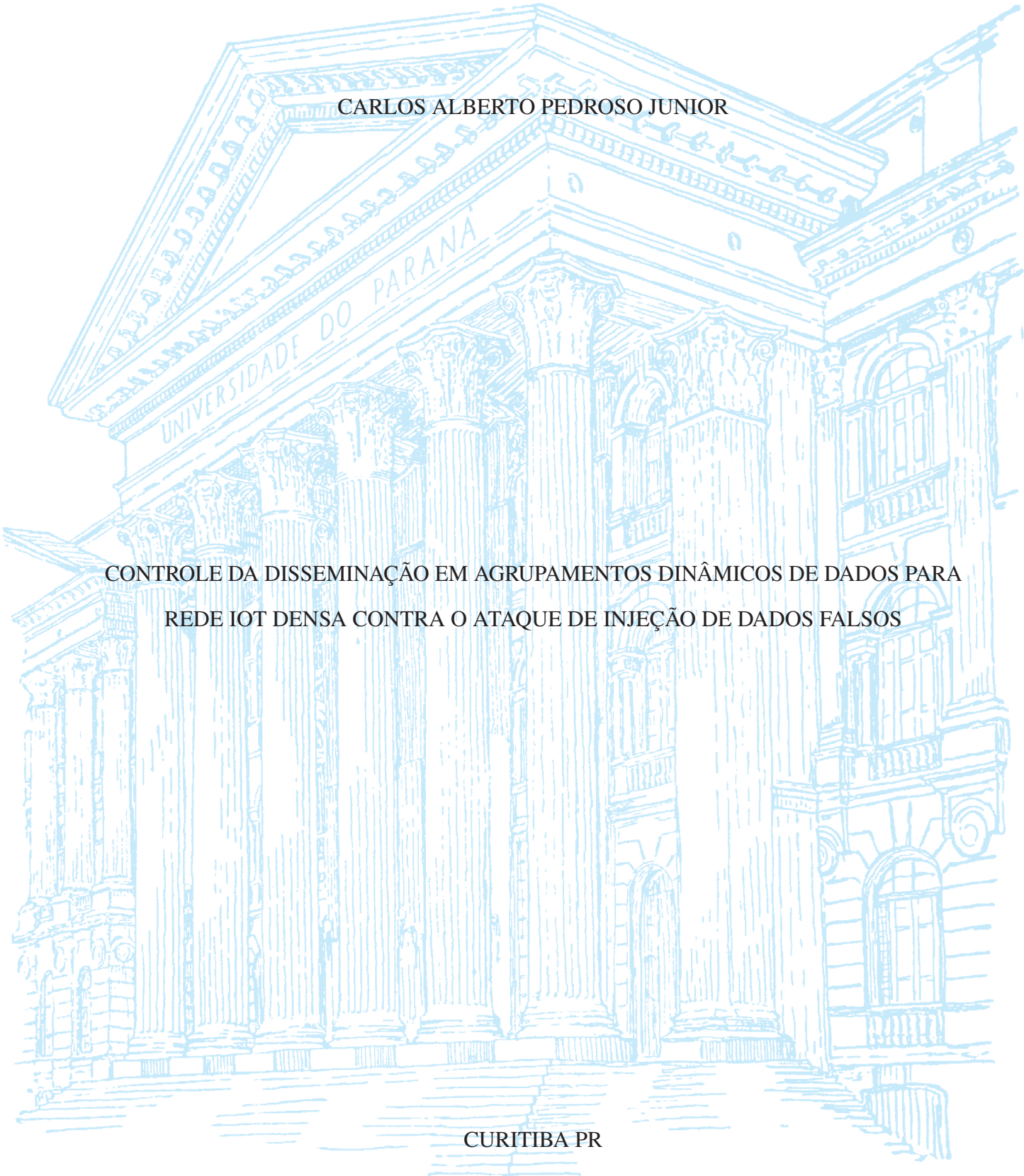
UNIVERSIDADE FEDERAL DO PARANÁ

CARLOS ALBERTO PEDROSO JUNIOR



CONTROLE DA DISSEMINAÇÃO EM AGRUPAMENTOS DINÂMICOS DE DADOS PARA REDE IOT DENSA CONTRA O ATAQUE DE INJEÇÃO DE DADOS FALSOS

CURITIBA PR

2019

CARLOS ALBERTO PEDROSO JUNIOR

CONTROLE DA DISSEMINAÇÃO EM AGRUPAMENTOS DINÂMICOS DE DADOS PARA REDE IOT DENSA CONTRA O ATAQUE DE INJEÇÃO DE DADOS FALSOS

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre em Informática no Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, da Universidade Federal do Paraná.

Área de concentração: *Ciência da Computação*.

Orientador: Aldri Luiz dos Santos.

CURITIBA PR

2019

CATALOGAÇÃO NA FONTE – SIBI/UFPR

P372c Pedroso Junior, Carlos Alberto

Controle da disseminação em agrupamentos dinâmicos de dados para rede IOT densa contra o ataque de injeção de dados falsos [recurso eletrônico]/ Carlos Alberto Pedroso Junior. Curitiba, 2019.

Dissertação (Mestrado) - Programa de Pós-Graduação em Informática, Setor de Ciências
Exatas, da Universidade Federal do Paraná.

Orientador: Aldri Luiz dos Santos.

1. Tecnologia da informação – Sistema de segurança. 2. Ciência da Computação. I. Santos, Aldri Luiz dos. II. Título.

CDD 005.8

Bibliotecária: Vilma Machado CRB9/1563

MINISTÉRIO DA EDUCAÇÃO
SETOR DE CIENCIAS EXATAS
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO INFORMÁTICA - 40001016034P5

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação em INFORMÁTICA da Universidade Federal do Paraná foram convocados para realizar a arguição da Dissertação de Mestrado de **CARLOS ALBERTO PEDROSO JUNIOR** intitulada: **Controle da disseminação em agrupamentos dinâmicos de dados em redes IoT densa contra o ataque de injeção de dados falsos**, sob orientação do Prof. Dr. ALDRI LUIZ DOS SANTOS, que após após terem inquirido o aluno e realizado a avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito de defesa.

A outorga do título de mestre está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

CURITIBA, 09 de Setembro de 2019.

ALDRI LUIZ DOS SANTOS
Presidente da Banca Examinadora (UNIVERSIDADE FEDERAL DO PARANÁ)

MICHELE NOGUEIRA LIMA
Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

EDUARDO DA SILVA
Avaliador Externo (INSTITUTO FEDERAL CATARINENSE)

MINISTÉRIO DA EDUCAÇÃO - UNIVERSIDADE FEDERAL DO PARANÁ - Setor de Ciências Exatas - Coordenação de Pós-Graduação em Informática

"Não importa o quanto você bate, mas sim o quanto aguenta apanhar e continuar. O quanto pode suportar e seguir em frente. É assim que se ganha."Rocky Balboa

AGRADECIMENTOS

À minha mãe Rosana Marcia Buzinaro, que sempre me apoio nos momentos difíceis me deu forças para continuar essa longa caminhada. Pela paciência, incentivos ao longo de todos o processo do mestrado. Sem esse suporte não conseguiria chegar a onde eu cheguei.

Ao Prof. Dr. Aldri Luiz dos Santos, meu orientador, sou grato por acreditar em mim desde o começo de nossa jornada no mestrado. Por sua paciência, dedicação, e estímulo de buscar sempre compreender o que era necessário para evoluir na pesquisa no decorrer do curso de mestrado.

À Prof. Dra. Michele Nogueira Lima pelos ensinamentos e conselhos durante todo o processo do curso de mestrado enquanto professora nas disciplinas e também coordenadora do Centro de Ciência de Segurança Computacional (CCSC) da UFPR.

Ao programa de Pós-Graduação em Informática da Universidade Federal do Paraná, por todo suporte administrativo prestado, que possibilitou minha participação em eventos e pela infraestrutura computacional disponibilizada. Agradeço a todos os funcionários do departamentos por sempre sempre atenciosos e corretos com os processos burocráticos.

Aos amigos do NR2 e CCSC Agnaldo Batista, Andressa Vergütz, Arthur Emilio Garcete Ferreira, Benevid Felix Silva, Bruno Henrique Schwengber, Bruno Marquez Cremonezi, Cainã Passos, Danilo Rodrigo Possati, Diego Milhomem Schmitt, Euclides Peres Farias Junior, Fernando Nakayama, Gustavo Henrique Carvalho de Oliveira, Igor Steuck Lopes, Ligia Francielle Borges, Marcos Antônio Dellazari, Mateus Pelloso, Nelson Gonçalves Prates Junior, Paulo Lenz Junior, Rafael Araújo da Silva e Yan Uehara de Moraes pela convivência, pelas argumentações e discussões técnicas e científicas, bem como pelo apoio durante o andamento das disciplinas e desenvolvimento da pesquisa.

Um agradecimentos especial a todos o amigos que sempre me apoiaram e deram suporte nos momentos de apreensão. Vocês fazem parte desta conquista.

RESUMO

A Internet das Coisas (IoT) considera a integração de diversos dispositivos e pessoas, em diferentes contextos. Essa integração tem possibilitado o surgimento de aplicações e serviços personalizados. Dentre as aplicações, aquelas voltadas ao contexto industrial (IIoT) têm se destacado, dado sua importância na produção de manufaturados e disponibilização de grandes volumes de dados. A disseminação desses dados representa o entendimento que aplicações têm sobre os serviços prestados e a interpretação deles gera respostas apropriadas. Porém, como qualquer rede, a IIoT está sujeita a apresentar vulnerabilidades, que quando são exploradas por usuários maliciosos, tendem a ser entrada para ataques, como o ataque de injeção de dados falsos (IDF). O ataque IDF tem por característica a adulteração, manipulação ou injeção de dados. Este tipo de ataque de intrusão se destaca por ser um dos mais agressivos às redes de dados como a IoT. A literatura apresenta diversas soluções para lidar com o ataque IDF, sejam baseadas em filtragem em rota, agrupamentos ou sistemas de detecção de intrusão. Contudo, elas não levam em consideração a validação dos dados, a identificação da atacante, a dinamicidade da rede. Portanto, elas ainda não atendem adequadamente os requisitos necessários para uma IoT densa. Nesses ambientes, os dados gerados pelos dispositivos devem estar disponíveis para as aplicações acessá-los e tomar decisões. Essa dissertação tem como objetivo proteger o serviço de disseminação de dados em rede IoT densa no contexto industrial, a fim de melhorar a tomada de decisão das aplicações. Foram pesquisadas técnicas de monitoramento (vigilância) *watchdog*, sistemas de detecção de intrusão e consenso colaborativo, de maneira de entender e investigar suas características e possibilidade para uma integração entre elas. Desta forma, este trabalho apresenta um mecanismo para mitigação do ataque IDF sobre o serviço de disseminação de dados de redes IoT densa, chamado CONFINIT (***CON****sensus Based Data* ***FI****lteri****N****g for* ***IoT***). Ele busca detectar e isolar da rede dispositivos IoT maliciosos que apresentem comportamento de ataque IDF. O CONFINIT utiliza agrupamentos por similaridade para lidar com densidade de dispositivos na rede; e combina as estratégias de *watchdog* para o monitoramento entre os participantes e consenso colaborativo para a tomada de decisão. Essa combinação favorece uma filtragem colaborativa que torna-se mais precisa e dinâmica diante de ataques. O CONFINIT foi avaliado no simulador NS-3, e os resultados obtidos mostram sua capacidade em garantir a disseminação de dados segura em um ambiente IoT denso no contexto industrial. Ele obteve uma taxa de detecção de até 99%, variando conforme o número de dispositivos presentes na rede; demonstrando que os dados sensoriados e disponibilizados às aplicações são assegurados.

Palavras-chave: IoT, Disseminação de Dados, Agrupamento Seguro, Ataque de Injeção de Dados Falsos, Segurança

ABSTRACT

The Internet of Things (IoT) considers the integration of multiple devices and people in different contexts. This integration has enabled the emergence of custom applications and services. Among the applications, those focused on the industrial context (IIoT) have been highlighted, given their importance in the production of manufactured goods and the availability of large volumes of data. The dissemination of this data represents the understanding that applications have about the services provided and their interpretation generates appropriate answers. However, like any network, IIoT is subject to vulnerabilities, which when exploited by malicious users, tend to be entry to attacks such as the false data injection (FDI) attack. The FDI attack is characterized by tampering, manipulation or injection of data. This type of intrusion attack stands out for being one of the most aggressive to data networks like IoT. The literature presents several solutions for dealing with the IDF attack, whether based on route filtering, clustering or intrusion detection systems. However, they do not take into account data validation, attacker identification, network dynamics. Therefore, they still do not adequately meet the requirements for dense IoT. In these environments, data generated by devices must be available for applications to access and make decisions. This dissertation aims to protect the dense IoT network data dissemination service in the industrial context, in order to improve decision making of applications. Monitoring techniques (surveillance) *watchdog*, intrusion detection systems and collaborative consensus were investigated in order to understand and investigate their characteristics and possibilities for integration between them. Thus, this paper presents a mechanism for mitigating the IDF attack on the dense IoT network data dissemination service, called CONFINIT (***CON*** *sensus Based Data****FI*** *lteri* ***N*** *g for* ***I*** *or* ***T***), which seeks to detect and isolate malicious devices that exhibit FDI attack behavior from the IoT network. The CONFINIT uses similarity clusterion to handle device density on the network; and combines *watchdog* strategies for monitoring among participants and collaborative decision-making consensus. This combination favors collaborative filtering that becomes more accurate and dynamic in the face of attacks. CONFINIT was evaluated in the NS-3 simulator, and the results obtained show their ability to ensure secure data dissemination in a dense IoT environment in the industrial context. It achieved a detection rate of up to 99%, varying according to the number of devices present on the network; demonstrating that the data sensed and made available to the applied ones are assured.

Keywords: IoT, Data Dissemination, Secure Clustering, False Data Injection Attack, Security

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

6LoWPAN	***IPv6 over Low power Wireless Personal Area Networks*** (IPv6 sobre redes sem fio pessoais de baixa potência)
AODV	***Ad Hoc On-Demand Distance Vector*** (Vetor de Distância Ad Hoc Sob Demanda)
BECAN	***Bandwidth-Efficient Cooperative Authentication*** (Autenticação Cooperativa Eficiente de Largura de Banda)
BS	***Base Station*** (Estação Base)
CDM	***Consensus Decision Making*** (Tomada de Decisão por Consenso)
CONFINIT	***Consensus Based Data Filtering for IoT*** (Consenso Baseado em Filtragem de dados para IoT)
CNR	***Cooperative Neighbor Router*** (Roteador Cooperativo de Vizinhos)
CoS	***Center-of-Stimulus*** (Centro de Estímulos)
CPS	***Cyber Physical System*** (Sistemas Ciber Físicos)
CWS	***Cooperative Watchdog System*** (Sistema de vigilância cooperativa)
DDoS	***Distributed Denial of Service*** (Ataque de Negação de Serviço Distribuído)
DDFC	***Dynamic Data-aware Firefly-based Clustering*** (Agrupamentos baseado em vaga-lumes para reconhecimento de dados dinâmicos)
DEF	***Dynamic En-route Filtering Scheme*** (Esquema de Filtragem Dinâmica em Rota)
EEMDT	***Energy Efficient Multipath Data Transfer Scheme*** (Esquema de Transferência de Dados Multicaminhos com Eficiência Energética)
GFFS	***Geographical-Information Based False Data Filtering Scheme*** (Esquema de Filtragem de Dados Falsos Baseado em Informação Geográfica)

GPS	***Global Positioning System*** (Sistema de Posicionamento Global)
HBT	***Bayesian Spatial-Temporal Hierarchical*** (Hierárquico Bayesiano Espacial-Temporal)
IDF	**Injeção de Dados Falsos**
IDS	***Intrusion Detection System*** (Sistema de Detecção de Intrusão)
IEEE	***Institute of Electrical and Electronics Engineers*** (Instituto de Engenheiros Eletricistas e Eletrônicos)
IETF	***Internet Engineering Task Force*** (Força Tarefa de Engenharia da Internet)
IoT	***Internet of Things*** (Internet das Coisas)
IIoT	***Industrial Internet of Things*** (Internet das Coisas Industrias)
IPv6	***Internet Protocol Version 6*** (Protocolo de Internet Versão 6)
MAC	***Message Authentication Code*** (Código de Autenticação de Mensagem)
MIT	***Massachusetts Institute of Technology*** (Instituto de Tecnologia de Massachusetts)
NFC	***Near Field Comunication*** (Comunicação por Campo de Proximidade)
NFFS	***Neighbor-Information Based False Data Filtering Scheme*** (Esquema de Filtragem de Dados Falsos Baseado em Informação de Vizinhos)
PPGINF	Programa de Pós-Graduação em Informática
RPL	***Radio-Frequency Identification Routing Protocol for Low-Power and Lossy*** (Protocolo de Roteamento para Baixa Potência e com Perdas)
RFID	***Radio-Frequency Identification*** (Identificação por Rádio Frequência)
RSSF	Redes de Sensores Sem Fio
SEF	***Statistical En-route Filtering*** (Filtragem Estatística em Rota)
SPAIS	***Self-checking Pollution Attackers Identification Scheme***

	(Esquema de Identificação de Ataques de Poluição)
STEF	***Secure Ticket-Based En-route Filtering Scheme***
	(Esquema Seguro de Filtragem em Rotas com Base em Tickets)
Tathachi	***Detection of Sinkhole And Selective-Forwarding for Supporting Secure Routing for Internet of ThIngs***
	(Detecção de Sinkhole e Encaminhamento Seletivo para Suporte ao Roteamento Seguro para Internet das Coisas)
VANET	***Vehicular Ad Hoc Network***
	(Rede Ad Hoc Veicular)
V-REP	***Virtual Robotic Experimentation Platform***
	(Plataforma Virtual de Experimentação Robótica)
VEBEK	***Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks***
	(Criptografia e Codificação Baseadas em Energia Virtual para Redes de Sensores sem Fio)
VPA	***Virtual Personal Assistent***
	(Assistente Pessoal Virtual)

LISTA DE SÍMBOLOS

C	Conjunto de nós da rede
n_j	Nó
Id	Identificador Único
G	Grafo
V	Vértice
E	Aresta
T	Tempo
Id_{ataq}	Identificador do atacante
L_{ataq}	Leitura individual do atacante
Id_{int}	Identificador do nó que identificou o atacante
N_c	Nó capturado
M_c	Conjunto de vizinhança
X_i	Primeiro valor
M_A	Média aritmética
N_a	Conjunto de valores
N_{ma}	Elemento avaliados
N	Numero de elementos da equação
M_c	Quantidade de elementos avaliados da equação
L_{ind}	Leitura individual
N_{viz}	Número de vizinhos
L_{agr}	Leitura agregada
A_α	Subconjunto de nós que fazem parte do agrupamento
T_{det}	Taxa de detecção
R_a	Acurácia
T_{fp}	Taxa de falsos positivo
T_{fn}	Taxa de falsos negativos

SUMÁRIO

1 INTRODUÇÃO

A evolução da Internet vem possibilitando o surgimento de diferentes paradigmas de comunicação entre dispositivos. Neste contexto, está a Internet das coisas (do inglês, *Internet of things* - IoT), que tem se consolidado como a Internet do futuro, devido à sua fácil integração e disponibilização em diferentes contextos e serviços (Palattella et al., 2016). Assim, estima-se que os investimentos para o desenvolvimento em torno da IoT possam chegar a 7,1 trilhões de dólares até o ano de 2025 (Heinonen, 2018), desde o seu desenvolvimento, atribuído ao trabalho do laboratório Auto-Id no Instituto de Tecnologia do Massachusetts (do inglês, *Massachusetts Institute of Technology* - MIT) (Fleisch, 2010). Logo, a IoT saiu do escopo que era atrelado ao Identificador de Radiofrequência (do inglês, *Radio Frequency Identification* - RFID) para integrar novos objetos como lâmpadas, geladeiras, máquinas industriais, veículos, entre outros (Borgia, 2014). Além disso, dispositivos como sensores, atuadores e celulares passaram também a fazer parte do escopo da IoT. O aperfeiçoamento desses dispositivos trouxe avanços com a composição de novos componentes físico e digitais, e tem estimulado ainda mais o desenvolvimento da IoT e possibilitado melhorias em diversos campos onde ela está inserida (Gubbi et al., 2013).

A IoT pode ser definida como uma rede híbrida, aberta e heterogênea que integra diversos dispositivos, sendo que sua característica híbrida atribui-se pela diversidade de modelos que compõem seu contexto, integrando as redes estruturadas e não estruturadas. Uma rede aberta permite que inúmeras entidades propiciem diferentes tipos de serviços a diversos clientes (Botta et al., 2016). Já a heterogeneidade da IoT é determinada pela grande diversidade de objetos abrangidos pela rede e que apresentam diferentes características, como mobilidade, identidades, recursos energéticos e atributos físicos. Esses dispositivos usam interfaces inteligentes para estabelecerem comunicação entre eles (Borgia, 2014). Logo, através da IoT é possível gerenciar os serviços de mensuração de temperatura, umidade, pressão de dutos, rastreamento de objetos e monitoramento de funções vitais de uma pessoa que pode ser oferecido em tempo real.

Diversos dispositivos passam a integrar a IoT e os domínios de aplicação podem cada vez mais desenvolver aplicações que tornam os serviços personalizados e impulsionam o crescimento na mesma proporção (Perera et al., 2014). Assim, as aplicações em diferentes contextos como Indústria inteligente (do inglês, *Smart Industry*), cidade inteligente (do inglês, *Smart City*), casa inteligente (do inglês, *Smart Home*) e saúde inteligente (do inglês, *Smart Health*), estão destacando-se entre os maiores investimento em pesquisa. No contexto de *Smart City*, as cidades são construídas por aplicações e serviços oferecidos à população em tempo real, que vão desde aferição de temperatura, controle de tráfego, controle de poluição, integração aos transportes inteligentes, monitoramento de vigilância e até melhorias no âmbito da saúde Li et al. (2018). Na *Smart Home*, os objetos domésticos passam a integrar uma rede onde todos trocam informações, desde geladeiras, lâmpadas a sensores de movimento. Uma realidade é o uso de "assistente pessoal virtual" (do inglês, *Virtual Personal Assistent* -VPA), criado pela Amazon e Google, e os ecossistemas domésticos como Apple Homekit e Alexa. O contexto de *Smart Health*, destacam-se o monitoramento de pacientes à distância e o controle de medicamentos via celular, além de todo o desenvolvimento e coleta de dados de pacientes (Chung et al., 2017).

Embora existam diversas pesquisas voltadas para os domínios em *Smart city*, *Smart Home* e *Smart Health*, as aplicações em *Smart Industry* têm se mostrado também um novo desafio para pesquisadores. Assim, o paradigma de Internet das coisas Industriais (do inglês, *Industrial Internet of Things* - IIoT) vem destacando-se pela fácil integração entre os dispositivos dentro de uma indústria possibilitando que eles trabalhem de forma sincronizada e organizada (Vermesan e

Friess, 2013). Além disso, os Sistemas Cyber Físicos (do inglês, *Cyber-Physical System* - CPS) têm possibilitado a integração dos meios físicos e digitais e integram a IIoT fazendo parte do novo paradigma chamado Indústria 4.0 ou 4ª revolução industrial (Lee et al., 2014). Desta forma, as fábricas totalmente conectadas são controladas por máquinas autônomas; a produção passa a ser gerenciada por sensores capazes de estimar quando o maquinário possa vir a apresentar falhas. O gerenciamento de estoque e a logística passam a ter integração total com a linha de produção, sendo capaz de avaliar o estoque em tempo real e enviar as informações ao centro de controle. Com essas informações é possível reduzir o tempo de produção, fornecer diagnóstico em tempo real e ter um melhor fluxo de informações, melhorando o desempenho como um todo. Logo, esses serviços geram um grande volume de dados que necessitam ser coletados e disseminados de maneira segura e eficiente. Assim, os serviços de disseminação de dados tornam-se fundamentais ao desenvolvimento das aplicações (Furlaneto et al., 2012; Yaqoob et al., 2017; Kouicem et al., 2018) e a segurança tem papel essencial na evolução da IoT (Atzori et al., 2010).

Contudo, devido às suas características, as ameaças à segurança de dispositivos IoT crescem à medida que novos dispositivos são inseridos na rede (Miorandi et al., 2012; Sadeghi et al., 2015). Muitas das ameaças buscam encontrar vulnerabilidades para que os atacantes possam observar e muitas vezes alterar os dados coletados e transmitidos na rede. Este comportamento prejudica os serviços de coleta e disseminação de dados, perturbando o funcionamento da rede e gerando inconsistência nos dados. Além de tudo, a IoT necessita prover atributos de robustez e segurança como confiabilidade, integridade e disponibilidade; características naturais que uma rede resiliente deve prover (Chen et al., 2017). Assim, soluções que atuem para evitar as falhas e os prejuízos causados por atacantes colaboram para consolidar a IoT como a Internet do futuro.

Em uma rede como a IoT, a coleta e a disseminação de dados devem considerar a heterogeneidade dos dispositivos integrantes da rede (Gielow et al., 2014) Existem dispositivos com recursos computacionais com restrições de processamento, armazenamento e energia; também existem os que não apresentam estas restrições. Deve-se considerar que, em alguns casos, a transmissão de dados representa grande parcela do consumo de energia, afetando a vida útil dos objetos IoT. Logo, uma disseminação eficiente e segura é vital para melhorar o tempo de funcionamento da rede e dos dispositivos e garantir que os dados estejam sempre disponíveis para serem acessados pelas aplicações (Rault et al., 2014). Consequentemente, considerar a capacidade dos dispositivos é essencial para garantir a continuidade de serviços realizados (Alduais et al., 2016). Assim, o serviço de disseminação de dados na IoT é imprescindível para o bom desenvolvimento de aplicações orientadas a dados (Meng et al., 2016).

1.1 MOTIVAÇÃO

A garantia de coleta e disseminação de dados segura aos dispositivos integrantes de um rede IoT é fundamental para apoiar o sucesso de aplicações nos diferentes domínios que ela está inserida. Assim, os serviços simples como mensuração de temperatura, ou os mais complexos, como a produção de manufaturados, devem ser livres de falhas (Nunes et al., 2015). Certificar a menor quantidade de falhas devido às características da rede torna-se um grande desafio. Estas falhas podem ser geradas por fatores como mobilidade, limitações de recursos, tecnologia de comunicação ou até mesmo o contexto onde a rede está inserida. Neste sentido, diminuir erros de transmissão, perdas de pacotes, que geram alta taxa de transmissão e consequentemente consomem mais recursos é essencial para reduzir essas falhas e contribui para uma melhor disponibilidade dos serviços, beneficiando o funcionamento da rede (Sethi et al., 2015). Contudo, nem todas as falhas se devem problemas de comunicação ou mobilidade. Algumas são decorrentes de usuários maliciosos (atacantes) que exploram as vulnerabilidades da rede. Os atacantes

se aproveitam de brechas no sistema para controlar os dispositivos, alterar seu comportamento, gerar inconsistência nos dados e, assim, degradar a qualidade do serviço. Esses atacantes são uma grande ameaça ao serviço de disseminação de dados visto que eles passam a conhecer os dados trafegados.

Existem diversos ataques que buscam comprometer a integridade, privacidade e disponibilidade dos dados em redes IoT, entre eles destacam-se o *selective forwarding*, *black hole*, *Sybil* e Injeção de dados falsos (IDF) (Sen e Madria, 2017). Um ataque *selective forwarding* tem como objetivo encaminhar apenas os pacotes selecionados pelos atacante, descartando os demais. O ataque *black hole* tem por característica os princípio de um "buraco negro", o de sugar tudo o que desejar, descartando de forma silenciosa todos os pacotes pretendidos. Já um ataque *Sybil* caracteriza-se por forjar diferentes identidades no mesmo dispositivo físico com o intuito de se passar por um legítimo. Por fim, o ataque IDF é responsável por manipular, adulterar e injetar dados não condizentes com os coletados pelos dispositivos. O atacante pode capturar dispositivos e controlar, ou mesmo se passar por um dispositivo legítimo, com o intuito de perturbar o funcionamento da rede (Illiano e Lupu, 2015). Esse ataque é considerado um dos mais nocivos às redes de dados devido à inconsistência das informações geradas e à imprevisibilidade do seu acontecimento (Deng et al., 2016; Sen e Madria, 2017). Assim, essa dissertação abordará a fundo o ataque IDF e sua forma de atuar contras redes de dados.

Com o objetivo de proteger a disseminação de dados contra a ameaça de ataques IDF, diversas contramedidas são implementadas para garantir a disponibilidade e integridade do serviço. Essas contramedidas são aplicadas na proteção de sistemas ou redes em diferentes contextos, dentre elas são evidenciadas as abordagens em filtragem em rota (Lu et al., 2012; Kumar e Pais, 2018), sistema de detecção de intrusão (IDS) (Yang et al., 2017; Cervantes et al., 2018) e detecção colaborativa (Li et al., 2017). Os esquemas de filtragem em rota são constantemente aplicados para proteger a rede, principalmente em redes de sensores sem fio (RFFS). Caracterizam-se por realizar a identificação de ataques IDF através da checagem do Código de Autenticação de Mensagens (do inglês, *Message Authentication Code*- MAC). O MAC é usado para verificar se existiu alguma alteração na mensagem entre a origem e o destino, podendo ocorrer nos nós encaminhadores ou mesmo na estação base. Entretanto, a verificação apenas do MAC não considera a alteração do dado transmitido, bem como a identificação e exclusão dos dispositivos que estão executando a ação maliciosa. Desta forma, problemas como a alta taxa de retransmissão, reincidência de ataques, consumo energético fazem com que a disponibilidade dos dados seja comprometida (Mahmoud et al., 2015).

Os IDS são alternativas robustas para lidar com os ataques de intrusão em diferentes contextos, pois oferecem informações sobre os invasores, facilitando a detecção e identificação de intrusos na rede (Kumar et al., 2016). Eles podem ser divididos em duas categorias: baseado em dispositivo ou baseado em rede. Os IDS baseados em dispositivos são sistemas que monitoram atividades de ataques em diversos ou em determinado dispositivo. As decisões são tomadas com base nas informações coletadas por estações específicas. Trata-se de uma abordagem distribuída, que pode utilizar diversos dispositivos em prol da proteção de um sistema. Os IDS baseados na rede normalmente utilizam apenas um dispositivo ou software para monitorar uma rede, que se encarrega de analisar o tráfego em busca de anomalias que possam afetar a rede ou um sistema. Se bem posicionado, ele é capaz de monitorar todo um sistema sem acarretar custos adicionais. Entretanto, o custo computacional pode ser elevado pois é gerado um alto consumo de recursos, e também podem gerar novas vulnerabilidades (Cervantes et al., 2018).

Embora as soluções de filtragem em rota, o IDS e a detecção colaborativa demonstrem ser adequadas para lidar com o ataque IDF. Elas não são totalmente adequadas quando aplicadas em um contexto de IoT. Usar diferentes abordagens para lidar com o problema torna-se

um desafio a ser superado. Para tal, há abordagens com potencial para suprir a busca por segurança na IoT, dentre elas destacam-se a técnica de consenso (Li et al., 2014) e a técnica de monitoramento *watchdog* (Nadeem e Howarth, 2013; Wahab et al., 2014). A abordagem de consenso pode ser utilizada de forma totalmente distribuída entre os participantes da rede, o que garante uma avaliação e decisão mais robusta e participativa entre os integrantes da rede. Normalmente, o consenso é empregado para desenvolver decisões colaborativas e distribuídas, podendo ser aplicado sem a presença de uma entidade reguladora (Li et al., 2014). Há vários trabalhos que abordam o consenso como uma forma de problema a ser resolvido (Colistra et al., 2014b). Porém, vem crescendo o movimento do uso de consenso como abordagem contra ameaça (Toulouse et al., 2015). Assim, ao empregar essa abordagem em um contexto como a IoT, ganha-se em escalabilidade, robustez e segurança.

A técnica de vigilância (monitoramento) *watchdog* é constantemente utilizada em sistemas distribuídos onde os próprios participantes ficam encarregados de vigiar seus vizinhos. Ela pode ser empregada na forma de monitoramento contínuo ou monitoramento discreto (Movahedi e Hosseini, 2017). Na forma contínua, o monitoramento ocorre sem um período de intervalos, o que adiciona uma nova função de monitoramento aos participantes do sistema. No discreto, os períodos de monitoramento podem variar de acordo com o sistema e o tipo de dispositivo verificado (Wahab et al., 2014). Nesse sentido, o uso das duas técnicas viabiliza detectar e isolar a presença de ameaças em uma rede IoT, garantindo assim a integridade e disponibilidade ao serviço de disseminação de dados de forma segura.

1.2 PROBLEMA

O desenvolvimento da IoT tem permitido que diferentes domínios de aplicação ofereçam serviços cada vez mais personalizados. Assim, atividades como o gerenciamento de chão de fábrica, o controle de produção e o monitoramento de recursos são propostas que buscam inovar a forma como a produção funciona. Isso torna-se viável devido às interações entre objetos que disponibilizam diversos tipos de informações. Essas informações são essenciais para o desenvolvimento de aplicações futuras, e portanto a consolidação da IoT em diferentes domínios. Entretanto, lidar com o grande volume de dados gerados por aplicações expõe a IoT a diversas vulnerabilidades, que violam atributos de segurança, integridade, autenticidade e disponibilidade de serviços, entre eles a disseminação de dados dentro da rede (Lima et al., 2009; Sicari et al., 2015).

Particularmente, entre as ameaças internas ao serviço de disseminação de dados na IoT, destaca-se o ataque de injeção de dados falsos (IDF), considerado um dos ataques de intrusão mais nocivos às redes orientadas a dados, devido à inconsistência das informações geradas e à sua imprevisibilidade de acontecimento (Hug e Giampapa, 2012). O ataque IDF é relativamente recente na literatura, e teve seus primeiros registros datados em meados da década passada. Porém, ele vem mostrando alto potencial contra redes como a IoT (Mo et al., 2010; Kumar et al., 2016). O ataque IDF pode realizar-se de duas formas: quando um dispositivo é capturado por outro dispositivo e tem os seus dados fabricados ou alterados, e quando o próprio dispositivo apresenta um comportamento de má conduta (Yang et al., 2015). Esse comportamento dificulta a identificação de dispositivos maliciosos e aumenta o tempo de mal funcionamento da rede, gerando inconsistência nos dados (Deng et al., 2016). Assim, o ataque IDF veem se mostrando uma real ameaça às redes orientadas a dados como a IoT (Kumar et al., 2016).

O principal problema abordado nesta dissertação consiste em **como viabilizar um ambiente seguro ao serviço de disseminação de dados em um ambiente IoT denso, diante da ameaça de atacantes que visam comprometer a autenticidade dos dados disponibilizados**

para tomada de decisão de aplicações. Contramedidas são aplicadas para identificar e isolar a presença de atacantes IDF com o intuito de melhorar o desempenho de segurança nas redes. As atuais abordagens empregadas para lidar com os ataques IDF são: *(i)* esquemas de filtragem em rota, *(ii)* detecção colaborativa e *(iii)* sistemas de detecção de intrusão. Contudo, elas têm falhado ou não são adequadas ao contexto de IoT densa, visto que podem gerar alto consumo de recursos, não checam os dados e não identificam e isolam a presença de ameaças. Além disso, poucas consideram a detecção colaborativa por parte de participantes da rede. Dessa maneira, torna-se necessário pesquisar novas formas de detecção a fim de viabilizar serviços mais seguros perante ameaças contra a disseminação de dados numa rede IoT. Assim, esta dissertação busca explorar e responder as seguintes questões de pesquisa atreladas ao problema levantado:

- **O monitoramento entre participantes dentro de uma rede IoT pode colaborar para melhorar a detecção de atacantes IDF?** Permitir o monitoramento entre os participantes de uma rede ajuda na criação de mecanismos robustos e dinâmicos. Tendo em vista que uma rede escalar como a IoT, quando monitorada apenas por uma entidade controladora, apresenta dificuldade no seu crescimento, afetando diferentes serviços;

- **As decisões consensuais podem garantir uma detecção e isolamento mais assertivos?** A tomada de decisão sobre possíveis ameaças dentro de uma rede orienta dados, como a IoT, deve ser extremamente precisa e eficiente, pois todos os dispositivos participantes são importantes para seu funcionamento. Logo, a execução de uma detecção e isolamento de ameaças garante que dispositivos maliciosos não continuem a afetar o funcionamento da rede e uma melhor tomada de decisão nas aplicações;

- **A união de consenso com o monitoramento *Watchdog* pode melhorar a segurança de uma rede IoT, e portanto garantir mais disponibilidade a serviços?** O monitoramento *watchdog* baseia-se na colaboração entre diferentes participantes de um mesmo ambiente. Já o acordo através do consenso baseia-se na tomada de decisão em conjunto. O relacionamento entre essas duas abordagens pode proporcionar melhores tomadas de decisão sobre a identificação e o isolamento de ameaças que desorientam a rede.

1.3 OBJETIVO

Esta dissertação tem como objetivo detectar e isolar a presença de atacantes IDF atuando no serviço de disseminação de dados das redes IoT massiva. Para atingir este objetivo é proposto um sistema de detecção de intrusão para mitigação do ataque IDF sobre o serviço de disseminação de dados de redes IoT massiva, chamado CONFINIT (***CON****sensus Based Data* ***FI****lteri****N****g for* ***IoT***). Este sistema tem como intuito possibilitar a identificação e isolamento de atacantes IDF a partir da comparação de leituras sensoriadas similares entre dispositivos IoT vizinhos espaciais participantes da rede. Ele combina as estratégias de *watchdog* para o monitoramento entre participantes e de consenso colaborativo para a tomada de decisão sobre a presença de dispositivos atacantes. Assim, quando os dispositivos maliciosos são identificados, eles são isolados e impossibilitados de participar da rede. Desta forma, apenas nós honestos podem disseminar seus dados dentro da rede. Dessa maneira, foram definidos os seguintes objetivos específicos com a finalidade de atingir o objetivo geral:

- Desenvolver um mecanismo para filtragem de dados falsos com base na similaridade de leituras entre os dispositivos de um rede IoT;

- Implementar o mecanismo proposto em um simulador de redes para analisar a real viabilidade da proposta;
- Pesquisar as principais contra medidas ao ataque IDF e elaborar uma síntese sobre ele com base em comparações e abordagens;
- Analisar os resultados obtidos de simulações e verificar a validação do modelo, atestando o atendimento aos requisitos, e avaliar suas vantagens e desvantagens, bem como pontos de melhorias.

1.4 CONTRIBUIÇÕES

O desenvolvimento desta pesquisa produziu contribuições científicas na área de redes de computadores, com ênfase na segurança de redes IoT voltada à gerência de dados, através do uso de sistema de detecção de intrusão baseado em vigilância *watchdog* e consenso colaborativos entre dispositivos.

- *Um levantamento sobre o estado da arte:* O estudo apresenta uma classificação e discussão em forma de síntese sobre as principais técnicas usadas contra o ataque IDF em diferentes contextos e tipos de redes, além de avaliar quais são as mais relevantes e abordadas. Ainda, foi analisado como são empregadas as técnicas de vigilância *watchdog* e Consenso colaborativo e como elas permitem estabelecer uma melhor segurança na rede, a partir do monitoramento e detecção de ameaças presentes;
- *A elaboração de um IDS chamado CONFINIT:* Ele baseia-se na similaridade para formar agrupamentos e lidar com a densidade da rede, além de combinar as estratégias de *watchdog* para o monitoramento entre participantes e consenso colaborativo para tomada de decisão sobre dispositivos IDF. Dessa forma, contribui para manter a disponibilidade dos dados disseminados na rede;
- *Avaliação e análise da eficácia do CONFINIT:* Uma análise e discussão sobre os resultados obtidos pelo mecanismo na detecção do ataque IDF, bem como o impacto que o ataque pode causar em uma redes de dados como a IoT. Além disso, uma investigação das vantagens e desvantagens das técnicas empregadas na construção do mecanismo.

1.5 ESTRUTURA

Esta dissertação de mestrado está estruturada em seis capítulos. O Capítulo 2 apresenta os fundamentos e a contextualização da rede IoT em diferentes aspectos e aplicações. Também apresenta os requisitos necessários à compreensão do problema e as principais técnicas abordadas. O Capítulo 3 discute os principais trabalhos que buscam resolver o problema do ataque IDF e quais são as suas vantagens e desvantagens. Também são apresentados como o consenso colaborativo e monitoramento *watchdog* vêm sendo empregados. O Capítulo 4 descreve o mecanismo CONFINIT para detecção e mitigação de ataque de injeção de dados falsos. O Capítulo 5 apresenta a implementação e avaliação de segurança sobre o mecanismo. O Capítulo 6 conclui esta dissertação e apresenta direcionamentos futuros para a pesquisas futuras.

2 FUNDAMENTOS

Este capítulo apresenta os fundamentos necessários para a compreensão do contexto da pesquisa, do problema e da proposta. A Seção 2.1 apresenta as características gerais da IoT, sua arquitetura, tecnologias existentes até o presente momento, disseminação de dados e domínios de aplicação. A Seção 2.2 descreve as técnicas de agrupamentos baseadas na dinamicidade de dispositivos e dados. A Seção 2.3 aborda os aspectos de segurança em redes IoT, bem como os requisitos necessários para alcançá-la. A Seção 2.4 apresenta as principais ameaças existentes na IoT e descreve o funcionamento do ataque IDF. Por fim, a Seção 2.5 descreve as técnicas aplicadas para mitigar o ataque IDF, além de detalhar como o uso das técnicas de Consenso e *watchdog* podem ser utilizadas contra o ataque IDF.

2.1 INTERNET DAS COISAS

A primeira vez que o termo "Internet das coisas" foi empregado ocorreu em 1999 pelo pesquisador do MIT Kevin Ashton (Parwekar, 2011). Ele referiu-se à IoT como uma coleção de objetos interoperáveis e identificáveis de maneira única e conectados através da tecnologia RFID (Li et al., 2015). Entretanto, o conceito foi ampliado e atribuído não apenas à coleção de muitos objetos interconectados, mas também à integração de serviços, seres humanos e dispositivos que possam se comunicar e compartilhar diferentes tipos de informação (Mahmoud et al., 2015). Conforme o desenvolvimento de novas pesquisas e tecnologias foram surgindo, outros dispositivos passaram a comunicar-se através da Internet, incorporando inteligência em seu comportamento. Assim, a IoT passou a englobar diferentes tipos de objetos, que vão desde lâmpadas, geladeiras e televisores a maquinário industrial e sensores corporais. Todos os objetos da IoT possuem características como identidade, atributos específicos e interfaces de comunicação, que os integra a uma rede de informações e os define como objetos "inteligentes" (Li et al., 2015). A identificação disponibiliza os dados para reconhecer cada objeto dentro da rede e facilita a troca de informações entre eles. Os atributos específicos oferecem informações sobre os objetos e usuários, o que garante um conhecimento entre os participantes sobre as características de cada um. A interface de comunicação permite a conexão entre os objetos e sistemas, garante a interação entre todos os participantes da rede e disponibiliza conexões personalizadas a todos.

Segundo Lu et al. (2018) na IoT, todos os objetos que se comunicam e disseminam informações são considerados inteligentes. Cada objeto dispõe de sensores, atuadores, microprocessadores, dispositivos de comunicação e fonte de energia. Todas essas propriedades possibilitam a comunicação e cooperação, assegurando a troca de informações entre os participantes presentes na IoT (Vasseur e Dunkels, 2010). Tanto a coleta como a comunicação entre os dispositivos viabiliza o surgimento de serviços personalizados, com tarefas que vão desde simples mensuração de temperatura, tráfego, monitoramento de ambientes e sistemas de vigilância, até os mais complexos como monitoramento de maquinário industrial e gerenciamento de produção industrial. Nessa situação, os dados coletados precisam estar à disposição para serem compreendidos por aplicações que gerenciam diversos serviços (Al-Fuqaha et al., 2015). Esses novos serviços personalizados garantem a integração entre o meio físico e o digital, possibilitando a interconexão de vários domínios de aplicação, criando um ecossistema inteligente que traz melhorias para todas áreas de atuação da IoT.

O desenvolvimento contínuo de dispositivos IoT impõe desafios à sua integração em diversos domínios de aplicação. Esse acontecimento pode ser constatado por diversas pesquisas

realizadas no mercado, evidenciando a importância que a IoT representará nos próximos anos para a evolução de diversas áreas. De acordo com Itforum365 (2018), o crescimento da IoT representa a proliferação de novos dispositivos conectados, o que tem ocorrido pelo aumento de aplicações emergentes e novos modelos de negócios, além da padronização de dispositivos. Segundo Nordrum (2018), estimativas com base em relatórios de empresas como Cisco, IBM e Ericsson, apontam que em 2025 o número de dispositivos IoT pode ultrapassar 50 bilhões. Assim, a IoT pode colaborar para o crescimento em diferentes domínios de aplicação como urbano, rural, militar e industrial (Li et al., 2015). Atualmente, os maiores esforços de pesquisadores encontram-se no domínio urbano, uma vez que apresenta uma variedade de serviços, que juntos formam as chamadas *cidades inteligentes.* Elas são construídas por serviços como mensuração de temperatura, controle de tráfego, vigilância e até serviços de saúde, entre outros. No domínio rural, a implantação de sensores vem proporcionando melhorias no plantio e na colheita, pois é possível mensurar níveis de chuva, desenvolver sistemas de irrigação autônomo, além de automatizar toda a colheita. O domínio militar apresenta melhorias na comunicação, reconhecimento de áreas e identificação de possíveis ameaças (Gubbi et al., 2013).

O domínio industrial tem se destacado entre os demais e ganhando espaço com a chamada quarta Revolução Industrial ou Indústria 4.0. Com os avanços da IoT e outras tecnologias emergentes, a Indústria 4.0 vem desenvolvendo-se em vários campos (Da Xu et al., 2014), tais como monitoramento de produção e gerenciamento da planta industrial, que engloba serviços de controle de temperatura, automação da linha de produção e controle de maquinário monitorado, além da gerência de estoque, que possibilita uma melhor gestão da logística. Segundo Zheng et al. (2018), com o aumento da demanda de produção de manufaturados, tem sido um grande desafio gerenciar todos esses serviços industriais. Portanto, a IoT pode contribuir para melhorias nos processos industriais através de dispositivos inteligentes, coletando e disseminando informações para tomadas de decisões em tempo real (Zheng et al., 2018).

Para que todos os serviços disponíveis na IoT possam ser utilizados, os dispositivos devem possuir tecnologias de comunicação. Normalmente, os dispositivos IoT atuam em ambientes usando baixo consumo de energia, e onde a comunicação apresenta ruídos, perda de enlace e perda de dados (Zheng et al., 2018). Nesse contexto, as tecnologias que viabilizam as comunicações entre os dispositivos são o padrão IEEE (do inglês, *Institute of Eletrical and Eletronics Engineers)* 802.11, conhecido como o WiFi; 802.15.1, o padrão conhecido como *Bluetooth* e criado pela IEEE, atualmente é mantido pelo SIG (do inglês, *Special Interest Group*) e; 802.15.4, que define operações de redes sem fio com baixa taxa; 6LowPAN (do inglês, *Internet Protocol v6 over Low-Power Wireless Personal Area Networks*), que foi desenvolvido pela IETF (do inglês, *Internet Engineering Task Force* é considerado uma evolução do padrão 802.15.4 e tem seu funcionamento sobre o protocolo (IPV6) (do inglês, *Internet Protocol v6*); Zigbee, utilizado para desenvolvimento de redes PAN (do inglês, *Personal Area Network*), também é baseado no padrão 802.15.4; O RPL (do inglês, *Routing Protocol for Low Power and Lossy Networks*), que foi padronizado para IoT; O Identificador por radiofrequência (do inglês, *Radio Frequency identification* - RFID); e a comunicação de campo próximo, (do inglês, *Near field Comunication* - NFC). O uso destas tecnologias na IoT promove o desenvolvimento de serviços nos seus vários domínios de aplicação. Entretanto, elas atuam em diferentes fases da comunicação e, para que haja um maior gerenciamento sobre elas, a literatura utiliza modelos de arquiteturas de três e cinco camadas para melhor organizá-las. Desta forma, a próxima subseção apresenta os principais modelos de arquitetura empregados na IoT.

2.1.1 Arquiteturas para IoT

Ainda não existe uma padronização do modelo de arquitetura para IoT (Lin et al., 2017). A literatura apenas determina quais características ela deve apresentar. São definidas diretrizes sobre o funcionamento de uma arquitetura IoT, tais como ser aberta, baseada em camadas para maximizar a interoperabilidade entre sistemas heterogêneos e recursos distribuídos. Isso permite sua implementação em diferentes contextos. Apesar de ainda não haver um modelo padrão de arquitetura, a literatura disponibiliza diversos modelos utilizando o conceito de camadas. Estes modelos apresentam variações entre três, cinco e até sete camadas, variando conforme os domínios de aplicação na qual a IoT está inserida (Wu et al., 2010; Borgia, 2014; Jun e Chi, 2014; Khan et al., 2012; Bandyopadhyay e Sen, 2011; Yang et al., 2011; Arış et al., 2018).

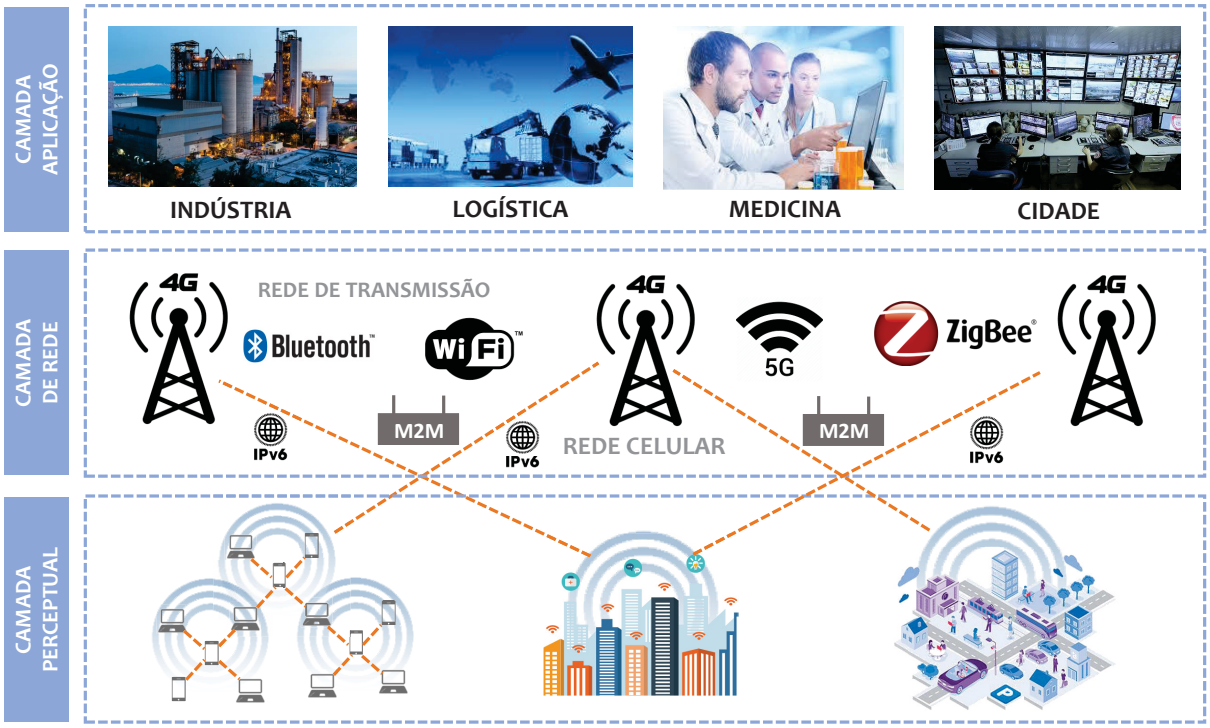


Figura 2.1: Modelo de arquitetura IoT em três camada baseado em (Jun e Chi, 2014)

Existem diferentes propostas para uma arquitetura padrão na IoT, porém a mais considerada é o modelo com três camadas, apresentado na Figura 2.1, que é baseado em (Jun e Chi, 2014). Este modelo é dividido nas camadas perceptual, rede e aplicação. A camada perceptual é representada pelos dispositivos de diversas características, que tem a função de coletar os dados através de sensoriamento e transmitir a informação para a camada de rede. Essa transmissão é realizada através dos dispositivos de acesso, como por exemplo *gateways*, sensores ou entre os próprios dispositivos. A camada de rede é composta por diversas tecnologias de comunicação e redes integradas baseadas no IPV6 (Yang et al., 2011) e no protocolo de roteamento RPL (Kim et al., 2017) com o intuito de garantir a transmissão dos dados entre origem e destino. Por fim, a camada de aplicação é responsável por interpretar os dados para os diferentes domínios tais como cidades inteligentes, indústrias inteligentes, entre outros, ao mesmo tempo que monitora e controla os dispositivos da rede IoT.

A arquitetura da IoT deve prover condições necessárias para realizar a comunicação entre dispositivos em diferentes domínios onde ela está inserida. Desta forma, o funcionamento organizado da IoT propicia que a comunicação ocorra de forma completa, para atender os requisitos

de aplicações como escalabilidade, disponibilidade e interoperabilidade entre dispositivos (Borgia, 2014). A escalabilidade gerencia o crescimento dos dispositivos na IoT, garantindo que eles atendam aos requisitos. A disponibilidade certifica que os dados coletados pelos dispositivos estejam acessíveis às aplicações para uso. Em contrapartida, a interoperabilidade envolve a padronização das diversas tecnologias de forma transparente, certificando a comunicação entre elas. Desta maneira, atender a tais requisitos garante um melhor desenvolvimento entre os dispositivos, possibilitando desenvolver aplicações e serviços cada vez mais confiáveis na IoT.

2.1.2 Redes Densas

A literatura ainda não dispõe de um modelo e conceito específico do que pode ser considerado uma rede densa, seja na quantidade de dispositivos, tamanho da área ou pela área de cobertura que cada dispositivo consegue cobrir. Desta forma, foi feito um levantamento de trabalhos que abordaram o conceito de redes densa, seja no contexto de RSSF (Gielow et al., 2015; Yu e Guan, 2010; Ye et al., 2005) ou redes IoT (Mota et al., 2019; Cervantes et al., 2018; Slabicki et al., 2018). Eles foram sumarizados em na Tabela 2.1.2 e classificados de acordo com o área (**Área(m²)**), número de nós (**Nº/nós**), densidade (**Densidade**), ocupação de nós por metro quadrado (**Ocup.(m²)**), mobilidade (**Mob.**) e raio de transmissão (**Raio(m)**). Como observar-se não existe um consenso sobre quais fatores são importantes para determinar quando uma rede pode ou não ser considerada densa. Fatores como mobilidade, e número de nós por m² tem grande impacto na cobertura da área pelo dispositivos. A densidade tem relação direta com o número de nós e também com a área onde os nós são alocados. Nós buscamos realizar o cálculo entre a área x o número de nós para se chegar em uma densidade, esse cálculo nos deu o valor do número de nós por m². Deve-se ressaltar que o raio de transmissão entre os nós também é um fator importantes a ser considerado na definição de denso, já que ele define qual a proporção cada nós pode cobrir.

Tabela 2.1: Sumarização de modelos de redes densa em RSSF e IoT

Autores	Área(m²)	Nº/nós	Densidade	Ocup.(m²)	Mob.	Raio(m)
Gielow et al. (2015)	302400	54	0,0002	5600	Não	100
Yu e Guan (2010)	1000000	10^3	0,001	1000	Não	50
Ye et al. (2005)	40000	340	0,085	12	Não	10
Mota et al. (2019)	100	20 e 40	0,02 e 0,04	5 e 10	Sim	Não
Cervantes et al. (2018)	40000	50	0,0013	800	Sim	50
Slabicki et al. (2018)	230400	100	0,0004	2304	Sim	Não

Fica claro, que o conceito de rede densa ainda carece ser mais explorado por autores, e abriga um campo a ser explorado, pois cada autor pode definir o que pode ser definido como rede densa em seu contexto. Vale ressaltar que a não existência de um padrão não significa que qualquer modelo rede pode ser considerado denso. Assim, cabe a quem for conceituar o que é denso leve em consideração o seu modelo de rede e quais são suas atribuições em relação à: área, número de dispositivos, área de cobertura dos dispositivos e o raio de transmissão utilizado.

2.1.3 Tecnologias Existentes na IoT

Para que o crescimento da rede IoT seja exponencial e contínuo são necessárias diversas tecnologias interligadas e formando uma grande rede (Khan et al., 2012; Lee e Lee, 2015).

Desta forma, os dispositivos que compõem a IoT variam conforme as tecnologias de cada ambiente onde estão aplicados. Assim, existem diversas tecnologias que mantém as conexões e as comunicações entre os dispositivos. Entre elas, pode-se destacar as redes de sensores sem fio (RSSF), identificador de radiofrequência (RFID) e frequência e comunicação por campo de proximidade (NFC). A partir da popularização dessas tecnologias, a IoT vem ampliando seu escopo de atuação, desenvolvendo novos serviços e provendo inovação à aplicações já consolidadas. Dentre as tecnologias apresentadas, o NFC não faz parte do escopo deste trabalho.

As RSSFs podem compreendem centenas ou milhares de dispositivos (nós) distribuídos em áreas de interesse para sensoriamento (Ko et al., 2010). Os nós são integrados com capacidades de sensoriamento, processamento e armazenamento de dados, transmitidos pelo meio sem fio (Loureiro et al., 2003; Rashid e Rehmani, 2016). Os nós que integram as RSSFs caracterizam-se por trabalhos cooperativos, limitações de recursos como energia, armazenamento e baixa capacidade computacional. Além disso, os nós podem ser organizados por diferentes tipos de topologias (Gonçalves et al., 2012; Rault et al., 2014). Os dispositivos que integram as RSSFs são projetados com bateria, rádio transmissor, processador, memória. Essas redes são usadas em diversas áreas de monitoramento e coleta de informações. Muitas dessas áreas são de difícil acesso e apresentam dificuldades para a chegada de pessoas. As RSSFs podem ser usadas em diversos domínios de aplicação tais como industrial, urbano, ambiental, militar e saúde, entre outros (Ko et al., 2010; Figueiredo et al., 2005). As RSSFs são essenciais para apoiar o desenvolvimento da IoT, pois sua alta capacidade de coletar e disseminar dados beneficia diversos serviços personalizados (Roman et al., 2011; Gonçalves et al., 2014; Melo et al., 2013).

A tecnologia RFID é um grande avanço no paradigma de comunicação incorporada, permitindo o design de microchips para comunicação de dados sem fio. As etiquetas RFID como são chamadas, possibilitam a identificação automática de qualquer tipo de objeto onde sejam empregadas, atuando como uma forma de código de barras eletrônico (Gubbi et al., 2013; Welbourne et al., 2009). O RFID pode ser dividido em etiquetas ativas e etiquetas passivas, conforme a condição de uso. Na forma ativa, as etiquetas contam com sua própria bateria para fornecimento de energia, fazendo com que tenham maior poder processamento e de transmissão, tendo maior autonomia comparada às passivas. Elas estão mais atreladas à aplicações de controle de estoque, gerência de produtos, além de serem usadas em contêineres de transporte. Na forma passiva, as etiquetas apresentam baixo poder de processamento e armazenamento, pois normalmente estão vinculadas a outros equipamentos. As etiquetas RFID passivas podem ser empregadas em diferentes aplicações, tais como gestão de varejo, cadeia de suprimentos, aplicações de controle de acesso, além de transporte, onde pode substituir bilhetes. A adoção da tecnologia RFID em larga escala viabiliza a padronização e organização de diferentes tipos de serviços. Desta forma, ela torna-se um dos pilares ao desenvolvimento de inúmeras aplicações na IoT (Sundmaeker et al., 2010; Sisinni et al., 2018).

2.1.4 Disseminação de Dados

O aperfeiçoamento da computação ubíqua tem proporcionado que diferentes dispositivos se comuniquem em qualquer lugar e a qualquer momento (Ngu et al., 2017). Esse desenvolvimento tem trazido melhorias para os dispositivos IoT, considerando que diversos modelos de serviços necessitam de uma comunicação onipresente entre seus dispositivos. Neste cenário, os dados coletados por diferentes dispositivos, com ou sem restrições de recursos (sensores, termômetros, atuadores, entre outros), devem ser transmitidos para dispositivos com maiores recursos computacionais, para que esses possam processar e disponibilizar tais dados (Sethi e Sarangi, 2017). Esse processo é definido como disseminação de conteúdo e é essencial para avanços em aplicações IoT. A Figura 2.2 ilustra um exemplo de modelo de comunicação para

disseminação de conteúdo entre dispositivos *Smart home*. Em ambientes como *Smart home* a disseminação de dados ocorre de objeto para objeto, dependendo do objeto o usuário tem acesso a esses dados para uma melhor tomada de decisão.

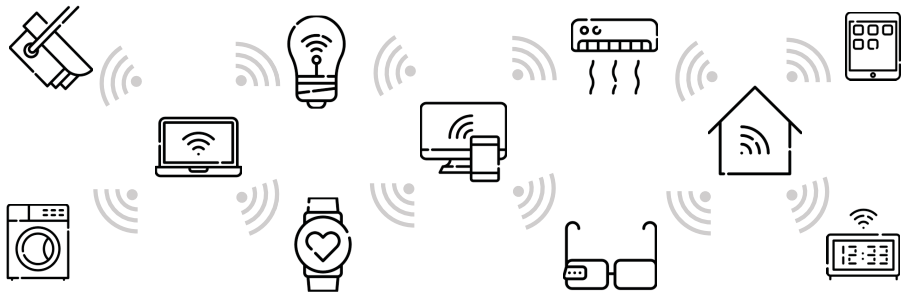


Figura 2.2: Exemplo de disseminação de conteúdo na IoT entre dispositivos *Smart home*

Os ambientes onde a IoT está inserida determinam o tipo e a forma como os dados serão disseminados pelos dispositivos. Esses dados podem ser do tipo textos, áudios, vídeos e imagens (Cai et al., 2017). Quando inserida no contexto industrial ou em rodovias inteligentes, o fluxo de dados trafegado na rede é predominantemente de texto, enquanto os dados trafegados em aplicações como casas ou comércio inteligentes dividem-se entre áudio, vídeo e imagem. Isso ocorre porque nesses ambientes são oferecidos principalmente serviços de *streaming* de vídeo, compartilhamento de áudio e imagens. O contexto urbano apresenta a maior diversidade do fluxo de dados. Nele são oferecidos múltiplos serviços, tais como mensuração de temperatura, gerenciamento de tráfego, serviços de vigilâncias, etc. Isso faz com que o fluxo de dados varie entre texto, áudio, vídeo e imagem. Essa variação do tipo de dados trafegando pela rede oferece desafios aos dispositivos IoT, que devem ser adaptados ao contexto onde estão inseridos.

A classificação destes dados é uma forma de identificá-los de acordo com sua criticidade, importância e periodicidade de coleta (Mendez et al., 2017). Em domínios de aplicação como indústrias, saúde e transporte são gerados grandes fluxos de dados. Assim, a coleta deve ocorrer de modo contínuo e seguro, pois essas informações são de extrema relevância para as aplicações. Em diversos casos, os dados que trafegam na rede IoT são de características sigilosas, críticas e pessoais, como por exemplo informações vitais, dados de processos de produção industriais, informações sobre acidentes em rodovias e informações veiculares (Gubbi et al., 2013). Os dados domésticos e de entretenimento não são de características críticas, nem emergencial. Logo, a coleta pode ocorrer de forma periódica. Portanto, uma disseminação de dados segura deve considerar as características do ambiente, criticidade e o tipo de dado trafegado pela rede. A classificação de dados possibilita o desenvolvimento de serviços cada vez mais personalizados dentro da IoT, além de melhorar aspectos como escalabilidade, disponibilidade e organização da rede para diversas aplicações.

2.1.5 Domínios de Aplicação

A contínua evolução das redes IoT tem proporcionado o surgimento de novos domínios de aplicação. Desta forma, a IoT pode contribuir para melhorias em diferentes aspectos das aplicações, como execução de tarefas, tomada de decisão, gerência de dados e interconectividade entre diferentes áreas (Botta et al., 2016). Esses benefícios são alcançados em diversos domínios como processos industriais, logística, domótica, cidades inteligentes, monitoramento ambiental e vigilância (Silva et al., 2018). Muitas dessas áreas são mantidas por seres humanos e sistemas com tecnologias ultrapassadas, necessitando maior integração. Sendo assim, o uso da IoT viabiliza

novas capacidades em termos de produtos e serviços, que podem ser oferecidos em áreas de interesse de pessoas e serviços. As aplicações em logística, vigilância e processos industriais tem se beneficiado cada vez mais do uso da IoT, através de tecnologias como RSSF, RFID e NFC. A integração entre elas proporciona serviços personalizados e inovadores, tais como monitoramento de ambiente industrial, desde a produção até o oferecimento aos clientes (Lu et al., 2018).

A IoT impõe novos desafios à sua integração e uso nos domínios de aplicação onde está inserida. Segundo Lu et al. (2018) esses desafios variam de acordo com o modo de atuação e os objetivos a serem atingidos pelas aplicações. No domínio industrial, por exemplo, há a dificuldade de integração entre a produção e o gerenciamento de estoque, o que impede uma padronização entre essas áreas. Essa integração possibilita que serviços, como logística, sejam cada vez mais dinâmicos e eficientes, garantindo um fluxo organizado de informações entre diferentes serviços. Em razão disso, a coleta e disseminação de dados deve acontecer de modo seguro, contínuo, escalar e organizado, abastecendo a tomada de decisão das aplicações. No entanto, fatores como mobilidade, escassez de recursos e fluxo de dados têm impacto direto na disponibilidade dos dados coletados e disseminados na IoT. No domínio de cidades inteligentes, os desafios são ainda maiores, pois há uma gama de serviços que podem ser propiciados, tais como mensuração de temperatura, gerenciamento de tráfego, vigilância, controle de poluição, entre outros. A agregação desses serviços torna viável a melhor qualidade de vida para as pessoas. Entretanto, essa variedade de serviços apresenta desafios quanto à sua integração e disponibilização, pois coletar e disseminar esse grande volume de dados gerado exige serviços robustos e seguros, a fim de assegurar as tomadas de decisões pelas aplicações. Abaixo são apresentados os principais domínios de aplicação onde a IoT tem sido empregada e usada para gerir serviços cada vez mais autônomos.

- **Segurança Pública:** Dentro do domínio de segurança pública existe uma diversidade de serviços que podem ser fornecidos através do uso da IoT. Esses serviços podem variar desde vigilância, predição de crimes, até pontos de recepção de crimes. Os serviços de vigilância são oferecidos a partir de câmeras inteligentes operadas via dispositivos IoT. Essas câmeras captam as imagens e as transmitem em tempo real para uma central de inteligência, via Internet, sem a necessidade de cabos e infraestrutura de alto custo (Li et al., 2018). Desta maneira, a expansão e implementação de sistemas de vigilância são facilitados, permitindo uma cobertura mais abrangente e precisa. As predições de crimes podem ser aplicadas a partir do monitoramento inteligente, onde as informações são coletadas em diferentes regiões e agrupadas em centrais, que identificam as probabilidades de acontecimentos de crimes em determinados pontos da cidade. Além disso, serviços como reconhecimento facial, controle de entrada e saída de ambientes, além de dispositivos baseados em biometrias para abertura de portas podem ser oferecidos através da IoT (Borgia, 2014). Logo, o maior avanço da IoT representará o surgimento de serviços cada vez mais aptos a atender as necessidades de segurança.

- **Monitoramento de Ambiente:** Este domínio geralmente está envolvido em serviços como proteção, controle e monitoramento de ambientes, entre outras atividades. Ele pode estar inserido em áreas como agricultura, cidades inteligentes, controle de tráfego e até serviços de reciclagem (Borgia, 2014). Os serviços oferecidos vão da gerência, controle do ambiente e segurança de áreas de interesse. Inicialmente esses serviços eram disponibilizados pelas RSSFs, que coletavam os dados e os disponibilizam através de uma central. Com os avanços da IoT, as aplicações passaram a disponibilizar o serviço de forma organizada, integrada e em tempo real, realizando uma melhor gerência para a disponibilização e a maneira com que os dados são acessados. Essas melhorias podem

ser observadas em diferentes contextos, como por exemplo as cidades inteligentes, que fornecem serviços de controle de poluição, mensuração de temperatura, controle de tráfego e até modernos sistemas de vigilâncias. Essas informações ficam acessíveis para acompanhamento em tempo real, ou seja, toda a classificação e entendimento dos dados são feitos de forma transparente. Os serviços agrícolas também têm se beneficiado do monitoramento inteligente, onde tem surgido aplicações cada vez mais inteligente. Serviços de irrigação, gerência de produção, plantio e colheita são exemplos de aplicações que usam a interconectividade da IoT e prol de melhorias. Graças aos sensores, torna-se possível mensurar as probabilidades de chuva ou condições do terreno para melhor realizar o plantio e a colheita da safra. Além disso, gerenciar desde a produção até a distribuição dos alimentos tornou-se tarefa mais simples, devido ao uso da IoT na coleta e disponibilização dessas informações (Zanella et al., 2014). Desta forma, a utilização de dispositivos inteligentes proporciona um melhor controle sobre os recursos, oferece maior segurança e contribui para melhorias no controle da colheita.

- **Domótica:** A domótica caracteriza-se por ser parte da robótica, onde é definida como parte da integração de mecanismos automáticos em um espaço, visando simplificar as tarefas do cotidiano das pessoas (Luria et al., 2016). Seu objetivo é tornar a vida de pessoas mais confortável, segura e prática em diferentes contextos. Para isso, as tarefas mais rotineiras podem ser automatizadas e realizadas de forma automática sem a necessidade da interação humana. Assim, existe um grande potencial a ser explorado pela IoT nessa área, seja no uso de sensores e equipamentos eletrônico ou na interconectividade deles. A IoT possibilita que o controle de climatização de ambientes seja controlado pelos usuários remotamente, o que permite um nível de conforto. Por sua vez, o controle de energia pode ser gerenciado para adequar-se aos usuários, disponibilizando informações sobre seu consumo, bem como quando o equipamentos devem ser desligados. Na área de segurança é possível desenvolver diversos níveis, desde sistema de monitoramento por câmeras, sensores de presença e serviços de reconhecimento facial (Li et al., 2018). Com a IoT, torna-se possível monitorar sistemas de forma remota e interligá-los. Assim, câmeras podem funcionar como sensores de presença para identificar situações anormais, além de gerar alarmes e gravar. Outra possibilidade é a utilização de etiquetas RFID em produtos, facilitando seu controle, localização e distribuição. Hoje, é comum geladeiras inteligentes que avisam aos donos sobre algum produto que está em falta e no futuro será possível a própria geladeira realizar as compras de acordo com o padrão de consumo das pessoas.

- **Transporte Inteligente:** O domínio de transporte inteligente abrange uma gama de novos serviços, tais como veículos autônomos, gerenciamento tráfego, logística e até o controle de poluição (Khatoun e Zeadally, 2016). A integração desses serviços, quando disponibilizados aos usuários garante uma melhor qualidade de vida. No que tange os veículos autônomos, seu objetivo é integrar um conjunto de tecnologias de sensores, sistemas de controle e atuadores para sensoriar o ambiente, determinar as melhores opções de ação e executá-las de forma mais segura e confiável. Um dos problemas que o gerenciamento de tráfego visa solucionar são os congestionamentos, que impõem custos significativos às atividades econômicas e sociais na maioria das cidades, afetando também a produção de suprimentos e operações *just-in-time* (Gubbi et al., 2013). O serviço de logística se beneficia do monitoramento de rotas para entregas de produtos e suprimentos, o que garante um maior controle sobre a frota de veículos. Neste contexto, a IoT permite a integração e desenvolvimento desses serviços, aprimorando

a comunicação, conectividade e desempenho. A instalação de sensores em rodovias gera informações em tempo real sobre as condições de estradas, ocorrências de chuvas, acidentes e tráfego, entre outras situações que possam ocorrer. Os veículos autônomos usarão essas informações para manter seu posicionamento e sua condição de movimento, o que acarreta em uma melhor fluidez do trânsito em geral. Além disso, os órgãos de fiscalização terão informações sobre as condições de trânsito em tempo real, o que facilita serviços de atendimento de emergências, agilizando o atendimento de acidentes.

- **Saúde Inteligente:** O domínio da saúde é um dos que mais têm se aperfeiçoado com adesão da IoT (Al-Fuqaha et al., 2015). O uso da IoT tem ampliado os tipos de serviços oferecidos a pacientes e profissionais da saúde, garantindo uma análise e tomada de decisões rápida e prática, melhorando a qualidade de vida de todos (Li et al., 2015; Wang et al., 2018). Com a utilização de sensores espalhados pelo corpo, informações como temperatura, pressão arterial, frequência cardíaca e níveis de colesterol serão transmitidas através de tecnologias de comunicação sem fio para os médicos, possibilitando o monitoramento de pacientes em tempo real (Borgia, 2014). A utilização da IoT na saúde possibilita que os dados vitais do paciente, além dos dados pessoais, estejam disponíveis para análise, otimizando o atendimento médico. Em momentos de emergência, dependendo do dispositivo que o paciente carrega junto ao corpo, é possível aplicar injeções de medicamentos de forma remota, agilizando os primeiros socorros. Além disso, o custo dos serviços de saúde pode ser reduzido, considerando que não será necessário uma grande quantidade de profissionais monitorando o estado dos pacientes a cada momento. Outras aplicações relevantes estão relacionadas à identificação de materiais e instrumentos médicos, através do uso do RFID para realizar o inventário hospitalar. Com as etiquetas RFID será possível monitorar e controlar entrada e saída de medicamentos e produtos hospitalares.

- **Indústria Inteligente:** Dentre os domínios de aplicação citados, o industrial tem chamado a atenção devido ao uso intensivo de dispositivos inteligentes em diferentes setores. Neste contexto, a IoT vem se destacando devido ao desenvolvimento das tecnologias como RFID, RSSF e NFC, ampliando a gama de serviços disponibilizados. Esses aspectos ganham maior relevância quando levado em consideração o processo de transformação tecnológica do qual a área industrial vem passando, denominado 4ª Revolução Industrial (Zhong et al., 2017). Tecnologias como *big data*, aprendizado de máquina e inteligência artificial, com a IoT, são essenciais para o desenvolvimento industrial. Toda essa evolução tem promovido melhorias na qualidade da produção, na gerência de estoque, na disponibilização de produtos e, consequentemente, traz maior lucro para os ativos da empresa.

  A IoT aplicada no contexto industrial tende a ser definida como Internet das coisas Industriais (IIoT) (Zhong et al., 2017; Molano et al., 2018). O termo IIoT refere-se aos dispositivos inseridos em um contexto industrial com funções de monitorar, coletar, trocar e analisar informações entre si. Ela conecta máquina, sensores críticos e diferentes partes da indústria de alto risco em áreas como energia, transporte e controle industrial. Esses dispositivos são essenciais para o funcionamento de sistemas e, geralmente, quando falham, resultam em situação de risco e emergência (Zhong et al., 2017). Desta forma, todas as atividades que envolvem a produção industrial, desde o armazenamento, disponibilização e transações financeiras, são beneficiadas pelo uso da IoT. Na linha de produção, a automação de máquinas transformam-nas em inteligentes, o que melhora o seu gerenciamento, possibilitando monitorar o maquinário e identificar com antecedência

quando é necessário trocar peças danificadas ou mesmo prever o tempo de uso. Na planta industrial, os benefícios são variados, indo desde monitoramento de temperatura, gerenciamento de alarmes e sistemas de vigilâncias, além da melhoria no gerenciamento do controle de estoque. Com essa integração, os dados de produção são coletados e processados em tempo real, o que facilita a tomada de decisão de forma rápida e precisa (Zheng et al., 2018).

Além de todos os serviços que podem ser beneficiadas pelo uso IoT dentro das fábricas, a gerência de logística é outra área que tem promovido mudanças e melhorado serviços. Através do uso da IoT, é possível rastrear cargas em tempo real, controlar a frota de maneira autônoma, além de gerenciar o estoque de produtos através de etiquetas RFID. Essas etiquetas são instaladas juntos aos produtos, o que facilita sua localização, controle e distribuição aos estabelecimentos (Sadeghi et al., 2015). Consequentemente, analisar os dados industriais permite que as tomadas de decisão sejam baseadas em informações, o que garante melhores escolhas em virtude de uma visão mais precisa do desempenho da indústria como um todo. Além disso, as alocações de recursos financeiros podem ser melhor avaliadas e determinar quais áreas precisam de um maior investimento (Lee et al., 2014).

2.2 AGRUPAMENTOS DE DISPOSITIVOS

Os agrupamentos de dispositivos em redes de computadores são utilizados para garantir uma melhor dinâmica entre os participantes, além de prolongar a vida útil da rede através da eliminação da redundância, organização do tráfego, economia de energia e uma maior escalabilidade (Pourghebleh e Navimipour, 2017). A eliminação da redundância está atrelada a um ponto centralizado responsável por receber e retransmitir dados. Assim, ele pode verificar prontamente se os dados que estão sendo transmitidos não possuem redundância. A organização do tráfego está diretamente ligada à replicação de dados, pois menos dados iguais trafegando contribui para uma menor taxa de retransmissões de dados e interferências no meio de comunicação, possibilitando um melhor proveito do meio. A economia de energia ocorre através da redução do volume de dados trafegados, ou seja, a maior redução no fluxo de dados representa menores colisões e retransmissões de dados. Como consequência, o uso de energia é otimizado e a rede ganha maior tempo de vida. A escalabilidade está relacionada à quantidade de dispositivos que a rede comporta, ou seja, o quanto a rede pode crescer sem perder as características acima citadas, além de melhorar a dinâmica da rede em relação a entrada e saída de dispositivos da rede. Essa participação pode ocorrer de forma dinâmica, manter a rede funcionando e garantindo que suas características não sejam afetadas torna-se um desafio (Talyansky e Tumarkin, 2018).

2.2.1 Agrupamentos Dinâmicos

Os agrupamentos de dispositivos podem ser formados com base em critérios, sejam pela dinamicidade dos dados ou por sua similaridade (Gielow et al., 2015). Assim, a dinamicidade dos agrupamentos está ligada diretamente aos participantes que são considerados para formá-los (Sanchez et al., 2014; Rossetti e Cazabet, 2018a). Os dispositivos tendem a apresentar atributos de diferentes formas, sejam por aspectos ligados à mobilidade, coleta de dados, restrições energéticas ou por falhas, fazendo com que os agrupamentos sofram com esses aspectos. A mobilidade indica que os agrupamentos devem ser formados levando em consideração que a entrada e saída de dispositivos será frequente, fazendo com que a rede se reconfigure de forma rápida e dinâmica para atender a este requisito. A coleta de dados pode ser dinâmica na forma de

como os dados são coletados pelos nós participantes da rede, podendo interferir na formação dos agrupamentos, tendo em vista que os dispositivos na mesma região tendem a apresentar dados similares ou não, indicando quando um nó deve deixar o agrupamento ou quando deve ser acrescentado a ele (Gielow et al., 2015).

As restrições energéticas fazem com que a vida útil da rede seja afetada. Por isso, agrupar dispositivos faz com que a rede prolongue seu tempo de vida, pois colabora com sua organização e consequentemente ajuda a manter a rede funcionando. (Li e Znati, 2007) Entretanto, quando os dispositivos com pouca energia começam a deixar os agrupamentos, eles precisam ser reconfigurados, o que pode apresentar uma maior dificuldades na formação dos agrupamentos. Devido à sua natureza, os dispositivos podem apresentar falhas, sejam elas causadas por mal funcionamento ou mesmo causadas por terceiras. Essas falhas afetam diretamente a formação dos agrupamentos, pois quando um dispositivo falha, os agrupamentos precisam lidar com esse problema (Saeed et al., 2018). Todos esses fatores tornam a formação dos agrupamentos dinâmicos um desafio a ser superado. A Figura 2.3 ilustra como agrupamentos dinâmicos podem ser formados ao longo do tempo. Cada instante ***T*** representa uma formação diferente dos agrupamentos: os nós mantém suas posições, o que varia são as interações entre eles.

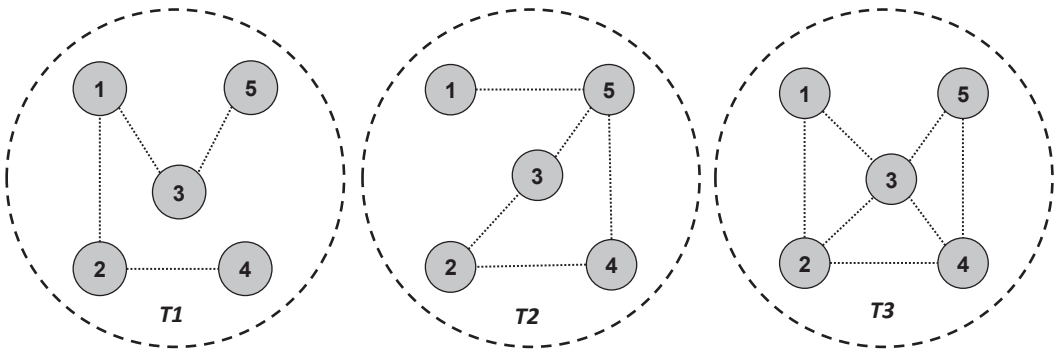


Figura 2.3: Exemplo de formação dos agrupamentos ao longo do tempo

Existem diversos fatores que podem impactar diretamente na formação de agrupamentos, sejam eles de disponibilidade, como o meio de comunicação, ligados à segurança ou mesmo à topologia da rede. O meio de comunicação sem fio está sujeito a interferências e colisões, fazendo com que os dispositivos por vezes não recebam mensagens devido à má condições temporárias. Nesse contexto, a dimensão temporal carrega uma informação de grande importância para a análise do processo de formação desses agrupamentos (Rossetti e Cazabet, 2018b). As questões de segurança estão relacionadas a usuários maliciosos, que agem para degradar a formação de agrupamentos, seja sobrecarregando o sistema, alterando ou descartando pacotes, ou mesmo interferindo na comunicação entre os usuários. A influência das topologias de redes está relacionada as grandezas como espaço e tempo, pois podem definir tamanhos e duração da formação dos agrupamentos e também atuar de forma dinâmica na rotas da rede, definindo como cada participante dissemina seus dados. Desta forma, a formação de agrupamentos deve considerar esses fatores de maneira a ser adaptativa e reconfigurável para atender a todos os requisitos da rede e dos dispositivos nela inseridos.

2.2.2 Protocolo DDFC para agrupamentos dinâmicos

Os agrupamentos tendem a ser dinâmicos em diferentes características, sejam elas relacionadas aos dispositivos ou o tipo de rede onde eles atuam. Dessa forma, a literatura tem

apresentados ao longo dos anos diversos trabalhos que abordam as relações dinâmicas entre dispositivos em RSSF. Entretanto poucos trabalhos buscam trabalhar a relação dinâmica com base na similaridade. Assim, os autores Gielow et al. (2015) exploraram as relações de similaridades de leituras desenvolvendo um protocolo DDFC (do inglês, *Dynamic Data-aware Firefly-based Clustering*), bio-inspirado no comportamento dos vaga-lumes que busca manter agrupados os nós que apresentem seus valores de leitura similar. Para isso cada nó envia uma mensagem beacon informando sua leitura e as leituras dos seus vizinhos. No trabalho para validar o protocolo, são usadas leituras de umidade e temperatura. Entretanto a ideia é que o DDFC possa ser configurado para ser usado com diferentes grandezas. Para formação dos agrupamentos lógicos o DDFC mantém duas estruturas locais de armazenamento em cada nó, sendo um dos vizinhos fisicamente próximos e outra dos vizinhos que satisfazem o limiar de similaridade. Este sistema visa determinar quando um agrupamento deve ser formado ou quando deve ser fragmentado. Depois de formados os agrupamentos, o DDFC define os líderes dos agrupamentos e os índices de roteamento interno e determina quais rotas os nós comuns devem seguir para alcançar o líder de cada agrupamento. Devido à grande densidade de nós presente na rede, cada agrupamento pode conter mais de um líder. Desta forma, para se atingir um líder, a mensagem pode utilizar mais de um salto. Os líderes têm duas funções principais, a comunicação entre agrupamentos e o roteamento dos dados até a Estação Base. A Figura 2.4 apresenta as estruturas de hierarquias formadas pelo DDFC juntos aos dispositivos.

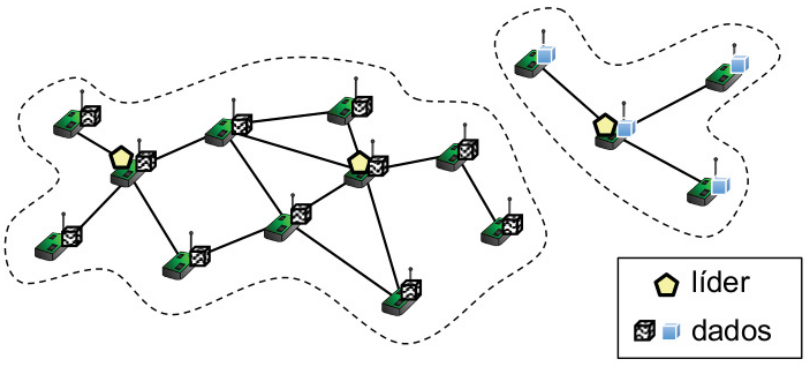


Figura 2.4: Estrutura hierárquica estabelecida pelo protocolo DDFC

Cada nó mantém duas estruturas principais da rede armazenada, uma com os vizinhos espaciais e outros com vizinhos que respeitam o limiar de similaridade. Para conseguir manter essas duas estruturas são necessárias informações de leitura de todos os vizinhos espaciais. Essas informações envolvem a leitura individual de cada nó vizinho, a leitura agregada da vizinhança do nó, além de quantidade leituras que foram agregadas. Com essas informações mantidas atualizadas, os nós são capazes de saber de tempos em tempos quando podem ou não fazer parte de um agrupamento.

No início, cada nó faz parte de um agrupamento. Conforme as interações vão acontecendo, o nó pode se manter no agrupamento ou muda-se para outro. Os agrupamentos podem ser fundidos ou mesmo fragmentados, tudo conforme os limiares de similaridades definidos. O limiar de similaridade é quem garante a formação dos agrupamentos, ele é responsável por definir quais nós são similares em leituras e quais nós apresentam leituras discrepantes comparadas aos seus vizinhos. Cada nó envia periodicamente uma mensagem *Beacon* em *Broadcast*, análoga ao piscar de um vaga-lume. Na mensagem *Beacon* o nó envia seu identificador único dentro da rede, sua leitura atual, a média de leitura agregadas e quantidade de leituras agregadas de sua vizinhança. Essas informações podem ser enviadas conforme a aplicação a ser beneficiada, ou

seja, o tempo do intervalo pode variar de aplicação para aplicação. Com a média sincronizada, as relações de similaridades são formadas juntamente com os agrupamentos.

Ao receber uma mensagem *Beacon*, o nó é capaz de saber, sua origem, a leitura individual, leitura agregada e quantidade de nós considerados na agregação. Através dessas informações as duas estruturas principais são atualizadas independentemente da relação de similaridade entre os nós. A agregação média das leituras onde o nó se encontra é considerada para definir se as leituras do nó de origem satisfazem o limiar de similaridade ou se não. Se respeitarem o limiar, eles podem fazer parte do mesmo agrupamento, caso contrário são considerados apenas vizinhos espaciais. Ao mesmo tempo que são formados os agrupamentos, a eleição dos líderes também é definida. Para isso, o DDFC utiliza a relação criada na formação dos agrupamentos, sendo o número de vizinhos como principal parâmetro para eleição. A eleição dos líderes considera as regras propostas por KHOPCA (Brust et al., 2008). Esse conjunto de regras foi escolhido devido sua flexibilização. Cada nó atualiza sua pontuação auto atribuída com base na pontuação de seus vizinhos de agrupamento. Assim, com as pontuações definida os nós a utilizam para determinar o número de saltos e rotas até os líderes. O processo de eleição de líderes é dinâmico, igualmente ao processo de agrupamento, ou seja, conforme as variações dos agrupamentos a escolha da liderança também varia.

2.3 PRINCÍPIOS DE SEGURANÇA PARA REDES IOT

O crescimento do uso de tecnologias de transmissão sem fio em redes como forma de comunicação entre dispositivos computacionais traz diversos desafios, especialmente para a garantia de segurança dos dispositivos. Isso ocorre pelo fato de que as informações que trafegam estarem mais expostas à receptores que estejam próximos de algum dispositivo (Atzori et al., 2010). Diferentemente do uso de conexões cabeadas que empregam uma maior segurança às informações da rede, pois elas não ficam expostas ao acesso não autorizado. A IoT utiliza a comunicação sem fio entre os dispositivos, desta forma, herda seus desafios pois são baseados no uso do padrão IEEE 802.11. Porém, por contar com dispositivos com recursos limitados computacionalmente, a segurança para a IoT apresenta desafios ainda maiores (Li et al., 2015). As questões associadas à segurança das redes IoT são fundamentais para o seu avanço como internet do futuro. Ela deve atender a temas como autenticidade, integridade e confidencialidade dos dados. Logo, contramedidas tradicionais não podem ser aplicadas diretamente em ambientes IoT, pois a diversidade de padrões de comunicação e tipo dos dispositivos influenciam na segurança (Li et al., 2015). Outro problema característico de IoT está na escalabilidade das soluções, uma vez que o alto número de dispositivos conectados demanda uma infraestrutura flexível para lidar com as ameaças de segurança em ambientes dinâmicos.

Segundo Sicari et al. (2015) a segurança deve ser construída através de atributos de confidencialidade, integridade e disponibilidade, que visam manter as informações livres de diferentes ameaças. A confidencialidade garante o acesso aos dados apenas quem têm direito ao acesso. A integridade garante que os dados coletados não sofram alterações entre a origem e o destino. Por fim, a disponibilidade representa a garantia de acesso aos dados a qualquer momento. Esses três atributos tem como finalidade garantir a segurança dos dados transmitidos na rede, provendo maior robustez e proteção para o ambiente (Avizienis et al., 2004). A falta de um desses atributos ou seu uso parcial cria vulnerabilidades na segurança dos dispositivos ou em serviços como um todo (Bennaceur et al., 2018). Essas vulnerabilidades, quando explorados por usuários maliciosos, podem causar anomalias, afetando diversos serviços providos pela IoT.

Embora existam diversas pesquisas na área de comunicação e infraestrutura, atualmente, o principal foco das pesquisas na IoT está voltando para área de segurança, sejam em soluções

para evitar vulnerabilidades, seja no desenvolvimento de sistemas de proteção ou detecção de ameaças a segurança. A segurança é o principal foco de pesquisa na IoT, especialmente pelo fato dos dados que são manipulados pelas aplicações serem confidenciais, ou seja, que necessitam de sigilo e proteção Adat e Gupta (2018). Por isso, é importante que esses dados fiquem livres de ameaças que visam interceptar, alterar ou mesmo falsificá-los (Bertino e Kantarcioglu, 2017). Consequentemente, a ascensão de atributos de segurança, autenticidade, confidencialidade e integridade, garante maior robustez e torna-se chave para a consolidação da IoT em diferentes domínios de aplicação.

2.4 AMEAÇAS NA IOT

No contexto geral, redes e seus dispositivos estão sujeitos a diferentes tipos de ameaças. Elas podem ser resultantes do mau funcionamento de dispositivos ou da rede, falta de energia, entre outros. No entanto, algumas dessas falhas podem ser causadas por usuários mal intencionados, que aproveitam vulnerabilidades deixadas por dispositivos e pela rede. Assim, eles passam a explorá-las de forma a tirar proveito, lançando ataques que buscam deteriorar a rede, afetando continuamente seu desempenho (Zarpelão et al., 2017). No contexto de redes IoT, existem diversos tipos de ataques que ameaçam a segurança das redes, sejam criando brechas ou mesmo aproveitando-as. Os ataques mais comuns na IoT são *Sybil, Black Hole, Sinkhole, Selective Forward, DDoS, On OFF* (Cervantes et al., 2015; Evangelista et al., 2016; Macedo et al., 2016; Zarpelão et al., 2017) e o ataque de *injeção de dados falsos* (Yang et al., 2017; Pedroso et al., 2019). Dentre esses ataques citados, destaca-se o ataque de injeção de dados falsos (IDF), que compromete a integridade (Hug e Giampapa, 2012), autenticidade e disponibilidade dos dados sensoriados pelos dispositivos e utilizados pelas aplicações.

O ataque IDF caracteriza-se pela manipulação ou alteração de dados, sistemas de alerta e inserção de *bugs* com o objetivo de enganar, deteriorar e sobrecarregar redes ou sistemas de coleta de dados (Hug e Giampapa, 2012; Deng et al., 2016). Os usuários maliciosos podem realizar o ataque IDF a partir da exploração de vulnerabilidades encontradas na rede, que podem ser ocasionadas por outros tipos de ataques. Além disso, o atacante pode interceptar pacotes e capturar dispositivos na rede aproveitando-se de falhas decorrentes do mau funcionamento (Yaqoob et al., 2017). Desta forma, a ocorrência de ataques IDF em sistemas presentes na IoT afeta atributos como integridade, disponibilidade, autenticidade dos dados disseminados pela rede (Potluri et al., 2017). Normalmente, os dispositivos estão autenticados na rede e exercem suas funções padrão de coleta e disseminação de dados quando podem ser capturados por atacantes (Yang et al., 2017). Este comportamento imprevisível dificulta a identificação do ataque aumentando o tempo de deterioração da rede. O ataque IDF é considerado relativamente novo na literatura, tendo seus primeiros registros no ano de 2004 (Ye et al., 2005) quando seu impacto foi estudado em RSSF. Em 2009, ele passou a ser analisado no contexto de *smart grids* (Deng et al., 2016; Liu et al., 2011). Em redes IoT, os primeiros trabalhos são datados do ano de 2017 (Yang et al., 2017), ou seja, ainda existem muito a ser estudos sobre o ataque IDF e como ele pode atuar em redes orientadas a dados como a IoT

Destaca-se a maneira como ocorre o ataque na rede, pois não existe um padrão para o seu acontecimento. Segundo Ye et al. (2005) o comprometimento de um dispositivo se dá quando um atacante obtém o controle dele na rede após sua implantação. Uma vez no controle desse dispositivo, o atacante está dentro da rede, podendo fazer com que esse dispositivo insira dados maliciosos, altere dados de coletas, ou mesmo provoque outros tipos de ataques. O ataque IDF pode ser efetivado de quatro formas, como pode ser observado na Figura 2.5. No ataque **A**, o dispositivo é capturado pelo atacante e manipulado para injetar informação falsa. No ataque **B**, o

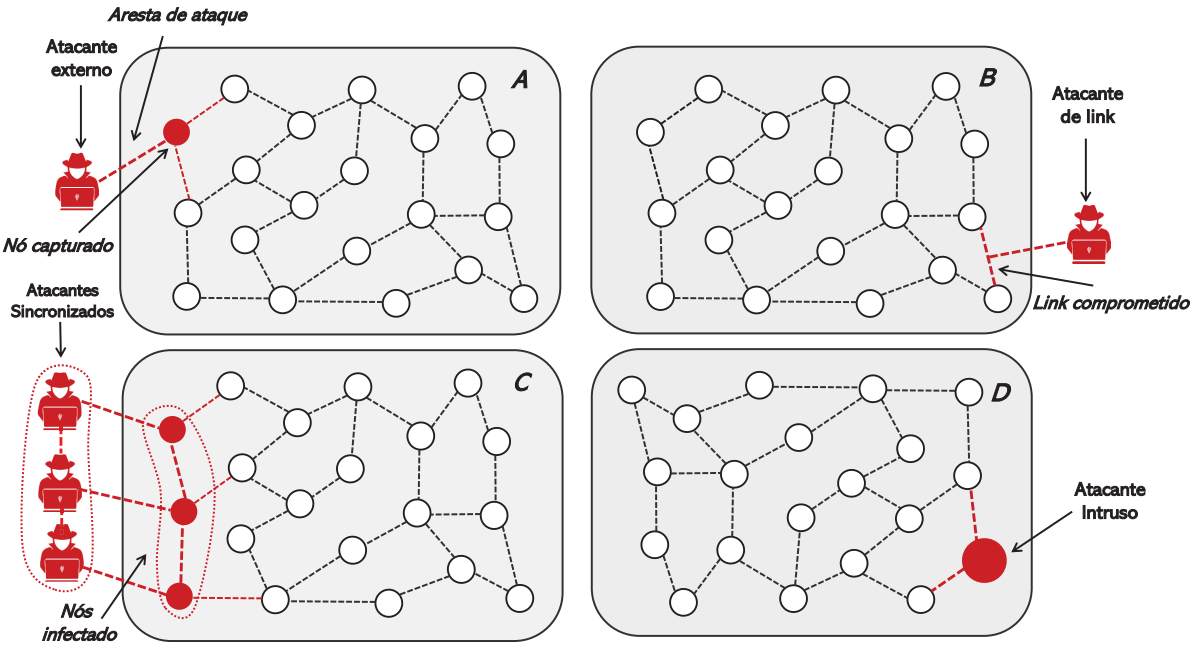


Figura 2.5: Os tipos de comportamentos do ataque IDF em geral

atacante intercepta os pacotes pelo canal de transmissão e manipula os dados antes de chegaram à origem. No ataque **C**, o ataque ocorre de forma sincronizada por mais de um atacante, fazendo com que os dispositivos capturado lancem ataques simultaneamente. No ataque **D**, o próprio dispositivo manipula as informações e as injeta na rede. Independentemente da forma como o ataque é lançando, ele pode dificultar o funcionamento da rede em diferentes níveis, fazendo com que ela venha a apresentar problemas relacionados ao seu desempenho. O ataque IDF pode muitas vezes ser iniciado após outro ataque, como o ataque de mascaramento, personificação ou mesmo o *Sybil*. Devido à sua grande participação em aplicações que utilizam dados para tomada de decisão, o ataque IDF vem ganhando cada vez mais atenção de pesquisadores. Aplicações como as industriais e cidades inteligentes, que utilizam a informação como forma de gerenciamento de funções, são as maiores vítimas do ataque (Sikder et al., 2018).

2.4.1 Ataque IDF na disseminação de dados

A disseminação de dados, como qualquer serviço dentro da IoT, também está sujeita a falhas e ataques entre eles o IDF, que tem como característica a manipulação de dados. Quando um ataque IDF é direcionado contra a disseminação de dados, ele afeta propriedades como integridade, confiabilidade e autenticidade dos conteúdos gerados, o que pode acarretar diversos problemas para a rede, considerando que o propósito dos dispositivos da IoT é coletar e transmitir dados livremente. Em aplicações orientadas a dados, a disponibilização de informações é essencial para tomada de decisão. Desta forma, quando dados disseminados sofrem qualquer tipo de problema, informações inconsistentes levam o sistema a tomar decisões equivocadas, gerando problemas para diferentes serviços. Um exemplo são os sistemas de alerta baseados em desvio de informações. Quando existem alterações causadas por anomalias, diversos alertas falsos são acionados causando uma pane em todo o sistema (Da Cunha et al., 2016). Em indústrias, máquinas são monitoradas em tempo real. Quando um dado é disseminado mas não representa o estado atual da máquina, pode representar inconsistência no sistema, mesmo a máquina estando

em perfeitas condições. Por essa razão, assegurar que a disseminação de dados aconteça sem interferências que a prejudique garante serviços mais eficientes.

Especialmente em redes IoT orientada a dados, proteger o serviço de disseminação representa manter o fluxo de dados sempre disponível para aplicações. Com esse propósito, os autores em (Potluri et al., 2017) avaliaram o impacto de um ataque IDF na disseminação de dados em um sistema de controle industrial e apresentaram os principais riscos que o ataque pode oferecer. O sistema analisado baseia-se em dados de tempo real e utiliza o serviço de disseminação para gerenciar as informações transmitidas. Assim, os autores propuseram uma abordagem apoiada em uma rede neural para identificar o ataque IDF, usando o rastreamento do dados coletados para saber a origem e destino dos dados transmitidos. Assim, desenvolveu-se um aprendizado supervisionado para treinar a rede neural, o que inclui um algoritmo de propagação para avaliar as possibilidade de anomalias presentes na rede. Para simular o ataque, foi desenvolvida uma ferramenta para injeção de dados falsos e usado indícios do ataque para treinar a rede neural a identificá-los. O ambiente foi emulado no simulador V-REP (do inglês, *Virtual Robotic Experimentation Platform*), buscando representar um sistema de controle industrial real.

Os resultados obtidos no trabalho evidenciam a eficiência do mecanismo proposto para detecção do ataque IDF. Entretanto, deve-se ressaltar que a avaliação por eles executada ainda se encontra em estágio inicial como eles mesmo destacam. Todavia, a não mitigação correta do ataque gera maiores impactos à rede como mau funcionamento, sobrecarga e deterioração dos serviços de disseminação e coleta de dados. Desta forma, fica evidente a necessidade de avaliações futuras pelos autores. É importante também que se conheça o tipo de ataque, o que facilita uma melhor taxa de detecção. Porém, a necessidade de desenvolver-se contramedidas capazes de prover segurança e proteção a rede, garantem que serviços como a disseminação de dados ocorra livre de ameaças, inclusive o ataque IDF é fundamental para o desenvolvimento de aplicações em diversas áreas além da industrial.

2.4.2 Ataque IDF em agrupamentos de dados

O serviço de agrupamentos de dados promove diversas melhorias em áreas onde é empregado, e na IoT não é diferente (Munir et al., 2017). Ele tende a deixar a rede mais organizada e fluída para quem a utiliza, já que melhora questões como topologia, comunicação e consumo de recursos. Por estas razões, o serviço de agrupamento passar a ser de extrema importância em redes orientadas a dados, pois o fluxo de dados gerados por elas demanda recursos que muitas vezes são escasso entre os dispositivos. Os agrupamentos podem ser formados levando em consideração diversas características de dispositivos, rede ou dados, o que influencia na forma como são gerenciados. Pensando nesses fatores, usar o serviço de agrupamento torna viável o uso da IoT em diferentes contextos de aplicações. Entretanto, como qualquer serviço em rede, ele está sujeito a ataques que buscam explorar vulnerabilidades, levando o serviço a interromper o seu funcionamento ou operar de forma incorreta. Dentre as ameaças, destaca-se o ataque IDF, que pode manipular informações e assim influenciar diretamente na formação dos agrupamentos.

Particularmente, assegurar a disponibilidade do serviço de agrupamento em um contexto IoT permite que as aplicações que dependem do serviço mantenham-se atualizadas e operantes. Isso porque redes orientadas a dados fazem uso de um grande fluxo de dados, e gerenciá-los pode sobrecarregar o sistema como um todo. Assim, o funcionamento do serviço de agrupamento garante fluidez, organização e disponibilidade da rede (Gaona-García et al., 2017). Desta forma, ataques como o IDF mostram-se prejudiciais ao serviço de agrupamentos de dados, pois o seu objetivo é deteriorar a rede e impedir a disponibilização desses dados. O sucesso do ataque IDF está atrelado ao lançamento arbitrário, o que dificulta a detecção de anomalias pelo serviço e aumenta o tempo de mau funcionamento da rede, tornando indisponível o acesso dos dados

pelas aplicações. Assim, preservar a segurança da rede, garante que os serviços como o de agrupamento atue com sucesso em diversas aplicações orientadas a dados. A Figura 2.6 ilustra como a ação do ataque IDF em três fases e como ele prejudica a formação dos agrupamentos. Na primeira fase o atacante captura o nó antes da formação do agrupamentos. Na segunda fase o nó capturado não consegue fazer participar do processo de formação dos agrupamentos. Na terceira fase o nó é isolado dos demais impossibilitado de formar o agrupamento e disseminar seus dados.

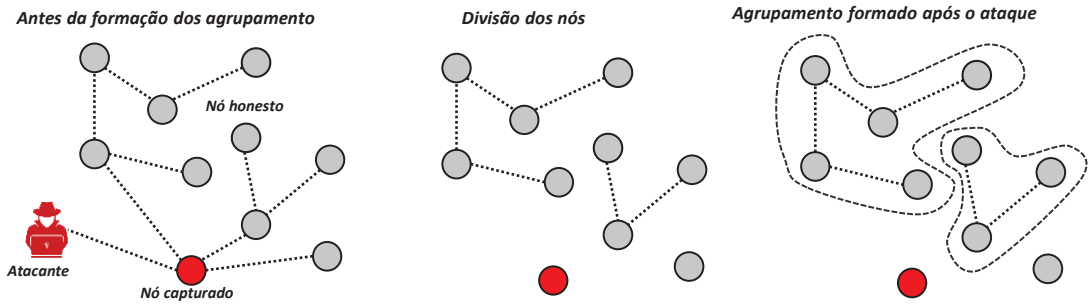


Figura 2.6: Comportamento do ataque IDF em agrupamentos

O desenvolvimento de aplicações em diferentes contextos está relacionado em como as informações trafegadas pela rede são entendidas. Porém, lidar com um grande volume de dados gerados por essas aplicações necessita de serviços capazes de disponibilizar esses dados de forma organizada e transparente. O serviço de agrupamento surge com alternativa para suprir essa necessidade, já que pode organizar a rede, melhorar o fluxo de transmissões, melhorar as retransmissões e lidar com o grande volume de dados gerados. Contudo, como qualquer serviço presente na IoT, o de agrupamento está exposto à diferentes ameaças, que visam prejudicar o sistema. Assim, permitir que os dados sejam disponibilizados sem qualquer tipo de alterações torna-se um desafio para redes vulneráveis como a IoT (Alaba et al., 2017).

2.5 TÉCNICAS DE MITIGAÇÃO

A literatura apresenta uma diversidade de técnicas para mitigação de ataques em redes, que dão suporte a sistemas e auxiliam na contenção de diversas ameaças. Para escolher uma técnica que seja adequada, alguns fatores devem ser levados em consideração, tais como o modelo de rede, a densidade dos dispositivos, a mobilidade, entre outros (Mannes et al., 2012a,b). No entanto, considerar as vantagens e desvantagens é fundamental na adequação do que cada técnica pode oferecer. Dentre as técnica que já foram empregadas na mitigação do ataque IDF, duas têm maior destaque: a Filtragem em Rota (do inglês, *En-Router Filtering*) e a Baseada em Agrupamentos. Ambas foram implementadas no ambiente de RSSFs e apresentam vantagens e desvantagens quando aplicadas para redes IoT. Também se considera a utilização de diferentes abordagens na mitigação do problema, como a utilização da técnica de Consenso e *Watchdog*, muito utilizada na detecção de ataques. Porém, até o presente momento, ainda não foram aplicadas na mitigação do ataque IDF. Além disso, existem os Sistemas de Detecção de Intrusão (IDS) que são empregados em diferentes contextos de rede, sendo alternativas a diversos tipo de ataques e auxiliando sistemas de prevenção a entender os tipos de anomalias encontradas.

2.5.1 Filtragem em rota

A filtragem em rota compreende inúmeros recursos que visam melhorar a segurança em diferentes tipos de rede (Kumar e Pais, 2017). Ela atua na classificação de dados, evitando

que dados comprometidos atinjam o destino final. A filtragem pode ser aplicada de duas formas: na rota entre os nós, antes de chegar no agregador de dados, ou seja, os dados não condizentes com os demais devem ser descartados antes de serem agregados e disponibilizados; na segunda forma, a filtragem ocorre após a agregação dos dados, quando é realizada pela central de controle, onde são verificados os dados. Caso não estejam de acordo, são descartados. O uso de uma central para filtragem acarreta problemas para rede, pois representa o ponto único de falhas, ou seja, caso a central apresente qualquer tipo de problema a rede pode vir a parar de funcionar. Ambas as formas apresentam um alto grau de detecção, visto que todos os dispositivos na rota de entrega podem verificar a integridade e autenticidade dos dados. Em contrapartida, o custo computacional utilizado na filtragem de pacotes tende a sobrecarregar a rede. Outra desvantagem está em apenas identificar os dados falsos, mantendo os dispositivos maliciosos, acarretando na continuidade do envio de dados falsos (Lin et al., 2011). Outras formas de filtragem em rota visam a criação de trajetórias de alternativas, fazendo com que os dados falsos não sejam encaminhados (Yu e Guan, 2010). Esse tipo de filtragem que apenas descarta ou desvia os dados falsos não garante que os dispositivos maliciosos sejam detectados pela rede. Por isso, outro fator deve ser levado em consideração quando a utilização da filtragem em rota, a mobilidade. A mobilidade dificulta a criação de filtram em rota, pois as rotas torna-se dinâmicas em relação a posição dos nós, ponto de verificação e autenticação.

2.5.2 Técnica baseada em agrupamentos

A detecção baseada em agrupamento caracteriza-se por ser dividida em duas categorias, quando a detecção acontece antes da formação dos agrupamentos e quando a detecção acontece depois de formados os agrupamentos. Assim, deve-se levar em consideração o tipo de detecção que se deseja realizar. Na primeira categoria é feita uma filtragem de dispositivos baseada na interação e recomendações entre eles. Logo após esse processo, apenas os dispositivos autenticados e honestos podem fazer parte do agrupamento (Zhu et al., 2015). O problema deste modelo está relacionado aos dispositivos maliciosos que conseguem enganar o processo de autenticação e participar do agrupamento, se passando por dispositivos honestos. Como o processo de filtragem acontece antes da formação de agrupamentos, o atacante será identificado apenas em uma nova rodada de formação. Desta forma, ele pode continuar a disseminar informações falsas. Na segunda categoria, a detecção de anomalias acontece após a formação dos agrupamentos e fica a cargo de um nó líder identificar os dispositivos maliciosos, através da interação que ocorre entre eles. Entretanto, existem ressalvas quanto ao seu uso, pois caso o nó líder seja comprometido, a identificação como atacante tornar-se-á mais complexa, pois será necessária uma entidade externa para identificar a ameaça. Logo, devem ser levadas em consideração questões energéticas, densidade da rede e a mobilidade ao empregar técnicas de agrupamentos como forma de contramedida a ataques em redes IoT (Rault et al., 2014).

2.5.3 Sistemas de detecção de intrusão

Os sistemas de detecção de intrusão (IDS) são soluções abrangentes, que muitas vezes comportam diferentes recursos e visam melhorar a segurança de sistemas computacionais ou redes de computadores na presença de ameaças (Zarpelão et al., 2017). Os IDS atuam como uma segunda camada de defesa e geralmente lidam com ameaças internas, que conseguem burlar a primeira camada de prevenção de anomalias. Assim, os IDS são responsáveis por detectar e monitorar eventos em busca de anomalias dentre diferentes tipos de sistemas. A intrusão em um sistemas caracteriza-se pela tentativa de um usuário malicioso burlar o sistema na tentativa de comprometer a confiabilidade, integridade e disponibilidade. O principal objetivo ao desenvolver

um IDS está no fato de não ser possível criar sistemas ou manter a rede totalmente segura. Com o desenvolvimento da IoT e diversas aplicações, cada vez mais se torna necessário lidar com questões de segurança. Desta forma, a identificação de ameaças garante a disponibilidade na comunicação e no acesso às aplicações.

Conforme Hodo et al. (2016) os IDSs podem ser divididos em duas categorias, baseada em máquina *(host)* e baseada em rede. Os IDSs baseado em *host* são sistemas que monitoram, detectam e respondem às atividades de ataques em determinado *host*. A tomada de decisão é influenciada por informações coletadas em pontos específicos. Entretanto, uma abordagem com essas característica é inviável em redes com recursos limitados, devido à sua característica distribuída, que necessita vários *hosts*. Os IDSs baseados em redes são aqueles que utilizam uma máquina ou um software monitorando pacotes em tempo real em busca de possíveis anomalias. Normalmente eles são configurados em pontos específicos da rede, onde é possível gerenciar todo o tráfego. O uso de IDSs proporciona a obtenção de informações como: *(i)* identificação do intruso; *(ii)* localização do intruso; *(iii)* o tempo de intrusão; *(iv)* tipo de intrusão e a *(v)* origem da intrusão. Essas informações são aplicadas na mitigação e correção de ataques em diferentes tipos de sistemas (Zarpelão et al., 2017). Além disso, os IDSs podem operar em modo autônomo ou em modo cooperativo. No IDSs autônomos cada nó funciona como detector de atividades maliciosas, enquanto nos IDSs cooperativos, a detecção é baseada em agrupamentos, onde cada nó monitora seu vizinho e quando são detectadas as atividades maliciosas, o líder do agrupamento é informado (Hodo et al., 2016).

Os IDSs podem atuar de três formas diferentes na detecção de anomalias: a partir de assinaturas, anomalias e híbrida (Bhuyan et al., 2013). A detecção por assinatura utiliza regras pré-estabelecidas para criar um conjunto de ações. Tem como objetivo comparar as informações monitoradas com as regras estabelecidas em busca de possíveis anomalias. Seu uso é adequado em ataques conhecidos, porém não consegue detectar novos tipos de ataques. A detecção por anomalias utiliza o princípio de que um ataque gera um comportamento anômalos aos demais nós da rede. Assim, esse IDS age como um classificador. Ele monitora as atividades classificando-as com base no comportamento normal ou anômalo. Um IDS baseado em anomalias é ideal para detecção de ameaças desconhecidas, mas, pode gerar altas taxas de falsos positivos e falsos negativos, devido ao seu pouco conhecimentos sobre a rede. O IDS híbrido destaca-se por utilizar as duas formas citadas, isto é, é composto por dois módulos, um responsável pela detecção de ataques conhecidos a partir das regras pré-estabelecidas, e outro, responsável pela detecção de anomalias e monitoramento do comportamento da rede. Os IDSs híbridos são mais precisos e robustos na detecção de ataques, geram menor número de falsos positivos e falsos negativos. Entretanto, ele consome mais recursos de rede (Alrajeh et al., 2013).

2.5.4 A abordagem de consenso

O consenso é descrito como um conceito que visa produzir um acordo por consentimento entre os membros de um determinado grupo ou entre vários grupos. Em sistemas computacionais ou redes de computadores, o consenso é peça chave para sistemas distribuídos, que visa a tomada de decisão em grupo (Herrera-Viedma et al., 2014; Palomares et al., 2014). Ele pode ser classificado em três categorias: **global**, **local** ou **híbrido**. O consenso global é atribuído a sistemas que necessitam de todos os participantes para tomada de decisões sobre qualquer tipo de atividade ou mudança de estados. Essa maneira de atuar prejudica o sistema, pois é necessário uma alta quantidade de informações trocadas entre todos os participantes para se chegar a uma decisão sobre o determinado assunto. O consenso local pode ser empregado em sistemas particionados ou dividido em extensões, onde cada grupo fica responsável por gerenciar uma área e obter uma decisão. Nesse modelo, uma decisão não interfere em outra.

Essa forma de consenso diminui o consumo de recursos, visto que é necessário um número menor de troca de mensagem. No entanto, uma visão particionada sobre a rede ou sistema pode ser prejudicial quando é necessário um conhecimento geral. Por último, o consenso pode ser aplicado de forma híbrida. Esse modo consiste na fusão de consenso local e global. Esse sistema pode ser dividido em subgrupos locais, que podem formar um grande consenso global. Esse modelo apresenta melhorias em ambos os sentidos, pois une o melhor dos dois tipos de consenso. Decisões particionadas para uma requisição global eliminam o alto custo computacional gerado pela comunicação entre todos os participantes.

O consenso pode ser evidenciado na computação de duas formas: pode ser tratado como problema, ou seja, como se obter um consenso em computação distribuída; ou pode ser usado como solução, através da realização de um acordo consensual entre participantes de um mesmo sistema. As duas formas necessitam de colaboração, troca de informações, união e coparticipação de todos os envolvidos nas decisões. Ao longo do tempo, o consenso computacional vem sendo estudado com intuito de buscar formas de resolver a colaboração entre entidades. Alguns autores apresentam formas de resolver o problema de consenso distribuído (Li et al., 2014) através de *decisões colaborativas* e *distribuídas entre participantes*. Outros (Colistra et al., 2014a) levam em conta a dinamicidade e precisão do consenso para resolver diversos problemas em sistemas distribuídos, que necessitam de ampla cooperação entre seus participantes (Augustine et al., 2013) Portanto, fica evidente a importância e relevância que o uso de consenso representa às redes e sistemas distribuídos, seja na forma de problema ou na forma de solução. Nesta trabalho, o consenso será abordado como técnica para apoiar na mitigação de ataques IDF.

2.5.5 A vigilância *watchdog*

A técnica de vigilância (monitoramento) cão de guarda (do inglês, *Watchdog*) tem papel fundamental na construção de sistemas confiáveis e seguros (Zhou et al., 2015). Além disso, o uso de monitoramento entre participantes visa garantir a confiança entre eles. O monitoramento pode ser executados de forma ativa ou passiva. A forma passiva caracteriza-se pela vigilância entre os participantes da rede ser realizada em modo promíscuo, onde todos os participantes vigiam-se em busca de anomalias. Desta forma, ao detectar um comportamento fora do padrão, os participantes informam uma entidade central sobre a anomalia, assim a central toma uma decisão mitigadora com base nas informações recebidas. Este tipo de monitoramento é mais empregado em redes centralizadas, onde há uma entidade controladora responsável pela segurança dos dispositivos. No monitoramento ativo, os dispositivos podem exercer duas funções, monitorar os participantes da redes, além de serem responsáveis pela tomada de decisão. Assim, quando identificam possíveis ameaças, eles podem definir o que deve ser feito. Essa característica melhora a identificação de anomalias e a fluidez e robustez da rede de maneira geral. Entretanto, esse modelo mais colaborativo exige que os dispositivos disponham de maiores recursos, pois exercem diferentes funções na rede. Ambas as formas de monitoramento têm como objetivo proteger o sistema de ameaças internas ou externas.

Para tornar os sistemas ainda mais robustos, o *watchdog* é por vezes vinculado a outras técnicas para garantir a segurança das redes, variando desde técnicas de cooperação Zhou et al. (2015), agrupamentos Cervantes et al. (2018) ou reputação Zhou et al. (2009). A literatura apresenta uma variedade no uso da técnica de *watchdog* na mitigação de ataques contra redes, como ao ataque *Sybil* Almas Shehni et al. (2017), contra o ataque de mau comportamento Dias et al. (2015), entre outros Cervantes et al. (2018); Zhou et al. (2015); Keally et al. (2010). Desta maneira, fica evidente que para a construção de sistemas mais robustos, o monitoramento é peça fundamental para se obter ambientes mais seguro. A técnica *watchdog* apresenta vantagens e desvantagens quando empregada em redes. As vantagens estão na forma como o monitoramento

pode ser realizado, ou seja, contínuo, discreto, de maneira passiva ou ativa, não dependendo de uma entidade externa e com a participação de todos os dispositivos presentes na rede. A desvantagem está no aumento do consumo de recursos computacionais dos dispositivos que fazem o monitoramento. O custo computacional elevado pode sobrecarregar a rede com as muitas trocas de informações. Nesse sentido, quando aplicado em redes dinâmicas, como a IoT, em que os dispositivos apresentam restrições de energia e processamento, a dificuldade é ainda maior para sua implementação.

2.6 RESUMO

Este capítulo apresentou os fundamentos sobre Internet das Coisas, exemplificando modelos de aplicações, tecnologias e modelos propostos de arquitetura, para redução de problemas de interoperabilidade de dispositivos até chegar na disseminação de dados dentro da IoT. Também foram descritos os requisitos de segurança em redes sem fio e como eles afetam o desenvolvimento da IoT. Foi demonstrado como os atacantes exploram as vulnerabilidades da rede com o intuito de realizar ações maliciosas, violando atributos como integridade, disponibilidade e confidencialidade das informações trafegadas na rede. Além disso, foram apresentadas as principais técnicas usadas na mitigação de ataques IDF e como as abordagens de consenso e *watchdog* podem ser empregadas para combater esse tipo de ataque em redes IoT.

3 ABORDAGENS E TÉCNICAS DE MITIGAÇÃO DE ATAQUES IDF EM RSSF E IOT

Este capítulo apresenta a revisão da literatura acerca do problema do ataque de injeção de dados falsos (IDF). A Seção 3.1 traz uma visão geral sobre esse problema e as técnicas utilizadas para contenção. A Seção 3.2 descreve como o tema foi abordado inicialmente, com a utilização da técnica de filtragem em rota e a evolução no tratamento do problema. Em seguida, uma tabela apresenta a síntese desses trabalhos, com suas vantagens e desvantagens. A Seção 3.3 destaca os trabalhos baseados na abordagem de agrupamento, além de apresentar suas vantagens e desvantagens também em forma de tabela. A Seção 3.4 destaca o uso do consenso no contexto da redes IoT, e, por fim, a Seção 3.5 evidencia o uso da técnica de monitoramento *watchdog* no auxílio a sistemas de detecção de intrusão.

3.1 VISÃO GERAL

A evolução de dispositivos computacionais capazes de coletar e disseminar informações vem possibilitando o surgimento de serviços personalizados e únicos. Por exemplo, serviços de mensuração de temperatura, localização de objetos e monitoramento de condições de equipamentos, entre outros, podem ser oferecidos de maneira rápida e eficiente. Assim, os dispositivos são inicializados em diferentes localidades, passando a trabalhar de forma organizada e dinâmica. Entretanto, algumas vulnerabilidades podem comprometer a oferta de serviços, tais como a presença de atacantes, falha dos dispositivos, a heterogeneidade de dispositivos e, até mesmo, o esgotamento de recursos energéticos. Além disso, o meio de comunicação sem fio está exposto à interferências, ruídos e colisões, que podem comprometer a qualidade e disponibilidade do serviço oferecido. Neste cenário, um ataque como o IDF pode aproveitar essas vulnerabilidades e comprometer a autenticidade dos dados disseminados, interferindo, assim, na disponibilidade da rede.

A detecção de ataques IDF em redes conta com diversas abordagens encontradas na literatura. Essas abordagens podem ser divididas em: baseada em filtragem em rota (Lu et al., 2012), baseada em agrupamentos (Wang et al., 2014) e sistemas de detecção de intrusão (Yang et al., 2017). A filtragem em rota considera a filtragem de pacotes na origem e no destino quando são considerados atributos como a marcação de pacotes e o descarte pelos nós intermediários e também pelo agregador de pacotes. Entretanto, desconsidera-se o dado coletado em si e a dinamicidade dos dispositivos, assim como também não se considera a detecção da origem do ataque. A abordagem baseada em agrupamentos leva em conta a eliminação de dados falsos de duas formas, uma antes da formação dos agrupamentos e outra após os agrupamentos estarem formados. Além disso, também considera o uso de de uma forma de filtragem. Porém, não avalia a verificação dos dados disseminados pelos dispositivos e, ainda assim, é limitada no quesito de detecção da origem do ataque. Os sistemas de detecção de intrusão são abordagens mais adequadas para detecção e mitigação dos mais variados ataques. Eles são capazes de identificar, mitigar e excluir ameaças da rede. Entretanto, o uso pode apresentar problemas para a rede, tais como o alto consumo de recursos, a geração de novas vulnerabilidades e a sobrecarga ao sistema.

Existem outras formas de abordar a ameaça de ataques IDF de forma colaborativa e dinâmica. Técnicas como monitoramento *watchdog* e consenso colaborativo, quando usadas de forma combinada, podem trazer diversos benefícios para a rede, tais como a colaboração entre participantes, o monitoramento contínuo, a detecção em tempo real e a precisão nas decisões. Contudo, seu uso necessita ser organizado e padronizado para evitar a criação de brechas na rede.

A criação de mecanismos capazes de mitigar e isolar a presença de ameaças como a do ataque IDF é cada vez mais essencial para o desenvolvimento de aplicações e serviços personalizados na IoT. A seguir são apresentados os principais trabalhos propostos para lidar com os ataques IDF em diferentes contextos e redes, além de serem discutidas suas vantagens e desvantagens ao contexto de IoT densa.

3.2 ABORDAGEM DE FILTRAGEM EM ROTA

Uma forma de lidar com ataques de injeção de dados falsos é a utilização dos esquemas de Filtragem em Rota (do inglês, *En-Route Filtering*). Essa filtragem visa melhorar a resiliência da rede, desempenhando um papel importante contra ameaças através da verificação de pacotes entre a origem e o destino. Desta forma, apenas pacotes filtrados são considerados honestos e recebidos no agregador (Lu et al., 2012; Ye et al., 2005). Na filtragem em rota, a verificação de pacotes também é responsabilidade dos dispositivos intermediários, que investigam se o pacote sofreu qualquer tipo de alteração que possa interferir em sua autenticidade e integridade. Assim, busca-se diminuir o número de saltos percorridos por mensagens adulteradas, que possam interferir no funcionamento da rede e, portanto, evitar o desperdício de recursos computacionais.

Na primeira fase da filtragem em rota, cada dispositivo de encaminhamento examina a validação do Código de Autenticação da Mensagem (do inglês, *Message Authentication Code* - MAC), calculado pelo dispositivo de associação inferior e, em seguida, remove esse MAC da mensagem recebida. Se a verificação for bem-sucedida, ou seja, não for detectada nenhuma alteração, ele calcula e anexa um novo MAC, que é baseado sem sua chave compartilhada recebida do dispositivos superior à sua posição. Finalmente, ele encaminha o relatório para o próximo nó em direção à Estação Base (do inglês, *Base station* - BS). A Figura 3.1 retrata uma estrutura base de um esquema de filtragem em rota em que o dispositivo na rota entre o destino e a origem recebe uma mensagem do dispositivo de origem ou de um dispositivo associado inferior a ele. Então, é verificada a integridade da mensagem recebida por meio do MAC do pacote. Caso a verificação ocorra de forma bem sucedida, a mensagem é encaminhada. Caso contrário, ela é descartada e a rede prossegue com seu funcionamento padrão (Yu e Guan, 2010; Ye et al., 2005; Lu et al., 2012; Uluagac et al., 2010).

A literatura apresenta uma diversidade de trabalhos que utilizam a abordagem de filtragem em rota para lidar com a ameaça do ataque de injeção de dados falsos. Dentre esses trabalhos, há uma linha promissora que foi iniciada por (Ye et al., 2005). Considerada a primeira proposta de filtragem para RSSF, seus autores desenvolveram um Esquema de Filtragem Estatística (do inglês, *Statistical En-Route Filtering* - SEF), que serviu como base para o surgimento de diversos trabalhos na linha de filtragem, sendo possível destacar os trabalhos (Yang et al., 2015; Yu e Guan, 2010; Lu et al., 2012; Davis e Clark, 2011; Kraub et al., 2007).

No modelo de filtragem desenvolvido em (Ye et al., 2005) há um *pool* de chaves globais que é dividido em n partições não sobrepostas, e partições. Antes da implantação, cada nó armazena um pequeno número de chaves de autenticação selecionadas aleatoriamente de uma partição do conjunto de chaves globais. Os nós com chaves da mesma partição são consideradas do mesmo grupo. Dessa forma, todos os nós são divididos em n grupos via chaves partições não sobrepostas. O esquema SEF adota a autenticação T, ou seja, para um relatório ser considerado legítimo, ele deve conter T MACs gerados por nós T de diferentes grupos. Cada um desses nós T gera um MAC com uma das chaves de autenticação armazenada. Cada nó de detecção de evento endossa o relatório, produzindo um MAC usando uma de suas chaves armazenadas. Caso um relatório apresente um número insuficiente de MACs, ele não será encaminhado ao seu destino. Assim, quando um coletor recebe os relatórios de eventos, ele verifica todos os

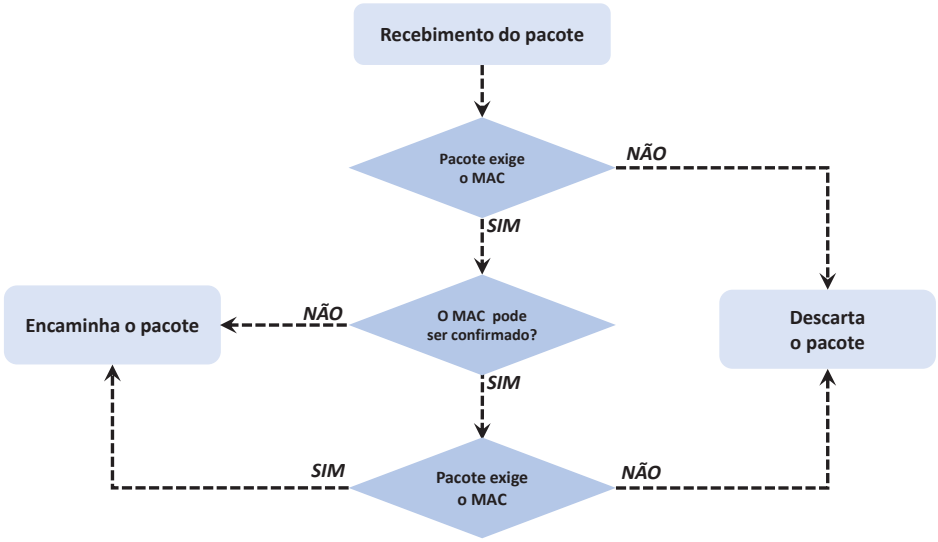


Figura 3.1: Estrutura de processo de filtragem em rota usando MAC para validação de pacotes baseada em Jeba e Paramasivan (2012)

MAC transportados e é capaz de identificá-los. Isso ocorre devido ao seu conhecimento sobre todo o *pool* de chaves globais disponibilizado. Logo, os relatórios com números insuficientes de MACs são descartados. Desta forma, os relatórios ilegítimos, que apresentam MACs incorretos, mas mesmo assim conseguem burlar os dispositivos e passar pela rota de filtragem sem serem detectados, ao chegar no controlador, serão descartados. O SEF é responsável por detectar e eliminar os relatórios ilegítimos de nós comprometidos dentro da rede. Entretanto, o SEF é incapaz de detectar quais são as origens dos relatórios (pacotes) ilegítimos. Isso ocorre porque os relatórios são filtrados na rota de modo probabilístico. Logo, a detecção de ataques IDF pode ocorrer com 80 a 90% de probabilidade entre 10 saltos. No entanto, há muitas limitações no modelo, e uma delas está no comprometimento dos nós. A medida que todos os nós armazenam as chaves, se um atacante comprometê-lo, ele passa a ter acesso a todas as chaves armazenadas pelo nó. Além disso, o SEF faz apenas a verificação do MAC. Assim, caso o conteúdo do pacote seja alterado, ele não é identificado. bem como não considera-se a identificação e o isolamento de atacantes. Logo, o mesmo nó pode continuar a enviar falsos relatórios.

Seguindo a mesma linha do SEF, Kraub et al. (2007) propuseram STEF (do inglês, *Secure Ticket-Based En-route Filtering*), que utiliza o conceito de *ticket* para a verificação de pacotes. Os *tickets* são emitidos pelos nós definidos como coletor. Nesse caso, os pacotes só são encaminhados se contiverem um *ticket* válido. Caso contrário, serão imediatamente filtrados e descartados. O funcionamento do STEF se assemelha ao SEF na forma de verificação dos pacotes, em que os *tickets* fazem a função do código de autenticação da mensagem. O conceito de *tickets* opera de forma unidirecional, ou seja, o nó verifica apenas uma única vez o pacote. Essa forma de funcionamento traz grande problema para detecção de ataques porque uma única verificação aumenta a incidência de falsos positivos e falsos negativos. Além disso, o modelo não considera a manipulação de dados nem a identificação e isolamento de dispositivos maliciosos.

Acompanhando a mesma linha dos trabalhos anteriores Yu e Guan (2010) propuseram o DEF (do inglês, *Dynamic En-route Filtering*), onde os relatórios legítimos são endossados por vários nós sensores utilizando suas próprias chaves de autenticação. No início, antes da implantação, os nós são pré-carregados com uma chave de autenticação primária e com chaves secretas escolhidas de forma aleatória, a partir de um *pool* de chaves globais. Além disso, a rede é organizada em subdivisões e cada uma delas conta com um líder. Assim, antes de

enviar os relatórios, o líder de cada subdivisão dissemina as chaves de autenticação para os nós de encaminhamento, criptografadas com chaves secretas, que serão usadas para endossar os relatórios. Os nós de encaminhamento armazenam as chaves apenas se puderem descriptografá-las com êxito. Assim, cada nó de encaminhamento valida a autenticidade dos relatórios e descarta os falsos. Posteriormente, os líderes das subdivisões enviam as chaves de autenticação para validar os relatórios. O esquema DEF envolve o uso de chaves de autenticação e chaves secretas para disseminar as chaves usadas para a autenticação dos relatórios. Esse modelo traz mais segurança para a rede. Entretanto, a utilização de muitas chaves gera um grande impacto no consumo de energia, além de acrescentar um tempo extra para criptografar e descriptografar as chaves. Além disso, não é considerado a manipulação dos dados pelo atacante.

Diferente dos trabalhos já apresentados, o VEBEK (do inglês,*Virtual Energy-Based Encryption and Keying for Wireless Sensor Network*) (Uluagac et al., 2010) é um protocolo desenvolvido para as RSSF, que visa minimizar a sobrecarga associada à atualização de chaves pelos dispositivos. O protocolo utiliza uma chave dinâmica única para uma mensagem gerada pelo sensor de origem. O VEBEK faz uso do mecanismo de criptografia RC4 para fornecer confidencialidade simples aos pacotes. A chave para a criptografia é obtida a partir do módulo de chaveamento baseado em energia virtual. O nó receptor deve controlar a energia do nó de envio para decodificar e autenticar um pacote quando um nó de encaminhamento o recebe. O nó confere sua lista de observações para determinar se o pacote veio de um nó que está em observação ou não. A lista é composta de nós que são considerados suspeitos. Se o pacote vier de algum nó dessa lista, ele é descartado. Caso contrário, o pacote é encaminhado sem modificação. O VEBEK suporta dois modos operacionais VEBEK-I e VEBEK-II. No modo VEBEK-I, todos os nós observam seus vizinhos. Quando um pacote é recebido de um nó sensor vizinho, sua autenticidade e integridade são verificadas. O VEBEK-I reduz a transmissão no topo, pois ele pode capturar pacotes maliciosos no próximo salto. Entretanto, aumenta a sobrecarga de processamento devido à decodificação e codificação que ocorre em cada salto na rede. No modo operacional VEBEK-II, os nós na rede são configurados para observar apenas alguns nós. Ele não é habilitado a capturar pacotes no próximo salto. Assim, o VEBEK-II consome mais recursos devido à sincronização dos nós, o que pode gerar uma maior sobrecarga na rede. Além disso, nas RSSF que dispõem de poucos recursos de processamento e energia, utilizar criptografia e sincronização degrada o desempenho da rede. Também, ao não considerar a detecção de dados falsos e o isolamento de ameaças, tende-se a comprometer o funcionamento da rede.

Dentre as abordagens que utilizam a filtragem em rota, (Lu et al., 2012) propuseram o uma linha diferente com o BECAN (do inglês, *A Bandwidth-Efficient Cooperative Authentication*) é o que apresenta melhor filtragem e confiabilidade quando comparado aos outros esquemas de filtragem citadas. No BECAN, cada nó requer um número fixo *(k)* de vizinhos para realizar a autenticação. Essa autenticação baseia-se no roteamento entre vizinhos cooperativos (do inglês, *Cooperative Neighbor Routing* - CNR), que representa a confiabilidade entre quem participa da filtragem. Os autores utilizam a injeção de dados falsos por meio da autenticação cooperativa de relatório de eventos. Cada nó vizinho de origem recebe k eventos falsos. A autenticação em rota do BECAN é distribuída para todos os nós ao longo do caminho do roteamento, evitando maior complexidade no seu modelo. Este esquema adota a técnica de autenticação bit comprimida para economizar largura de banda na troca de informações. A técnica proposta é adequada para lidar com o comprometimento do link de comunicação e também na filtragem de dados injetados em RSSF. Ela também evita que atacantes comprometam os nós, utilizando um protocolo de roteamento AODV (do inglês, *Ad Hoc On-Demand Distance Vector*), que gerencia de forma dinâmica as rotas entre os dispositivos. Entretanto, o BECAN não é capaz de lidar com ataques que manipulem os dados coletados por sensores, pois não faz

a verificação de dados. Além disso, o roteamento AODV gera maior sobrecarga na redes e é vulnerável a ataques no roteamento. Estas desvantagens demonstram que ele não é adequado para lidar com a dinamicidade de redes massivas.

3.2.1 Discussão das abordagens de filtragem em rota

O desempenho dos esquemas de filtragem em rota pode ser analisado baseado na eficiência de filtragem dos pacotes, detecção da fonte e quanto ele consome de recursos. O esquema de filtragem SEF foi o primeiro a tentar resolver o problema de injeção de dados falsos em RSSF. Porém, limitou sua capacidade de filtragem de forma a não poder impedir ataques representativos e contínuos. No SEF, uma única chave compartilhada é usada para gerar e verificar MACs. Consequentemente, as chaves podem ser usadas incorretamente para gerar falsos relatórios, além de gerar uma sobrecarga maior na rede. Para evitar esse problema, foi proposto o mecanismo STEF, que buscava eliminar os problemas já citados. Ele foi introduzido com o conceito de uso de *ticket*, ao invés de MAC, para autenticar os pacotes. Um relatório é gerado juntamente com o *ticket*, que necessita de uma chave compartilhada entre os nós na rota de destino. No entanto, como o SEF, o STEF também insere uma carga adicional devido à resposta da consulta à comunicação para o percurso dos relatórios. Porém, os requisitos de armazenamento de relatório são menores se comparados à outras abordagens. O STEF pode ser aplicado em RSSF de alta densidade.

As abordagens DEF e SEF são independentes das alterações de topologia. Também, só podem filtrar os relatórios falsos gerados por um nó malicioso sem a chave de sessão, em vez daqueles gerados por um líder de subdivisão comprometido ou outros nós sensores. O VEBEK e BECAN, mesmo inspirados nos modelos de filtragem, buscaram novas formas de resolver os problemas de ataques IDF. Porém, ambas as abordagens, da mesma forma como seus antecessores, também apresentaram desvantagens quanto ao seu uso, seja na sobrecarga da rede, não identificação da fonte do ataque e por não lidar satisfatoriamente com a densidade de RSSF. Como visto nos trabalhos apresentados, as filtragens dinâmicas em rota são mais resistentes à ataques de injeção de dados falsos do que as estáticas. Uma desvantagem significativa é que elas aumentam a sobrecarga de comunicação quando as chaves são eventualmente atualizadas ou redistribuídas. Há muitas razões para a atualização das chaves, o que inclui a sua atualização após a revogação para evitar que elas se tornem antigas ou devido a mudanças dinâmicas na rede.

A Tabela 3.1 apresenta o desempenho dos principais esquemas de filtragem em rota. A eficiência dos esquemas de filtragem em rota pode se destacar pelo tamanho da mensagem usada para autenticar o relatório de eventos, pela capacidade de filtragem do nó de cada rota no caminho da transmissão dos dados e na quantidade de energia consumida para filtrar dados falsos injetados. Além disso, é considerada a identificação da fonte do ataque. O VEBEK apresentou o menor consumo de energia em comparação com outros esquemas, porém é o que necessita do maior número de saltos para identificar e descartar os pacotes falsos, até 15 saltos. O BECAN também necessita de até 15 saltos para conseguir descartar todos os pacotes. O DEF é o que necessita do menor número de saltos para realizar a filtragem, de 5 a 10 saltos. Portanto, é o que apresenta menor economia de energia, pois a mensagem de autenticação gerada por ele é maior em relação à dos outros. Como observado, nenhuma das abordagens apresentadas na Tabela 3.1 realiza a verificação dos dados coletados pelos sensores, o que impacta diretamente no funcionamento da rede.

Os esquemas de filtragem em rota são uma alternativa interessante na mitigação de ataques de injeção de dados falsos, visto que apresentam uma alta taxa de eliminação de pacotes falsos. Entretanto, existem lacunas abertas como a não identificação da fonte do ataque, o que pode ser observado na coluna identificação da fonte, onde nenhum dos esquemas realiza

Tabela 3.1: Análise de desempenho das abordagens baseados em filtragem em rota

Esquemas	Mensagens de autenticação	Filtragem por Saltos	Eficiência Energética	Id. da Fonte
SEF	Relatório de eventos contém o MAC de todos os nós detectados	90% dos pacotes falsos são detectados dentro de 10 saltos	Economiza 80% de energia	Não
STEF	Relatório de eventos contém *Ticket* de todos os nós detectados	90% dos pacotes falsos são detectados dentro de 10 saltos	Economiza 32% a 65% de energia	Não
DEF	Relatório de eventos contém mensagem de autenticação de todos os nós do subgrupo	90% dos pacotes falsos são detectados dentro de 10 saltos	Economiza 50% de energia	Não
VEBEK	Valor de energia de um nó é a identidade do nó de envio	90% dos pacotes falsos são detectado dentro de 15 saltos	Economiza 60% a 100% de energia	Não
BECAN	Cada relatório contém a mensagem de autenticação de todos os vizinhos	90% dos pacotes falsos são detectados dentro de 15 saltos	Economiza 80% de energia	Não

essa função. Isso fica evidente, pois toda a verificação de autenticidade foca na validação do código de autenticação de mensagem, seja pelo MAC ou *tickets*. Essa forma de atuar, acarreta a maior incidência de ataques contra a rede, pois os atacantes podem enviar repetidas vezes dados alteradas que não serão identificados. Logo, a rede é sobrecarregada e o seu funcionamento é deteriorado, gerando diversos problemas para disponibilizar os dados legítimos. Esse problema acontece porque quando foram projetados, esses esquemas tinham como objetivo manter a resiliência da rede perante às ameaças. Logo, para serem aplicados em redes como a IoT, essas soluções necessitam adequar-se a fatores como a mobilidade dos dispositivos, consumo energético, heterogeneidade, grande volume de dados, além da dinamicidade da rede e dos dados que podem variar conforme o modelo de aplicação. Assim, tornam-se inviáveis por consumirem muitos recursos e não eliminarem as ameaças por completo.

3.3 ABORDAGEM BASEADA EM AGRUPAMENTO

Buscando avaliar outras formas de lidar com os ataque IDF, novas abordagens foram desenvolvidas, entre elas destacam-se as que usam técnicas de agrupamentos. Desta forma, trabalhos como (Zhu et al., 2015; Zhang et al., 2006, 2010; Jeba e Paramasivan, 2013; Wang et al., 2014) apresentam uma nova perspectiva na maneira de lidar com essa ameaça. Os agrupamentos são usados como forma de detectar ataques. Logo, eles herdam características da filtragem em rota, como por exemplo o uso de autenticação de mensagens e o descarte de pacotes na rota até a central. Além disso, usam formas de localização baseadas em GPS (do inglês, *Global Positioning System*). Assim, buscam melhorar a resiliência da rede e ainda garantir a disponibilização dos dados de forma segura e rápida.

O funcionamento das abordagens baseadas em agrupamentos está na forma como são formados e classificados os diferentes tipos de agrupamento. Como elas têm forte relação com as filtragens, a composição considera fatores como detecção pré e pós agrupamentos. Desta forma, a detecção do ataque pode ocorrer antes dos agrupamentos serem formados, ou seja, os atacantes são detectados e, assim, são bloqueados de participar dos agrupamentos. Na pós formação, a detecção ocorre após os agrupamentos serem formados e essa detecção pode ser feita pelo líder do agrupamento ou por uma central. Cabe ressaltar que, em ambas as formas, a detecção do ataque pode ser efetuado por uma entidade central ou pelos próprios dispositivos. A seguir são descritos os principais trabalhos que fazem uso de agrupamentos contra a ameaça do ataque IDF.

Seguindo essa linha é apresentando uma nova forma de mitigar o problema de injeção de dados falsos, em (Zhang et al., 2006) foi proposto um conjunto de ferramentas para filtragem e identificação de injeção de dados falsos. Esse conjunto foi denominado “Algoritmo de Reação baseado em Alertas para a Identificação de Nós Comprometidos”. Esse conjunto demanda que todos os nós da rede sejam pré-carregados com uma chave simétrica e, à medida que os eventos vão acontecendo, os nós próximos a ele geram alertas. Esses alertas são assinados através de um MAC, que é computado com a chave armazenada em cada sensor. Esse modelo permite à Estação Base (do inglês, *Base Station*- BS), reconhecer o tipo de alerta gerado. Normalmente, mais de um nó está próximo dos eventos registrados. Desta forma, a BS receberá vários alertas, assegurando a autenticidade deles. Entretanto, não é levado em consideração o consumo energético no carregamento das chaves por todos os nós, além de que, caso a BS apresente falhas, nenhum relatório será verificado. Além disso, o trabalho não avalia a possibilidade de o agrupamento próximo à região onde o evento foi registrado estar fortemente comprometido e gerando uma grande quantidade de falsos alertas, mesmo as suas chaves estando devidamente autenticadas. Nesse caso, a BS não teria a possibilidade de identificar quais as informações são falsas, pois existiriam diversos alertas transmitindo o falso evento detectado.

O trabalho desenvolvido em (Zhang et al., 2010) tem como foco principal detectar, filtrar e descartar os dados falsos, classificado no trabalho como "falso relatório". Assim que detectado, o dado é descartado imediatamente pelo esquema, com o objetivo de reduzir o consumo de energia. Todavia, os autores não buscam a identificação da origem da injeção de falsa informação, ou a mitigação e exclusão da rede. O esquema utiliza o MAC como forma de computar os relatórios transmitidos através da rede e a organiza em níveis, onde o próximo salto sempre estará em um nível acima, ficando responsável por verificar a autenticidade do MAC proveniente do nível abaixo. Nesse sentido, essa proposta pode ser eficiente para detectar injeções como falsos alertas de determinados eventos, mas seria ineficaz contra as falsas coletas, que são o foco do presente trabalho. Além disso, as propostas não levaram em consideração a possibilidade do agrupamento estar fortemente comprometido, o que afeta a verificação entre os níveis. Porém, é fundamental destacar que a característica de identificar a fonte do ataque tem um alto custo agregado à rede. Entretanto, sem essa capacidade, os mecanismos não seriam eficientes a ponto de frear a inundação da rede com falsas informações.

Em Jeba e Paramasivan (2013), os autores propõem EEMDTS (do inglês, *Energy Efficient Multipath Data Transfer Scheme*), um esquema de transferência de dados multicaminhos com eficiência energética, para mitigar o ataque de injeção de dados falsos em RSSF. Os autores utilizam a técnica de transferência de dados em roteamento multicaminhos com a finalidade de prevenir que os nós comprometidos tenham acesso ao roteamento e aos dados coletados que são transmitidos. O EEMDTS utiliza chaves privadas distribuídas por uma central para cada participante da rede, assim que são inseridos na rede. A central também administra o fluxo dos dados que são encaminhados pelos nós e armazena essas informações. Após a implantação da rede, ela é organizada em agrupamentos formados através de uma arquitetura hierárquica, que se utiliza de líderes de agrupamentos para melhorar o roteamento entre nós e a central. Entretanto, o uso de uma entidade de distribuição de chaves centralizada expõe a rede a diversos problemas. Caso ela venha a apresentar falhas, toda a rede pode ser afetada e entrar em colapso. O EEMDTS não se preocupa em identificar a origem do ataque, bem como a não exclusão dos nós maliciosos da rede, o que acarreta que o nós, mesmo que tenham seu pacote descartado, continuaram a enviar dados falsos. Além disso, o EEMDTS não realiza a comparação entre agrupamentos. Assim, caso existam agrupamentos comprometido por atacantes, o mecanismo não é capaz de identificar, gerando um problema ainda maior.

Em Wang et al. (2014) os autores introduziram um novo conceito para o ataque de injeção de dados falsos, apresentando um conceito do ataque de forma colaborativa. Dessa forma, eles desenvolveram dois esquemas para mitigação do ataque em RSSF. O primeiro é o GFFS (do inglês, *Geographical Information based False Data Filtering Scheme*), que realiza uma distribuição de chaves entre os nós da rede baseada na localização, que é aferida através de dispositivos de GPS acoplados nos sensores. Essas chaves são utilizadas para filtrar os dados falsos. O mecanismo cria agrupamentos com o intuito de melhorar a filtragem dos dados. Para isso, um dispositivo é eleito como líder, que os autores classificam como CoS (do inglês, *Center-of-Stimulus*). Os CoS verificam as chaves e agregam as coletas em forma de relatórios, encaminhando-os à central. As verificações acontecem nos nós encaminhadores, onde são analisadas as chaves dos CoS, além da análise das coletas, averiguando a legitimidade, baseada nas posições dos sensores e os locais onde foram realizadas. Assim, caso sejam detectados, relatórios inconsistentes são descartados.

O segundo mecanismo é o NFFS (do inglês, *Neighbor-Information based False Data Filtering Scheme*), que funciona de maneira similar ao GFFS. A mudança está na forma como as chaves são distribuídas. Ao invés de utilizar posições baseadas nas informações de GPS, ele utiliza as informações sobre os nós vizinhos. O mecanismo garante que os sensores, após a fase de implantação, distribuam suas chaves pela rede baseados na sua lista de vizinhos. Assim, é necessário armazenar uma lista dinâmica de vizinhos capaz de se adaptar às mudanças de vizinhança. O NFFS exige o armazenamento de listas, que podem extrapolar a limitação de memória dos sensores, e, com 37% de nós maliciosos, o mecanismo zera sua detecção. Os próprios autores afirmam que o GFFS requer custos adicionais para o melhor funcionamento, pois com a implantação de um dispositivo caro em cada sensor, o GPS aumenta o custo econômico da rede. O mecanismo tem sua taxa de detecção zerada quando 33% dos nós são injetores de falsa informação, ou seja, existe uma grande limitação do GFFS. Além disso, ambos os esquemas desconsideram a comparação entre os agrupamentos próximos para identificar os nós maliciosos. Também não consideram a carga extra na distribuição de chaves, bem como o consumo energético que a rede pode apresentar.

Os autores em (Zhu et al., 2015) apresentam SPAIS (do inglês, *Self-checking Pollution Attackers Identification Scheme*). O trabalho aborda o conceito de poluição de dados ao invés de dados falsos. Esse termo é utilizado por sua característica de alta propagação na rede, podendo afetar todos os participantes. Assim, o trabalho apresenta um esquema para mitigar esse problema. O SPAIS organiza a rede em uma arquitetura hierárquica, o que viabiliza a correta formação de agrupamentos. O objetivo do mecanismo SPAIS com os agrupamentos é possibilitar o monitoramento em modo cooperativo dos nós em níveis inferiores pelos nós sensores nos níveis superiores. O referido mecanismo utiliza a técnica de geração de alertas para notificar a central que existe um ataque de poluição acontecendo, para que ela possa tomar providências. Entretanto, ao não prever a possibilidade de um agrupamento fortemente comprometido, o SPAIS permite que falsos alertas sejam repassados à rede quando vários níveis da hierarquia estiverem comprometidos. Caso um líder venha ser o atacante, o mecanismo não é capaz de detectar.

3.3.1 Comparação sobre as abordagens baseadas em agrupamentos

A Tabela 3.2 apresenta uma síntese dos trabalhos abordados fazendo um comparativo entre as abordagens que utilizam agrupamentos para lidar com o problema de injeção de dados em RSSF. Os atributos avaliados são auxílio externo, arquitetura, detecção da fonte do ataque e resiliência da rede. Observa-se que o GFFS faz uso de auxílio externo, as demais abordagens utilizam os recursos dos próprios participantes. Isso demonstra o alto custo que é a implementação de uma entidade externa para detectar ataques, porém não garante melhorias e pode sobrecarregar

a redes. No uso de arquitetura é possível destacar que não existe um padrão de preferência de organização da rede, visto que os modelos centralizado e distribuído estão empatados. Contudo, vale destacar que um arquitetura centralizada permite uma menor troca de mensagens entre os participantes da rede, bem com a correta organização dos agrupamentos, além de oferecer uma melhor gerência aos mecanismos de segurança. Quando se pensa em escalabilidade de redes, uma arquitetura distribuída oferece maior poder de crescimento e organização, além de não apresentar um ponto único de falhas.

Tabela 3.2: Síntese das Abordagens Baseadas em Agrupamentos

Abordagens	**Aux. Externo**	**Arquitetura**	**Font. Ataque**	**Resiliência**
Zhang et al. (2006)	Não	Centralizada	Sim	15%
Zhang et al. (2010)	Sim	Distribuída	Não	26%
Jeba e Paramasivan (2013)	Não	Distribuída	Não	6%
Wang et al. (2014)	Sim	Centralizada	Não	33%
Wang et al. (2014)	Não	Centralizada	Não	37%
Zhu et al. (2015)	Não	Distribuída	Sim	30%

A detecção da fonte do ataque não é levada em conta na maioria das propostas apresentadas, e fica evidente quando observado que apenas (Zhang et al., 2006) e (Zhu et al., 2015) realizam a identificação do atacante. Essa não identificação gera consequências para as redes, como a continuidade de emissão de dados falsos, consumo de recursos e a inconsistência dos dados trafegados. Logo, o desempenho da rede é afetado de maneira geral. Por fim, a capacidade da rede em continuar funcionando perante os ataques, pode ser observada na coluna resiliência, onde é mensurada a porcentagem máxima que a rede suporta de atacantes. Observa-se que o NFFS apresenta a melhor resiliência ao ataque,, suportando até 37% de comprometimento total. O GFFS consegue suportar até 33% de comprometimento. Já o EEMDTS apresentou o pior desempenho, suportando apenas 6% de ataques contra a redes. Nos outros mecanismo não foi possível mensurar esse comprometimento, pois é informado pelos autores.

Desta forma, ao analisar os trabalhos da literatura que utilizam agrupamentos como forma de detecção de ataques IDF de diferentes natureza, é possível observar que existem lacunas a serem exploradas para futuras soluções. Por exemplo, quando foca apenas em manter a rede funcionando perante ataques, desconsiderando a identificação da sua origem, o que acarreta diversos problemas como mau funcionamento, inconsistência dos dados e má distribuição de informações.

3.4 ABORDAGEM DE CONSENSO NA IOT

O desenvolvimento constante da computação distribuída tem possibilitado o surgimento de novos modelos de detecção de anomalias em redes, sejam em redes estruturadas e não estruturadas. Beneficiando-se desse desenvolvimento, a literatura apresenta uma ampla variedade de trabalhos focados em consenso, sejam aplicados na resolução do problema de consenso distribuído ou na sua utilização de consenso para tomadas de decisão. Cada vez mais redes não estruturadas optam por abordagens com o foco em decisões colaborativa entre seus próprios participantes, sem a necessidade de entidades externas. Desta forma, o uso de consenso entre participantes para tomada de decisões tem se mostrado uma alternativa interessante em relação

aos métodos convencionais. Assim, esta dissertação aborda o consenso de tomada de decisão, enquanto os objetivos são definir formas colaborativas de mitigação. Desta forma, destacam-se propostas mais relevantes para esse trabalho, iniciando com a proposta que apresenta um algoritmo de consenso distribuído para fornecer decisões robustas quando vários serviços estão envolvidos e necessitam um consenso global (Li et al., 2014).

Em Li et al. (2014), os autores apresentam o CDM (do inglês, *Consensus Decision Making*), que usa um consenso distribuído para orientar as aplicações da IoT. O CDM auxilia os serviços da camada de aplicação, fazendo com que as decisões e serviços sejam orientados a tomarem decisões baseadas nas requisições das aplicações. Para isso, é aplicada uma estrutura de provisionamento de serviços de três camadas, para implantação na IoT. Assim, mecanismo CDM é capaz de detectar, descobrir e compor serviços em nós de borda. Ele é proposto para tomada de decisões robusta que envolvem variedades de serviços, que buscam atingir um consenso global entre os diferentes participantes. Contudo, o CDM não leva em conta a dinamicidade da rede e como ela pode afetar a execução de um consenso global de forma organizada. Além disso, não considera questões de segurança que envolvem os dispositivos.

A proposta de Carvin et al. (2014) consiste em um método para distribuir e monitorar uma rede móvel dinâmica. Para esse propósito, a teoria de consenso é aplicada com o intuito de disponibilizar uma visão comum da rede para cada nó. O monitoramento da rede acontece de forma totalmente dinâmica e baseado nas medições locais de cada nó e de seus vizinhos. A troca de mensagens entre os dispositivos acontece para rastrear e identificar a distribuição da rede. Todo o monitoramento baseia-se na teoria de consenso, a partir da qual os autores puderam derivar as condições do modelo e convergir o limite de erros. O uso de diversas formas consensos mostrou que os nós podem se comportar visando o benefício de toda a rede. Os autores também observaram que, quando acoplados à distribuição de satisfação com a densidade geográfica da rede, alguns nós tendem a mover-se em direção à zona de trânsito e aumentar a qualidade da rede de maneira global. Entretanto, quando levado em consideração a densidade geográfica, a velocidade de convergência entre os nós torna-se um limite. Isso ocorre pelo fato de que todos os nós da rede têm alto grau de mobilidade e todos fazem parte do consenso. As decisões de consenso neste trabalho são afetadas pela dinamicidade do funcionamento da rede, o que acarreta problemas na tomada de decisão entre os participantes.

Em Toulouse et al. (2016) é apresentado o problema de aplicativos distribuídos baseados em consenso. Os autores alegam que aplicativos baseados em consenso não são resistentes a nós comprometidos, que enviam dados falsificados para seus vizinhos, ou seja, eles podem ser alvo de ataques Bizantinos. Assim, eles propõem duas técnicas para mitigar e proteger os sistemas de detecção de intrusão de redes baseadas em consenso. A primeira abordagem é baseada em modelo de detecção, que tem o comportamento antecipado e descrito usando modelos matemáticos. As variáveis medidas do sistema são comparadas com as estimativas do modelo. Comparações entre o sistema e o modelo mostram desvios quando há uma falha no sistema real. A segunda abordagem, a detecção *Outlier*, tem cada módulo associado a interações de ligação entre os vizinhos que geram o consenso. Ambas as abordagens são utilizadas para detectar interrupções no consenso da rede e para prevenir o sistema contra falsas avaliações de tráfego de rede. Contudo, as avaliações realizadas pelos autores demonstram que ambas as abordagens aumentam o custo computacional do sistema significativamente, devido ao número de interações para detecção dos ataques. Apesar de melhorar as questões de segurança, a relação com o consumo energético da rede pode não valer a pena, pois em alguns casos a rede não dispõe de tantos recursos, como é o caso das redes IoT.

A utilização do consenso para mitigação de ataques mostra-se uma boa alternativa para sistemas que necessitam de cooperação entre seus participantes para a tomada de decisão.

Em Toulouse et al. (2015), os autores propuseram um sistema distribuído para detecção de anomalias baseado em um protocolo de consenso médio entre participantes. O sistema busca identificar anomalias que possam gerar ataques DDoS (do inglês, *Distributed Denial of Service*). Para isso, são realizadas análises em cada ponto de coleta de dados usando um classificador Bayes. Assim, os valores de probabilidades são computados por cada classificador e compartilhado entre os usuários para que cheguem em um consenso médio. Ao final, a análise é realizada de forma redundante e em paralelo ao nível de cada ponto de coleta de dados, o que evita o ponto único de falhas. O fato de utilizarem o consenso de forma distribuída, facilita a tomada de decisão em grupo, melhora o funcionamento e o desempenho da rede em relação a detecção de anomalias. Entretanto, o custo computacional de comunicação entre os participantes pode sobrecarregar a rede e diminuir a efetividade do sistema em relação ao seu funcionamento.

Os autores Kailkhura et al. (2015) propuseram um algoritmo robusto de consenso de média ponderada distribuída. O algoritmo visa permitir uma adaptação à regras locais estipuladas pela rede. Para isso, foi desenvolvida uma técnica de aprendizagem para estimar parâmetros operacionais ou peso de cada nó. Assim, é possível automatizar regras locais de fusão ou atualização para mitigar de ataques. O trabalho foi proposto para funcionar em uma rede distribuída, entretanto, os autores não consideram a dinamicidade como fator de impacto, o que facilita as ações de atacantes. Assim, quando descobertas as regras da rede, torna-se fácil a entrada e saída de nós, já que não há um controle de acesso para participar da rede. Assim, a incidência de ataques tende a aumentar.

3.4.1 Discussão sobre as abordagens de consenso

A utilização de consenso entre participantes mostra-se uma abordagem adequada para mitigação de ataques de diferentes formas. Quando se busca a colaboração entre participantes para tomada de decisões mais assertivas sobre uma determinada decisão, o uso de consenso mostra-se uma alternativa robusta e eficaz para esse objetivo. Por característica, ele funciona de forma distribuída e é atrelado a decisões colaborativas, o que melhora o desempenho de sistemas distribuídos ou embarcados. Entretanto, como pode-se observar nos trabalhos selecionados, existem desafios a serem alcançados quanto ao uso de consenso como abordagem de mitigação de ataques, pois são necessárias trocas constantes de mensagens entre participantes para se obter uma resposta. Além disso, deve-se considerar também o tipo de consenso a ser alcançado, seja ele global, local ou híbrido. Quanto maior o consenso for maior poderá ser o consumo de recursos atribuídos à rede. A literatura ainda carece de trabalhos voltados ao uso de consenso com técnica de mitigação de ataques. Esse campo ainda é pouco explorado por autores, o que abre margem para novos trabalhos serem desenvolvidos.

3.5 ABORDAGEM DE MONITORAMENTO *WATCHDOG*

A construção de redes seguras passa diretamente pelos participantes que fazem parte das linhas de defesa (Al-Qurishi et al., 2018). O desenvolvimento desses sistemas de segurança necessita de diferentes técnicas de monitoramento, entre elas destaca-se o monitoramento *watchdog*, responsável por realizar monitoramento entre diferentes níveis de participantes de redes. O *watchdog* pode ser executado de forma permanente ou em intervalos discretos de tempo. Além disso, ele pode avaliar diferentes tipos de comportamento, ações e, até mesmo, encaminhamento de mensagens, podendo, muitas vezes, ser utilizados como parte de sistemas de detecção mais complexos e dinâmicos. A literatura fornece uma variedade de trabalhos que abordam o uso do *watchdog* como forma de auxiliar os sistemas de detecção de anomalias (Nadeem e Howarth,

2013), ficando evidente sua importância. Dentre os trabalhos que utilizam essa técnica, foram selecionados os mais relevantes para essa pesquisa.

O trabalho desenvolvido em (Wahab et al., 2014) apresenta um modelo de detecção de nós egoístas em Redes Veiculares *Ad hoc* (do inglês, *Vehicular Ad Hoc Network* - VANET). Os autores criaram uma hierarquia baseada em agrupamentos, como ilustrado na Figura 3.2. O modelo possui duas fases de funcionamento: a primeira é capaz de motivar os dispositivos a se comportar de forma cooperativa durante a formação dos agrupamentos, e, a segunda, detecta quais os nós são egoístas depois da formação dos agrupamentos. Na primeira fase, os benefícios são oferecidos na condição de reputação que permite a motivação dos nós a se comportarem de forma cooperativa durante a formação dos agrupamentos. Os serviços de comunicação são oferecidos somente quando verificada a reputação acumulada do nó. Na segunda fase, o modelo aplica a técnica de *watchdog* baseada na teoria de Dempster-Shafer para detecção de nós egoístas, observando as evidências cooperativas e aumentando a probabilidade de detecção. A comunicação entre agrupamentos é realizada por nós que cumprem a função de retransmissão. Entretanto, o modelo apresentam uma alta taxa de falsos positivos e negativos na detecção dos nós egoístas, o que sobrecarrega e afeta o desempenho e a estabilidade da rede.

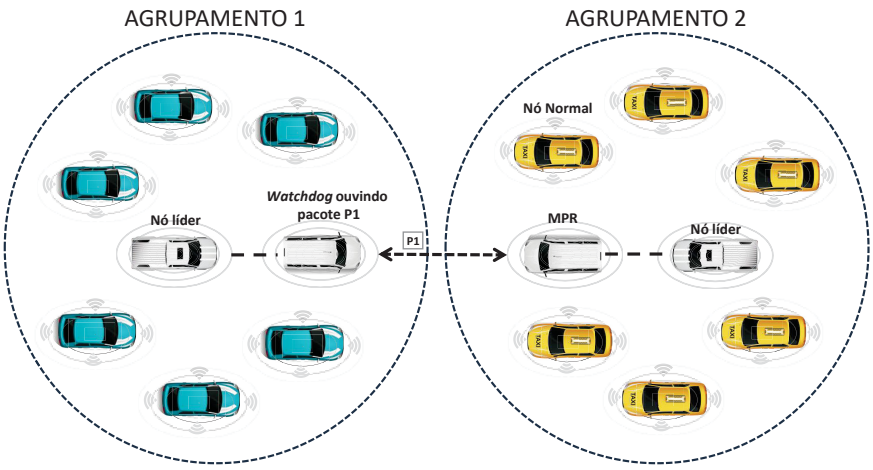


Figura 3.2: Operação do modelo de detecção de nós egoístas proposto por Wahab et al. (2014)

Em Dias et al. (2015), os autores propuseram o CWS (do inglês, *Cooperative Watchdog System*), que detecta nós egoístas dentro da rede. Ele utiliza uma atribuição de pontuação e reputação em cada nó da rede. Assim, a cada vez que os nós participam de uma interação entre si, o CWS atualiza sua pontuação de reputação com base nas considerações de três módulos: classificação, avaliação e decisão de vizinhos. O módulo de classificação categoriza os nós em diferentes tipos, de acordo com sua pontuação de reputação instituída em sua categorização. O módulo de avaliação calcula o valor cooperativo de cada nó, que é transmitido para o módulo de decisão visando punir ou recompensar os nós em função de seu comportamento cooperativo. O módulo de avaliação de decisão de vizinhos determina como vizinhos avaliam a reputação de um nó na rede, realizando perguntas de recomendação sobre determinado nó. No final de uma oportunidade de contato, o módulo de decisão atualiza a pontuação de reputação dos nós com base nas informações transmitidas pelos outros módulos. Com essa abordagem, o CWS classifica, monitora e age contra nós egoístas dentro da rede. Quando um nó egoísta é detectado, o CWS envia um alarme para todos os vizinhos do nó para ser disseminado por toda a rede. Este alarme informa aos nós cooperativos a presença de um nó egoísta. No entanto, para garantir um melhor monitoramento da rede, é necessária uma troca de mensagens maior que o padrão, o que aumenta

o número de retransmissões e gera um maior consumo computacional por parte dos nós. Além disso, caso o sistema de recomendação apresente falhas, toda a detecção fica comprometida.

Yang et al. (2017) desenvolveram um IDS baseado em detecção de anomalias usando *Watchdog* para detecção robusta de ataques de injeção de dados falsos. O modelo foi proposto para redes IoT de vigilância ambiental de predição de eventos naturais urbanos. No modelo, os nós de monitoramento são classificados como nós testemunhas, sendo selecionados pela estação base. Todos os dados coletados pelos sensores são enviadas para os nós agregadores, monitorados pelos nós testemunhas e depois encaminhados para a estação base, como pode ser observado na Figura 3.3. Para a definição das características dos dados, foi proposta a utilização de um modelo Hierárquico Bayesiano Espaço-Temporal (do inglês, *hierarchical Bayesian Space-Time*-HBT). Em seguida, é empregada uma estratégia de decisão estatística baseada num teste de probabilidade sequencial para identificar um dispositivo atacante. O modelo centralizado utilizado pelos autores cria um ponto único de falha dentro do sistema, pois todas a decisões são tomadas pela estação base. Ainda, o modelo HBT apresenta um alto consumo de energia como destacado pelos autores. Desta forma, o teste probabilístico empregado assume uma margem de erros que tende a afetar os resultados obtidos, pois ela abrange um intervalo considerável de limite superior e inferior. Outro fator que afeta o desempenho do modelo, são os critérios escolhidos para eleição dos nós testemunhas, o que pode acarretar na escolhas de nós maliciosos para realizar o monitoramento. Assim, caso um atacante seja escolhido ele terá total conhecimento sobre o modo de operação do sistema e será capaz de lançar ataques mais precisos.

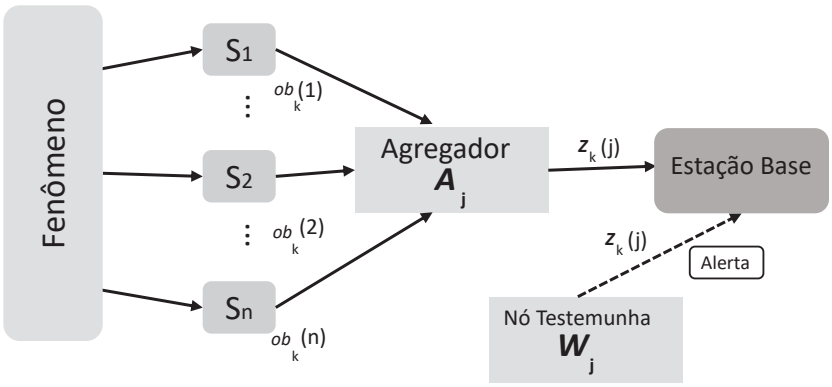


Figura 3.3: Estrutura do modelo de detecção de ataques proposto por Yang et al. (2017)

No trabalhos de Cervantes et al. (2018), os autores apresentaram uma um IDS chamado Thatachi *Detection of Sinkhole And Selective-Forwarding for Supporting Secure Routing for Internet of Things*, para mitigação de ataques *sinkhole* e *selective forwarding* em roteamentos em redes IoT densas com mobilidade. Para lidar com a densidade da rede, o Thatachi organiza a rede em forma de *clusters*, onde os nós são classificados em associados, membros e líderes, como observado na Figura 3.4. Ele estabelece caminhos entre os nós baseados nos líderes e associados com o intuito de oferecer maior escalabilidade e prolongar a vida útil da rede. As classificações atreladas aos nós são adaptáveis e podem mudar de acordo com a reconfiguração da rede. Essa reconfiguração ocorre quando um nó deixa de participar do *cluster*, seja por falhas, por ser um atacante ou deixar área de cobertura.

Para garantir a segurança e confiabilidade entre os nós, o Thatachi utiliza uma estratégia de monitoramento entre os participantes. Ele verifica o comportamento dos nós quanto ao encaminhamento dos dados recebidos. É aplicada uma combinação de estratégia *watchdog* em dois níveis. Para isso, o nó monitor calcula o número de transmissões encaminhada por um nó superior, em relação à sua própria mensagem. Os autores definem o nó superior como sendo

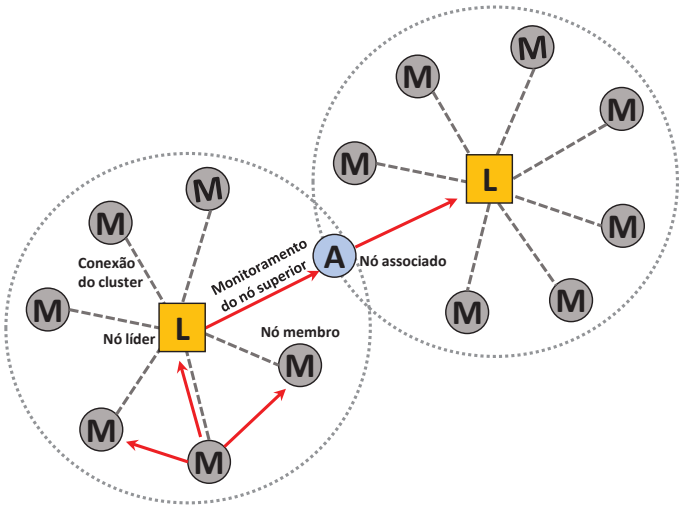


Figura 3.4: Modelo Thatachi para detecção de ataques proposto por Cervantes et al. (2018)

aquele que possui uma classificação mais baixa que os outros. Assim, torna-se possível o cálculo da quantidade de transmissões recebidas e, dessa forma, definir se um nó está apresentando um comportamento normal ou se há um desvio de comportamento. Contudo, o cálculo da confiança entre participantes apenas com base na quantidade de dados recebidos e transmitidos não exclui a possibilidade do nó modificar os dados coletados. Esse modelo, então, facilita a execução de ataques de injeção de dados falsos (Yang et al., 2017). O Thatachi apresenta-se ineficaz ao âmbito da IoT, uma vez que trabalha de maneira centralizada e não apresenta nenhuma forma de controle de acesso. Isto colabora para que qualquer nó faça parte dos agrupamentos e possam comprometer a integridade dos dados disponibilizados.

3.5.1 Discussão sobre as abordagens do monitoramento *watchdog*

O uso de monitoramento entre participantes em redes apresenta vantagens e desvantagens quando aplicado a modelos com restrições de recursos. Sua principal vantagem é o funcionamento de forma distribuída e organizada, sem a necessidade de uma entidade controladora. Além disso, o monitoramento de participante para participante apresenta melhorias para as redes IoT, tais como melhores taxa de detecção de ataques, rapidez na detecção e identificação de ameaças e facilidade na localização da fonte do ataque. Como desvantagem pode-se destacar a possibilidade de diferentes nós estarem comprometidos e gerarem alto número de falsos positivos e falsos negativos na rede. Também deve-se considerar o tipo de monitoramento utilizado, contínuo ou discreto. Ambos apresentam vantagens e desvantagens quando aplicados em sistemas de monitoramento. A forma contínua pode gerar um maior consumo de recursos da rede, porém é a mais eficaz contra ataques. A discreta não consome muitos recursos, porém tem menos eficácia contra ataques. Desta forma, usar monitoramento *watchdog* atrelado a outras técnicas de mitigação torna o sistema de detecção mais robusto e completo para lidar com diferentes tipos de ameça, entre elas o ataque IDF.

3.6 RESUMO

Este capítulo apresentou uma discussão sobre os trabalhos encontrados na literatura que abordam o problema de Injeção de dados falsos, seja no contexto de RSSF ou redes IoT. Primeiramente, foram abordadas as propostas baseadas no uso de filtragem em rota para mitigação

do problema. Em seguida, foram abordados trabalhos que utilizam técnicas de agrupamentos para lidar com o problema em questão. Também foram apresentadas novas abordagens para lidar com o problema. Desta maneira, foi detalhado como o uso de consenso e *watchdog* são utilizados na literatura como contramedidas e de que maneira a união dessas técnicas podem auxiliar no desenvolvimento de sistemas de detecção de intrusão com ataques IDF em redes IoT.

4 CONFINIT: UM MECANISMO PARA MITIGAÇÃO DE ATAQUES IDF EM REDES IOT

Este capítulo apresenta o mecanismo CONFINIT (***CON****sensus Based Data* ***FI****lteri****N****g for* ***IoT***), que busca detectar e isolar da rede dispositivos que apresentem comportamento malicioso ao serviço de disseminação de dados em redes IoT. A Seção 4.1 apresenta uma visão geral sobre o mecanismo proposto, suas características e onde ele atua. Também é apresentado o modelo de rede IoT e suas características, o modelo de disseminação de dados abordado e descrição o comportamento do ataque IDF. A Seção 4.2 descreve a arquitetura do mecanismo, detalha o processo de agrupamento dos dispositivos da rede e como atua o monitoramento entre eles, além da forma como ocorre a identificação dos atacantes. A Seção 4.3 demonstra o funcionamento do CONFINIT e o uso das abordagens de consenso e *Watchdog* na mitigação do ataque IDF.

4.1 VISÃO GERAL

O CONFINIT atua como um *middleware* em uma rede IoT densa, contribuindo para a segurança do serviço de disseminação de dados contra a presença de ataques de intrusão, como o ataque IDF, que visa deteriorar o funcionamento da rede. Para isso, o CONFINIT se fundamenta na vigilância (monitoramento) *watchdog* entre participantes para detectar anomalias na rede, e usa uma técnica de **consenso colaborativo** para tomada de decisão. O uso dessas técnicas visa criar uma filtragem colaborativa precisa e dinâmica. O objetivo do mecanismo é garantir a autenticidade e disponibilidade dos dados disseminados na rede IoT para apoiar a tomada de decisões das aplicações atuando como uma terceira linha de defesa da rede. Neste trabalho, assume-se que os dispositivos presentes na rede passaram por algum tipo de mecanismo de controle de acesso, o que garante a autenticidade e legitimidade das ações dos nós dentro da rede IoT. Logo, a partir destas informações o mecanismo pode atuar de forma efetiva em uma rede como a IoT. Inicialmente, descreve-se o modelo de rede, de agrupamento e disseminação, e o comportamento do ataque IDF. Em seguida, detalham-se os componentes da arquitetura do CONFINIT e seus algoritmos, bem como o seu funcionamento.

4.1.1 Modelo de rede IoT densa

O modelo da rede IoT densa proposto baseia-se no apresentando em (Cervantes et al., 2018), além de considerar a Seção 2.1.2, onde são considerados diferentes dispositivos, e pode ser definido por um conjunto C de n nós denotados por $C = \{n_1, n_2, n_3, ..., n_n\}$, onde $n_i \in C$. Cada nó n_i tem um endereço físico exclusivo (Id), que o identifica na rede. Assume-se que os nós participantes da IoT exercem suas funções de coleta e disseminação de dados conforme os ambientes onde estão inseridos, o que define também o tipo e a frequência de dados transmitidos. Essas características determinam o tipo de nós que integram a rede: esses nós podem ser fixos ou móveis, apresentar ou não restrições de energia, processamento e armazenamento. Os nós em uma rede como IoT densa tendem a formar grupos para melhorar a organização da rede, economizar recursos, otimizar a comunicação entre os participantes e aumentar a duração do funcionamento da rede. O modelo de rede é ilustrado na Figura 4.1, definido em uma estrutura de três níveis, no qual o primeiro nível compõe os objetos IIoT, o segundo nível realiza a comunicação entre os dispositivos e o terceiro nível coordena a formação dos agrupamentos.

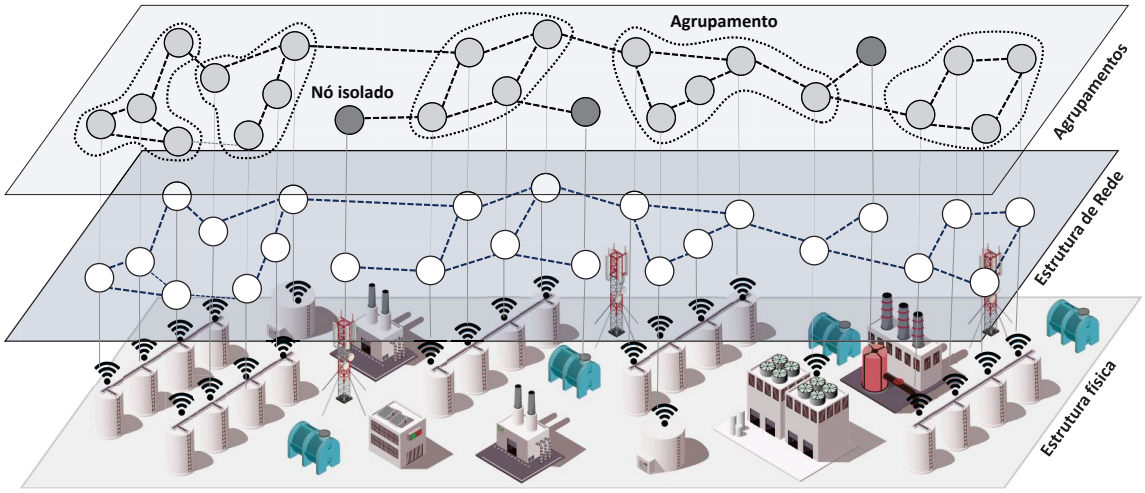


Figura 4.1: Modelo de rede

Os agrupamentos são formados conforme a similaridade entre os dados coletados pelos nós participantes da rede e formam o subconjunto $A_\alpha \subseteq N$ de nós; $\forall\, n_j \in N$. Para a formação dos agrupamentos, são considerados grandezas como espaço e tempo entre os nós. O espaço está relacionado à condição de estarem fisicamente próximos. O tempo refere-se ao momento em que os nós compartilham similaridades entre seus dados. Desta forma, cada agrupamento será formado em função de interesses comuns entre os nós e por sua proximidade física, o que viabiliza uma comunicação direta entre eles. Todos os nós começam como nós isolados, buscando vizinhos para formarem os agrupamentos, podendo ou não participar de um agrupamento. Um nó não pode fazer parte de dois agrupamentos simultaneamente, porém na rede podem existir inúmeros agrupamentos formados. Os agrupamentos são formados com base na similaridade dos dados entre os nós, eles devem estar próximos devido ao raio de transmissão. Assim, verifica-se a similaridade de dados entre os nós com relação ao espaço e tempo compartilhados. Essa técnica trata de uma adaptação do modelo desenvolvido por (Gielow et al., 2015). Os nós podem ser identificados como honestos, suspeitos e atacantes. Os nós honestos, quando agrupados, podem assumir dois papéis, o de nó comum ou nó líder. Os nós comuns integram os agrupamentos enviando seus dados em direção aos líderes. Os líderes, por sua vez, são responsáveis por receber os dados e disponibilizá-los à aplicação.

O modelo de rede IoT proposto no trabalho é representado por um grafo temporal. Deste modo, a rede é definida por um grafo $G = (V, E)$, onde o conjunto de vértices representa os nós da rede, e o conjunto de arestas representa as ligações existentes entre os nós. Esta representação aponta para uma rede estática, ou seja, que não apresenta mobilidade entre seus participantes. Nesta proposta, a associação entre os nós ao longo do tempo demanda a integração de dimensões espaciais e temporais aos grafos utilizados, o que implica a utilização de grafos dinâmicos, ou seja, que variam de acordo com as interações dos participantes (Şensoy et al., 2016). A dimensão temporal representa a influência da dinamicidade das leituras entre os nós. Ela impõe que os agrupamentos sejam representados por diversos grafos $G_0, G_1, ..., G_T$, um para cada momento $T = T_0, T_1, ..., T_T$, ao longo do funcionamento da rede. Essas variações são vistas na Figura 4.2, elaborada com base no trabalho de (Sizemore e Bassett, 2017), que ilustra as interações formadas entre os nós ao longo do tempo em uma rede IoT.

A rede IoT gerada pela interação é definida pelo grafo $G = (V, E)$, onde $V = \{A, B, C, D, E, ...M\}$, e, E varia ao longo do tempo, pois para cada instante T há uma grafo G com ligações distintas. A Figura 4.3, adaptada de Sizemore e Bassett (2017), representa os grafos relativos às interações no tempo $T = 1$, onde $G(E_1) = \{(B, H), (L, G), (M, F)\}$. Para $T = 2$, onde há o

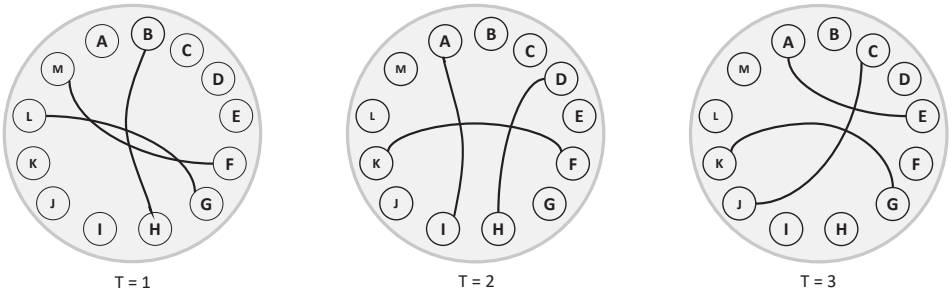


Figura 4.2: Variações das ligações de rede ao longo do tempo

grafo $G(E_2) = \{(A, I), (K, F), (D, H)\}$ para $T = 3$, há o grafo $G(E_3) = \{(J, C), (A, E), (K, G)\}$. Os nós mantêm ligações dinâmicas ao longo do tempo, assim as informações de coletas entre eles determinam quando o agrupamento deve ser continuado ou deve ser desfeito.

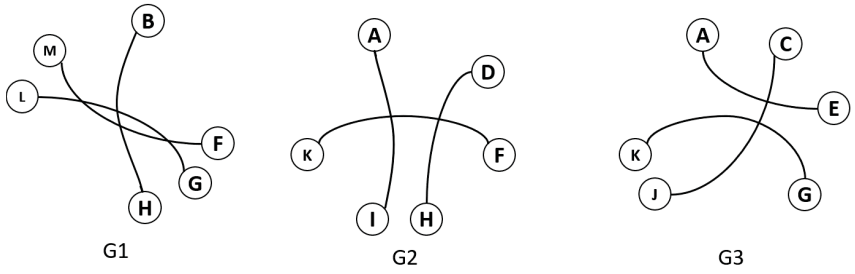


Figura 4.3: Configuração de grafos ao longo do tempo

4.1.2 Modelo de disseminação de dados

Os nós que integram a rede IoT desempenham o serviço de disseminação de dados. Assim, os sensores, atuadores e outros têm a função de coletar e disseminar esses dados, a fim de disponibilizá-los às aplicações para que possam utilizá-los da melhor forma possível. A disponibilização desses dados é fundamental para que aplicações como, por exemplo, as indústrias obtenham integração entre os mais diversos serviços. A viabilização dos dados pode ser executada de forma individual ou em agrupamento. Na primeira forma, os dados são disponibilizados individualmente pelos nós na rede, ou seja, cada nó torna-se responsável por disseminar seus dados até uma central ou a um outro nó da rede. Na segunda forma, os dados podem ser disponibilizados agrupados, ou seja, todos os dados coletados são sumarizados para representar a região onde ele foi coletado. Ambas as formas de disseminação são utilizadas de acordo com a requisição da aplicação onde a IoT está inserida, que determina qual a melhor forma de disponibilizar esses dados. A decisão de como ocorre a disseminação tem influência de fatores como o tipo de dado, a densidade da rede e a frequência com que esse dado é coletado e disponibilizado. O perfil de dado que é disseminado em uma rede IoT pode variar de acordo com o tipo de ambiente onde a IoT está inserida, que pode variar entre dados de texto, video e imagem. Este ambiente também define o fluxo, a quantidade e a frequência com que são coletados e disseminados os dados. Esse dado pode variar entre (texto, número, áudio e vídeo, entre outros), além da criticidade que ele representa. Com o desenvolvimento de novas aplicações, o volume de dados tende a crescer ainda mais e classificar esses dados torna-se uma tarefa não só da aplicação (Bandyopadhyay e Sen, 2011), como também dos dispositivos que o coletam.

O modelo do serviço de disseminação adotado nesta dissertação considera que os nós no início disseminam seus dados em busca de vizinhos para formarem agrupamentos e, dessa forma, disponibilizar seu dados a aplicação. Além disso, os dados coletados são do tipo numérico e o fluxo de dados ocorre de forma contínua e dinâmica. Assim, a disponibilização desses dados considera esses fatores. Devido ao grande volume de dados, a disponibilidade dos dados disseminados ocorre de forma agrupada, e a similaridade entre os dados é o critério para formar os agrupamentos. Logo, apenas os nós que participam de algum agrupamento podem disponibilizar seus dados as aplicações, os demais nós ficam impossibilitados. São consideradas também medidas que visam preservar os atributos de segurança como autenticidade e disponibilidade dos dados coletados. Atender a esses requisitos assegura uma disseminação segura e livre de ameaças, além de atender às demandas impostas pelas aplicações.

4.1.3 Modelo de ataque IDF

A disseminação de dados como qualquer outro serviço de rede IoT está sujeita a diversos tipos de ameaças que buscam interromper a disponibilidade do serviço e assim prejudicar a rede. Dentre essas ameaças está o ataque de injeção de dados falsos (IDF), no qual o atacante, uma vez intruso na rede, apresenta má conduta com características de adulteração, falsificação e fabricação de dados coletados por dispositivos IoT (Yang et al., 2017). Este comportamento pode ferir atributos de segurança como disponibilidade, autenticidade e confiabilidade dos dados transmitidos. O sucesso do ataque IDF afeta diretamente o desempenho da rede IoT, pois redes orientadas a dados necessitam de alta disponibilidade para funcionar corretamente. Desta forma, este trabalho busca criar um mecanismo resiliente ao ataque IDF, assumindo que o atacante tenha total conhecimento sobre a rede e seja capaz de capturar um nó autenticado que esteja exercendo suas funções regularmente. Também se considera que os nós infectados operam de forma individual, ou seja, sem cooperação entre eles, o que acarretaria em uma formação de ataque em conluio.

O modelo de ataque IDF seguido nesse trabalho é baseado no apresentado em (Deng et al., 2016), porém é acrescentada uma extensão do ataque base, pois ele foi proposto para outro contexto de rede. Assim, o ataque pode ser efetuado de duas formas para alcançar seu objetivo. Na primeira forma, o atacante captura um nó N_c autenticado na rede e manipula seus dados, seja alterando ou falsificando-os. Na segunda forma, o próprio N_c é o atacante, o qual executa as mesmas ações com o objetivo de fraudar a rede. Ambos os comportamentos atuam da mesma forma e com a finalidade de gerar diferentes tipos de inconsistências de dados, sobrecarga e degradação da rede. Logo, para simplificar a explicação do modelo, optou-se por usar a primeira forma como modelo principal. Assim, N_c após ter seus dados manipulados inicia a disseminação dos dados falsos a fim de dificultar o processo de formação de agrupamentos da rede.

Esses comportamentos são destacados pela Figura 4.4. Por se tratar de um ataque de intrusão considera-se que o ataque ocorra por meio da exploração de vulnerabilidades decorrentes de outros ataques contra a rede. Esses ataques exploram brechas encontradas e abrem caminhos para que ataques como o IDF acorra. Normalmente os atacantes buscam analisar a rede, entendendo seu funcionamento e dessa forma, realizar um ataque mais efetivo. Além disso, entende-se que para realizar um ataque como esse é necessário que o atacante tenha total conhecimento sobre o modo de operação da rede e tipo de dado trafegado. Esse tipo de comportamento dificulta a identificação da fonte dos ataques, aumenta o tempo de mau funcionamento da rede e gera incoerência sobre os dados disponibilizados. Logo, entender esse comportamento torna-se o maior desafio do mecanismo para mitigação do ataque IDF, pois quanto mais rápida e eficiente for a identificação do atacante, melhor será a recuperação da rede.

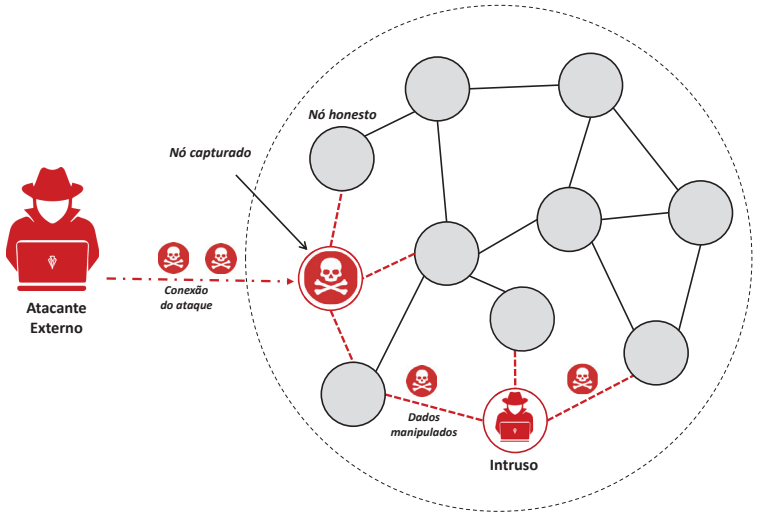


Figura 4.4: Modelo do comportamento dos ataques IDF à rede IoT

4.2 ARQUITETURA CONFINIT

Esta seção apresenta a arquitetura do mecanismo CONFINIT para garantir uma disseminação de dados segura na presença de ataques IDF, bem como o funcionamento do mecanismo. Inicialmente, são descritos os seus componentes, suas características e a operação de cada módulo. Em seguida, detalha-se a formação dos agrupamentos e a decisão de consenso sobre possíveis dispositivos que possam apresentar comportamento malicioso contra a rede.

A arquitetura do sistema CONFINIT é composta por dois módulos, **Gerência Agrupamentos** e **Gerência de Falhas**, como ilustra a Figura 4.5. Ambos trabalham de maneira conjunta e em paralelo para garantir a disseminação segura de dados na rede IoT. O módulo gerência de agrupamentos organiza a rede em *clusters* e o módulo gerência de falhas trata do monitoramento e detecção dos dispositivos da rede e isolamento de ações maliciosas de atacantes IDF.

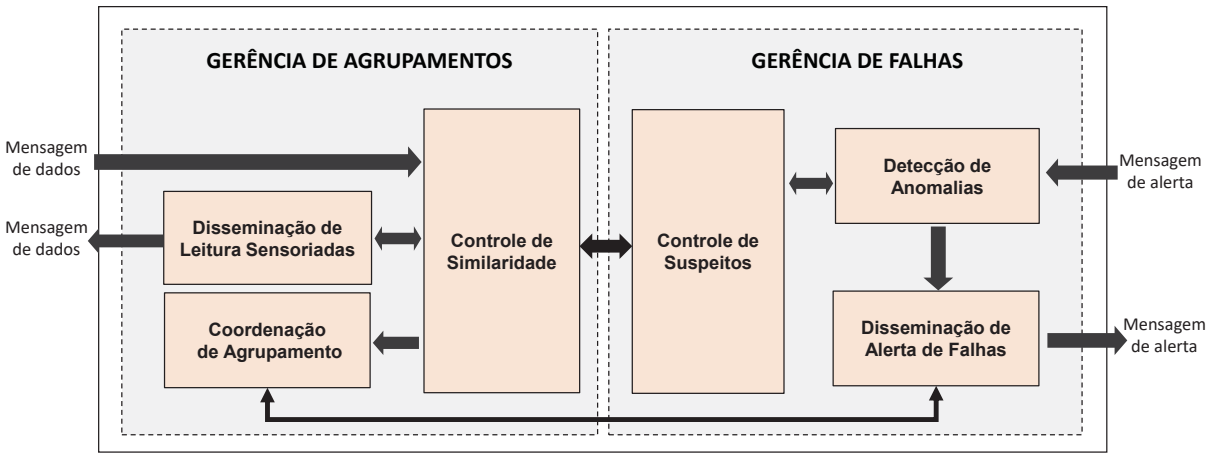


Figura 4.5: Arquitetura do CONFINIT

O **Módulo Gerência de Agrupamentos (MGA)** é responsável pela formação e manutenção dos agrupamentos dentro da rede. Ele forma os agrupamentos com base em um limiar de similaridade de leituras dos dispositivos (nós) que estão próximos e determina quando estão aptos para formar um agrupamento. Assim, ao receber uma mensagem de dados, que será explicado a seguir, ele verifica a identificação, a quantidade de vizinhos e as leituras desses vizinhos. O MGA

é composto pelos componentes de *Controle de Similaridade (CS)*, *Coordenação de Agrupamento (CA)* e *Disseminação de Leitura Sensoriadas (DL)*. O componente CS é responsável por receber e interpretar as mensagens trocadas entre os nós da rede. O componente CA trata de formar e manter os agrupamentos a partir da similaridade dos dados coletados pelos nós, ele também é responsável pela eleição dos líderes. O componente DL é responsável por divulgar sua leitura, quantidade de leituras e vizinhos. Com isso, todos os nós que receberem a mensagem saberão quando fazem ou não parte de um agrupamento. O processo de agrupamento opera de maneira local em cada nó, utilizando-se das leituras que respeitem o limiar de similaridade entre os participantes. Isso por que, cada nó da rede mantém uma visão local da rede, pois uma visão global sobrecarregaria suas funções. A relação de similaridade de dados é expressa em cada par de vizinhos e, a partir do conjunto de pares similares é possível definir de maneira global os agrupamentos aos quais os nós pertencem. A dinamicidade é inerente aos agrupamentos, devido à frequência das leituras que os nós estejam carregando consigo.

O **Módulo Gerência de Falhas (MGF)** garante a segurança da disseminação de dados entre os nós da rede IoT de modo que apenas dispositivos honestos participem de um agrupamento, e disseminem seus dados. Ele consiste dos componentes *Controle de Suspeito (CS)*, *Detecção de Anomalias (DEA)* e *Disseminação de Alerta (DA)*. O componente VS monitora os nós verificando aqueles que não respeitam o limiar de similaridade. O DEA emprega a técnica de consenso colaborativo e desvio padrão para detectar os nós IDF. O consenso é a concordância e uniformidade de opiniões que os nós estabelecem por meio de troca de informações entre eles. O desvio padrão visa determinar quão discrepantes estão as leituras do nó em relação às que estão sendo comparadas. O componente DA atua para isolar os nós atacantes e informar aos demais membros sobre essa ameaça. Logo, quando um ataque é detectado, os nós participantes da detecção propagam um alerta para que os líderes do agrupamento disseminem-o pela rede. Os dados propagados na mensagem de alerta consistem no identificador (Id_{ataq}) e leitura individual (L_{ataq}) do atacante. Esse processo acontece toda vez que um nó é detectado como atacante. Assim, a segurança é mantida pelos próprios participantes da rede sem a necessidade de entidades externas.

Os **tipos de mensagens** periodicamente trocadas entre os participantes da rede IoT podem ser de dados, relacionada à coleta de dados, elas são utilizadas para realizar o controle da rede e formar os agrupamentos. As mensagens de alerta são mensagens de controle sobre as ameaças, elas são disseminadas quando um ataque é identificado e os nós da rede precisam ser informados. A Figura 4.6 ilustra como são compostas cada tipo de mensagem e quais campos são definidos por elas. Dessa forma, quando um nó receber uma mensagem ele será capaz de diferenciá-la e compreendê-la.

MD	Id	L_{ind}	N_{viz}	L_{agr}
MA	Id_{int}	Id_{ataq}	L_{ataq}	

Figura 4.6: Tipos de mensagens

- **Mensagem de dados (MD):** ela é composta por cinco campos; *(i)* o campo (MD) permite diferenciar o tipo de mensagem; *(ii)* o campo (Id) contém o identificador do nó que enviou a mensagem; *(iii)* o campo L_{ind} envolve a leitura individual o nó emissor; *(iv)* o campo N_{viz} identifica o número de vizinhos similares que o nó em questão apresenta; *(v)* o campo L_{agr} é preenchido com as leituras agregadas da vizinhança do nó emissor. Entretanto, deve-se destacar que em um primeiro momento os nós iniciam

suas atividades como nós isolados buscando por vizinhos, dessa forma, os campos N_{viz} e L_{agr} são enviados sem seus campos preenchidos.

- **Mensagem de alerta (MA):** ela é utilizada pelos nós diante da ocorrência de um ataque. Esta mensagem é formada por quatro campos; *(i)* o campo (MA) permite identificar o tipo da mensagem; *(ii)* este campo Id_{int} é preenchido pelo nó que o identificou; *(iii)* o campo Id_{ataq} contém o identificador do atacante na rede; *(iv)* o campo L_{ataq} inclui a leitura individual do atacante.

4.2.1 Módulo gerência de agrupamentos (MGA)

Uma vez que o modelo de rede IoT densa é composto por uma grande diversidade de dispositivos com diferentes características, torna-se um desafio gerenciar e controlar esses dispositivos. Assim, o módulo **Gerência de Agrupamentos** organiza a rede em grupos, com base nos líderes, para criar uma topologia de rede. A técnica de agrupamento é muito utilizada na organização de dispositivos (nós) na rede, melhorando o fluxo de dados, aumentando a escalabilidade, além de estender a vida útil da rede, permitindo uma comunicação mais adequada Gubbi et al. (2013). Inicialmente, os nós começam suas operações de forma isolada, transmitindo e coletando mensagens de dados dos nós vizinhos para composição dos agrupamentos. As transmissões das mensagens são realizadas em *broadcast* a fim de serem escutadas pelos nós que estão próximos fisicamente. As mensagens de dados trocadas entre os nós para formarem os agrupamentos devem conter o (Id) do nó emissor, leitura individual (L_{ind}), número de vizinhos do nó (N_{viz}) e leitura agregada (L_{agr}). Caso alguma das informações não seja recebida pelo nó receptor a mensagem é automaticamente descartada. Assim, as informações são verificadas pelo *Controle de Similaridade (CS)* que realiza o cálculo da similaridade de leituras entre os nós com base nos valores das leituras, quantidade de vizinhos e leituras agregadas desses vizinhos.

O Algoritmo 1 apresenta o funcionamento do controle de agrupamentos. Periodicamente cada nó envia em *broadcast* uma mensagem de controle, informando seu identificador (Id), sua leitura atual ($L_{ind}()$), a média de leitura agregada dos nós com leituras similares em sua vizinhança ($L_{agr}()$) e a quantidade de vizinhos ($N_{viz}()$) ($l.1$-$l.5$). O envio das mensagens leva em consideração um intervalo definido aleatoriamente a fim de evitar transmissões simultâneas entre todos os nós. Ao receber uma mensagem de dados ($l.6$), o nó saberá a origem (org), a leitura individual (iR) do nó emissor, a leitura agregada (aR) de sua vizinhança e a quantidade de nós vizinhos considerados (nR). Inicialmente, o nó atualiza as informações recebidas ($l.7$). As leituras agregadas médias são consideradas para verificar se a leitura do nó atual satisfaz ou não o limiar de similaridade ($l.8$). Assim, a verificação de similaridade é executada na ($l.9$). A vizinhança (N_{viz}) é atualizada incluindo a origem(org) caso o limiar de similaridade seja respeitado ($l.10$) ou removendo o nó caso não ($l.12$). Esse processo ocorre dinamicamente em cada nó da rede, garantindo que todos possam manter sua estrutura de vizinhança atualizada.

A relação de similaridade entre dois nós é calculada com base nos valores dos dados de leitura, além de considerar o valor do limiar entre eles. A Equação 4.1 verifica a similaridade entre duas leituras, seguindo o modelo desenvolvido por Gielow et al. (2015). Em sua composição são atribuídos, às leituras dos nós, a quantidade de vizinhos e as leituras agregadas desses vizinhos, para determinar quando existe similaridade entre dois nós. Na equação 4.1, X representa a leitura atual do nó e Y a leitura com a qual ele está sendo comparado, a fim de verificar com base no limiar de similaridade se satisfazem essa diferença.

$$\left| Y - \frac{X + \sum_{v \in SN_{viz}} (N_{viz}[v].aR * N_{viz}R[v].nR)}{1 + \sum_{v \in SN_{viz}} (N_{viz}[v].nR)} \right| < CThresh \tag{4.1}$$

Algoritmo 1: Estabelecimento dos Agrupamentos

input : Conjunto de nós $N = \{n_1, n_2, ...n_n\}$
output : Decisão de agrupamento $\{org\} \in N_{viz} \ \vee \ \{org\} \notin N_{viz}$

1 **procedure** SendDataMessage()
2 $Send(Id, L_{ind}, L_{agr}, |N_{viz}|)$
3 $WaitIntervalnextmsg$
4 $RControlTimerExpire()$
5 **end procedure**
6 **procedure** ReceiveDataMessage(Org, iR, aR, nR)
7 $N_{viz}[Org] \leftarrow \{iR, aR, nR\}$
8 $localRead \leftarrow L_{agr}()$
9 **if** $(|iR - localRead| < Threshold)$ **and** $(|L_{ind}() - aR| < Threshold)$ **then**
10 $N_{viz} \leftarrow SN_{viz} \bigcup \{org\}$
11 **else if**
12 $N_{viz} \leftarrow SN_{viz} \bigcap \{org\}$
13 **and if**
14 **end procedure**

Paralelo à formação dos agrupamentos, o processo de eleição dos líderes ocorre com base na quantidade de vizinhos. Os agrupamentos podem ser formados com mais de um líder, o que pode acontecer devido ao número de nós integrantes da rede. Ao enviar uma mensagem de dados, o nó que apresentar o maior número de vizinhos em relação aos nós participantes do agrupamento é eleito como líder. Desta forma, todos os nós participantes serão capazes de identificar o líder do agrupamento. Além disso, à medida que os agrupamentos são formados ou desfeitos, o processo de eleição acompanha toda essa dinamicidade. A escolha de um líder visa criar uma hierarquia entre os nós participantes da rede, pois para que os dados sejam disseminados a ponto de ficarem disponíveis às aplicações, esses devem passar pelos nós líderes. A manutenção dos agrupamentos ocorre quando um dos participantes falha ou deixa o agrupamento. Assim, cada nó mantém uma lista de vizinhos que é atualizada à medida que um nó queira participar ou deixar o agrupamento. Essa atualização ocorre devido à periodicidade das mensagens que são trocadas entre os participantes da rede em razão da frequência da coleta de dados.

4.2.2 Módulo gerência de falhas (MGF)

Na formação dos agrupamentos, os nós que não atendem ao limiar de similaridade de leituras em um primeiro momento são considerados suspeitos, passando a integrar uma lista de suspeitos. A utilização da lista se dá pelo fato de apresentar melhor avaliação sobre a detecção de falhas, pois os dispositivos em alguns momentos podem apresentar falhas, o que não caracteriza o comportamento de atacantes. O Algoritmo 2 detalha o funcionamento da detecção de falhas dentro da rede diante de uma ameaça IDF. A detecção passa a atuar efetivamente após a primeira troca de mensagens de dados, visto que os nós necessitam de outras mensagens para fazer comparação. Assim, em um primeiro momento, é analisado se o nó em questão consta na lista de suspeito (l.1-l.7). Caso ele não esteja, mas suas leituras sejam consideradas suspeitas, ele é inserido na lista de suspeitos (l.12). Caso seja verificado que ele consta na lista de suspeitos, mas suas leituras respeitam o limiar definido, ele é removido da lista de suspeitos (l.14).

Algoritmo 2: Detecção de Nós Atacantes

```
input  : Conjunto de nós para consenso C_ni = {c_1, c_2...c_n} ⊂ N, Nó avaliado n_i
output : Decisão sobre n_i avaliado boolean
procedure CheckSuspicious (Id, ConsensusParticipant)
    if(ID ∈ SuspectList & ConsensusParticpant == False)
        return1
    else if(ID ∈ SuspectList & ConsensusParticpant == True)
        return2
    end if
end procedure
procedure CheckAttack(Id, Read)
    Valid ⟵ checkSuspicious(Id, ConsensusParticpant)
    if(Read ≤ Thresholdconsensus)
        Switch ⟵ Valid
            Case 1
            Atklist ← Attacklist ⋃{Id, Read}
            Case 2
            Suspectlist ← Suspectlist ⋂{Id, Read}
        Switch ⟵ Valid
    else
        Suspectlist ← Suspectlist ⋃{Id, Read}
    end if
end procedure
```

A Equação 4.2 descreve o cálculo do consenso para verificar o desvio dos valores aferidos. Para tal, são utilizados os dados de leituras coletados nos participantes do consenso para comparação entre eles e depois validação do nó em questão.

$$DP = \sqrt{\frac{\sum_{i=1}^{n} (X_i - M_A)^2}{N}} \leq Thresholdconsensus \tag{4.2}$$

A Equação 4.2 é utilizada em dois momentos com o objetivo de otimizar a filtragem colaborativa. No primeiro momento, ela utiliza os dados do conjunto $M_c = (c_i, c_{i+1}, ..., c_n)$ que representam as informações da vizinhança do nó receptor, DP que é o valor obtido do desvio padrão, $\sum_{i=1}^{n}$ que, por sua vez, soma todos os valor do conjunto M_c, desde a primeira posição *(i=1)* até a posição $n \in$. O valor de X_i é representado na posição i no conjunto de dados M_c a sere avaliado. A média aritmética dos dados é representada por M_A. N_{mc} representa a quantidade de dados a serem avaliados na equação. No segundo momento, que pose ser observado através da Figura 4.7, a equação utiliza o conjunto $M_A = (x_i, x_{i+1}, ..., x_n)$, que é obtido através da equação empregada entre os nós da região de consenso. $\sum_{i=1}^{n}$ soma todos os valores do conjunto M_A desde a primeira posição *(i=1)* até a posição n do total de nós pertencentes ao consenso. O valor de X_i é representado na posição i no conjunto de dados M_A, que representa a média aritmética dos dados. N_{ma} representa a quantidade de dados a serem avaliados na equação. O *Thresholdconsensus* representa o limiar predefinido para comparação dos valores, ele pode variar de acordo com o tipo de variação dos dados a serem avaliados e o tipo de aplicação que o utiliza. Dessa forma, ele pode ser adaptável a qualquer tipo de variação apresentada pelos dados.

4.2.3 Filtragem Colaborativa

A filtragem colaborativa tem como objetivo identificar os nós maliciosos que buscam fazer parte da disseminação de dados através da formação de agrupamentos. Para isso, é empregado um esquema filtragem que visa garantir em fases quais nós são maliciosos e quais são normais. Desta forma, são utilizados limiares para definir quando um nó é malicioso ou honesto. Essas interações são ilustradas na Figura 4.7, que apresenta o modelo de filtragem colaborativa utilizada pelo CONFINIT e como a Equação 4.2 é aplicada em casa fase. Na primeira fase, ao receber uma mensagem de controle de um nó suspeito, o nó receptor verifica os campos da mensagem. Na segunda, o nó receptor consulta as informações da sua vizinhança para formar o consenso e avaliar o nó em questão. Na terceira fase, é empregada a Equação 4.2, buscando analisar o quão distintos são os dados informados pelo nó. Na quarta fase, a decisão sobre o nó em questão é tomada com base no resultado da equação. Dessa forma, quando um nó não respeita o *Thresholdconsensus* descrito como *Thrsensus* ele é apontado como um nó atacante. Esse modelo de filtragem colaborativa visa atender à dinamicidade da rede, fazendo com que o processo de tomada de decisão seja preciso e distribuído entre os participantes da rede.

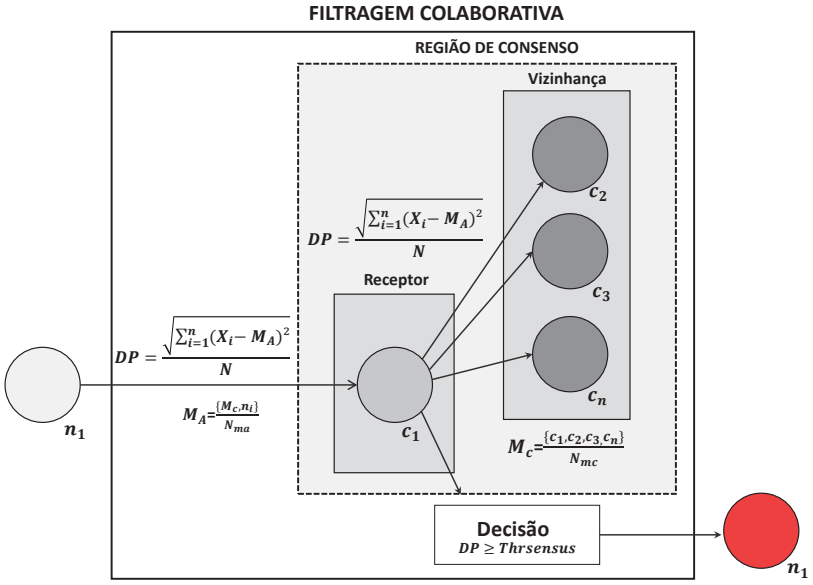


Figura 4.7: O funcionamento da filtragem no CONFINIT

As relações entre as entidades participantes da rede podem ser representadas em diferentes fases de operação do mecanismo, desde a formação dos agrupamentos até a detecção de falhas. Desta forma, uma fase tem relação direta com a outra criando uma colaboração entre os participantes da rede. Além disso, uma fase interfere na outra, pois caso um nó malicioso seja autenticado como honesto ele poderá participar do agrupamento e disseminar seus dados falsos dentro da rede. Essas ações são destacadas por cada componente do mecanismo, criando uma sinergia entre todos. A Figura 4.8 ilustra o processo de interação com base na formação dos agrupamentos e na filtragem colaborativa. No total, o mecanismo é composto por quatro fases relacionadas a atuação dos dispositivos dentro da rede IoT. A interpretação sobre cada fase tem o intuito de criar uma visão geral sobre o processo de tomada de decisão e formação de consenso colaborativo em um conjunto de dispositivos.

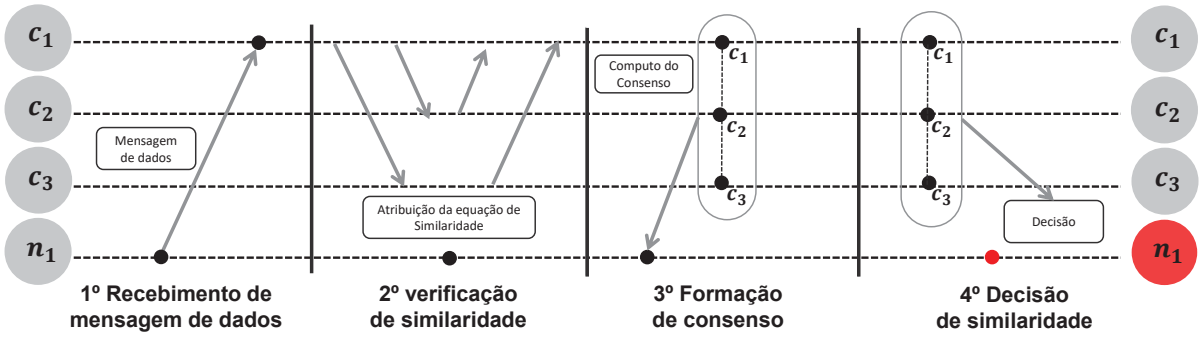


Figura 4.8: Interações entre as entidades durante as fases do CONFINIT

4.3 EXEMPLO DO FUNCIONAMENTO

Esta seção ilustra o funcionamento do CONFINIT atuando na formação dos agrupamentos e na detecção de um ataque IDF em uma rede IoT densa. Suas etapas e passos são descritos a fim de demostrar sua eficácia contra o ataque IDF e a manutenção da disseminação de dados entre os dispositivos participantes da IoT.

4.3.1 Formação dos Agrupamentos

A operação de formação dos agrupamentos acontece de forma dinâmica e variável. Desta forma, as interações entre os nós ocorre sob grandezas de espaço e tempo, ou seja, para que sejam formados os agrupamentos os nós devem estar dentro do raio de transmissão um do outro em determinado tempo e espaço físico. Para isso, cada nó deve periodicamente uma mensagem de dados aos seus vizinhos físicos, em forma de *broadcast* através da camada de rede, informando sua leitura individual, seu número de vizinhos e as leituras agregadas de seus vizinhos. Essas mensagens são recebidas pela verificação de similaridade, que as interpreta e realiza os cálculos com base no limiar de similaridade definido. Assim, cada nó saberá quando pode fazer parte de um agrupamento ou quando deve deixá-lo devido às diferentes leituras. Deste modo, diversos agrupamentos são formados gradualmente de acordo com a similaridade de leituras entre os nós. Paralelamente à formação dos agrupamentos, a eleição dos líderes visa eleger o nó com maior número de vizinhos como líder. Os agrupamentos podem conter mais de um líder, pois dependendo do número de participantes apenas um nó como líder pode não suportar a demanda. Desta forma, os nós podem realizar suas tarefas de coletar e disseminar os dados na rede IoT organizadamente e conhecendo suas rotas até os líderes do agrupamento.

A Figura 4.9 ilustra o funcionamento do CONFINIT na formação dos agrupamentos e eleição dos líderes. Na figura, as arestas sólidas indicam que os nós estão dentro do raio de transmissão um do outro e podem trocar mensagens de dados. As caixas ao lado de cada nó correspondem à estrutura que indica, de cima para baixo, a leitura individual do nó, a leitura agregada sua e de seus vizinhos e a quantidade de leituras agregadas. Cada instante T corresponde à troca de mensagens de dados entre os nós próximos fisicamente e, assim, conseguem verificar quais deles respeitam o limiar de similaridade e podem integrar um agrupamento.

Desta forma, considerando um limiar de similaridade = 3, no instante *T1* os nós iniciam a troca de mensagens de dados buscando atualizar suas lista de vizinhos e leituras agregadas com base na Equação 4.1. Eles iniciam o processo de formação de agrupamentos e eleição dos líderes com base nas leituras obtidas no instante Ra_{T-1}. No instante $T2$, $Ra_{T2}(A) = \frac{15+1*16}{1+1}$, $Ra_{T2}(B) = \frac{16+1*15+1*18}{1+1+1}$, $Ra_{T2}(C) = \frac{18+1*16+1*16+1*16+1*17}{1+1+1+1}$, $Ra_{T2}(D) = \frac{17+1*16+1*18}{1+1+1}$, $Ra_{T2}(E) =$

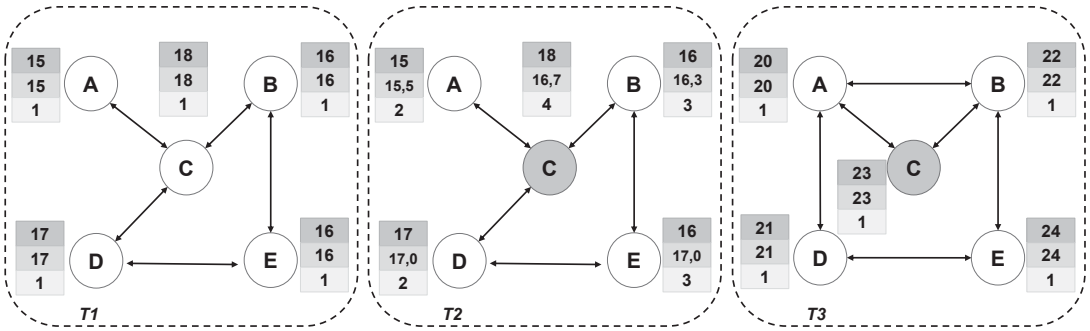


Figura 4.9: Formação dos agrupamentos e eleição dos líderes

$\frac{16+1*17+1*18}{1+1+1}$. Como pode ser observado, após a realização dos cálculos entre o nós, o nó **C** é o que apresenta um maior número de vizinhos, portanto é eleito como líder do agrupamento. A eleição de um líder de agrupamento leva em consideração o número de vizinhos que cada nó dispõem, além disso, um agrupamento pode conter mais de um líder, o que vai depender do número dos participantes contido no agrupamento. Esse modelo de estrutura funciona de forma dinâmica em cada nó e é atualizada conforme as mensagens de dados são trocadas, respeitando o limiar de similaridade. No instante *T3*, a estrutura precisará ser refeita, ou seja, o mesmo processo será aplicado visando manter a formação dos grupamentos, então em os cálculos são refeitos $T3$, $Ra_{T3}(A) = \frac{20+1*22+1*21+1*23}{1+1+1+1}$, $Ra_{T3}(B) = \frac{22+1*20+1*23}{1+1+1}$, $Ra_{T3}(C) = \frac{23+1*22+1*20}{1+1+1}$, $Ra_{T3}(D) = \frac{21+1*24+1*20}{1+1+1}$, $Ra_{T3}(E) = \frac{24+1*21}{1+1}$. Com a gerência de agrupamentos operando desta maneira, cada nó conseguirá manter atualizadas suas informações através da troca de mensagens de dados e saberá quando deve permanecer parte do agrupamento ou quando deve deixá-lo.

Essa estrutura indica quais nós da vizinhança são vistos como membros do mesmo agrupamento e quais não. Logo, apenas os nós com leituras similares que respeitam o limiar de similaridade farão parte do agrupamento. Desta maneira, o reflexo da configuração atual da rede nos agrupamentos é diretamente dependente da troca de mensagens de dados entre os nós, pois para que os agrupamentos se adaptem com maior dinamicidade às constantes mudanças de leitura é possível que esse envio seja controlado. Entretanto, isso vai depender do tipo de aplicação e frequência com que os dados são disponibilizados. Essa organização simples garante melhor escalabilidade à rede, além de facilitar na classificação de nós que estejam com leituras divergentes comparadas aos de seus vinhos espaciais, facilitando a identificação de atacantes pelo módulo de controle de falhas.

4.3.2 Detecção de Falhas

O módulo detecção de falhas de um nó opera considerando a formação dos agrupamentos de acordo com a relação de similaridade entre os participantes. A classificação dos nós que não fizeram parte do agrupamento tem início na mensagem de dados, que sem os campos devidamente preenchidos são descartadas pelos nós. Na formação dos agrupamentos, um nó que está próximo fisicamente de seu vizinho em relação às grandezas e espaço e tempo, e apresenta leituras muito discrepantes que extrapolam o limiar de similaridade, podem ser considerado um nó suspeito em um primeiro momento. Dessa forma, quando ele é identificado como suspeito, ele passa a integrar uma lista de suspeitos, a qual contém nós que apresentam variações muito grandes em relação aos demais nós. No entanto, não são necessariamente atacantes. A lista contém um histórico de leitura anterior, ou seja, o histórico é a última leitura disponibilizada pelo nó através da mensagem de dados. Quando o nó em questão entra para lista de suspeitos e tenta participar do agrupamento, e, novamente, não consegue devido às leituras distintas, ele é classificado

como atacante. Por consequência, tem seu (Id) inserido em uma lista que contém todos os (Ids) das ameaças. Em seguida, o nó que o identificou envia uma mensagem de alerta para o líder do agrupamento informando seu Id, o Id do atacante e a leitura do atacante em questão. Em seguida, o líder do agrupamento dissemina essa mensagem aos outros líderes da rede para que, caso o nó atacante tente se agrupar em outro momento, ele seja impedido.

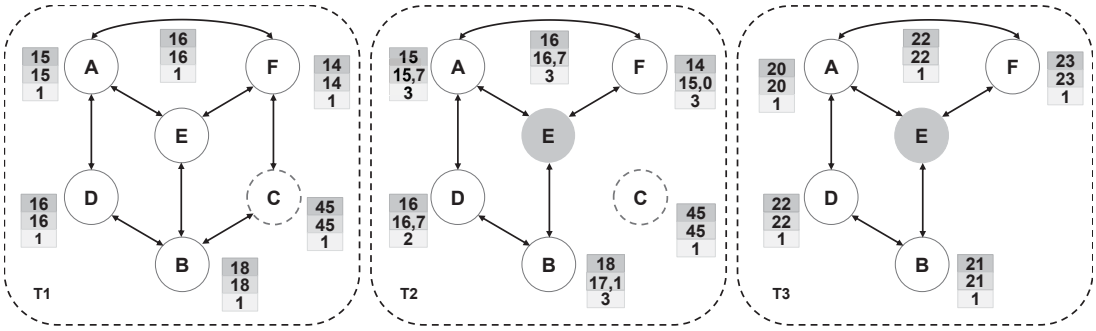


Figura 4.10: Processo de detecção de falhas

A Figura 4.10 ilustra um exemplo do processo de detecção de um nó atacante na rede por parte dos nós do agrupamento. Cada instante T corresponde ao processo de agrupamento, onde os nós que respeitam o limiar de similaridade formam os agrupamentos. No instante *T1*, os nós **(A, B, D, E, F)** estão respeitando esse limiar, porém o nó **C** apresenta um valor de leitura muito discrepante em relação aos seus vizinhos, isto é, não está respeitando o limiar de similaridade. Assim, o nó **C** não pode fazer parte do agrupamento neste momento e passa a integrar uma lista de suspeito. No instante *T2* o nó C tenta novamente agrupar-se e envia uma nova mensagem de dados, essa mensagem é recebida pelo nó A que então aplica a Equação 4.2 em duas partes para avaliar o quanto os dados de C estão variando em relação ao agrupamento. Na primeira parte, A avalia com relação aos seus vizinhos de agrupamento. Na segunda, são avaliados os valores de C com relação aos agrupamentos como um todo. Desta forma, tomado de um *Thresholdconsensus* = 4 a verificação de falhas pode prosseguir. Na primeira parte 4.3, o cálculo segue seis passos. O primeiro passo *(1)* é calcular o valor da média do conjunto de vizinhos, no passo *(2)* obtém-se o valor. Em seguida, no passo *(3)*, o valor é aplicado para efetivar o cálculo do desvio padrão do conjunto. Nos passos *(4)* e *(5)*, é realizada a continuação dos cálculos, e ao final no passo (6), chega-se ao valor de **1,76** entre os nós.

$$DP(1) \leftarrow \begin{cases} (1)\ M_A = \frac{15+16+14+16+18}{5} \\ (2)\ M_A = 15,80 \\ (3)\ \sqrt{\frac{(15-15,80)^2+\ (16-15,80)^2+\ (14-15,80)^2+\ (16-15,80)^2+\ (18-15,80)^2}{5}} \\ (4)\ \sqrt{\frac{(-0,8)^2+\ (0,2)^2+\ (-1,8)^2+\ (0,2)^2+\ (2,2)^2}{5}} \\ (5)\ \sqrt{\frac{(8,8)}{5}} \\ (6)\ 1,76. \end{cases} \tag{4.3}$$

$$DP(2) \leftarrow \begin{cases} (1)\ M_A = \frac{45+15,80}{2} \\ (2)\ M_A = 30,40 \\ (3)\ DP = \sqrt{\frac{(45-30,40)^2+\ (15,80-30,40)^2}{2}} \\ (4)\ DP = \sqrt{\frac{(14,6)^2+\ (-14,6)^2}{2}} \\ (5)\ DP = \sqrt{\frac{(213,16+213,16)}{2}} \\ (6)\ DP = 10,32. \end{cases} \tag{4.4}$$

Na segunda parte 4.4, a sequência da aplicação do cálculo é a mesma, a diferença está nos valores referentes à média do conjunto, comparado ao valor do nó avaliado. Assim, o primeiro passo *(1)* é calcular o valor da média do conjunto de vizinhos, no passo *(2)* obtém-se o valor. Em seguida, no passo *(3)*, o valor é aplicado para efetivar o cálculo do desvio padrão do conjunto. Nos passos *(4)* e *(5)* é realizada a continuação dos cálculos, e ao final do passo *(6)*, chega-se ao valor de **10,32** entre os nós.

Com a obtenção desses valores, é possível compará-los ao *thresholdconsensus* e constatar que **C** é um atacante e não pode fazer parte do agrupamento. No instante *T3*, o nó **C** é retirado da rede e o nó que o detectou dispara uma mensagem de alerta para o líder do agrupamento com o identificador do nó e sua leitura. No caso da detecção ter sido realizada pelo líder, ele dissemina uma mensagem de alerta entre os outros líderes sobre atacante em questão. Com a detecção de falhas trabalhando com essa estrutura simples de monitoramento entre vizinhos, os nós conseguem identificar as ameaças, isolá-las e garantir que elas sejam eliminadas e não consigam participar da disseminação de dados.

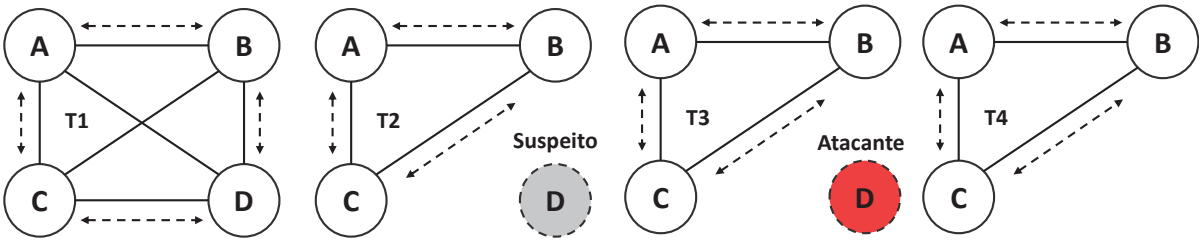


Figura 4.11: Formação de consenso entre os nós

A Figura 4.11 ilustra um exemplo apenas da formação de consenso colaborativo entre os participantes para a detecção de falhas em razão de um atacante IDF. As setas pontilhadas representam a comunicação entre os nós (**A, B, C, D**) no instante *T1*, garantindo assim a troca de mensagem de controle entre eles. Já no instante *T2*, apenas os nós (**A, B, C**) agrupam-se, visto que eles respeitam o limiar de similaridade. Entretanto, o nó **D** não respeita este limiar, então em um primeiro momento é classificado como suspeito. No instante *T3*, o nó **D** envia novamente mensagens de controle para tentar fazer parte do agrupamento e, então, o conjunto formado pelos nós **(A, B e C)** executa o cálculo da Equação 4.2, e classifica o nó **D** como atacante, já que ele novamente apresenta leituras distintas em relação ao conjunto. Por fim, em *T4* apenas os nós honestos fazem parte do agrupamento. Desta forma, a segurança da rede é mantida pelos próprios participantes sem a necessidade de entidade externas.

4.4 RESUMO

Este capítulo apresentou o mecanismo CONFINIT baseado em monitoramento *watchdog* e no consenso colaborativo para a mitigação de ataques IDF em redes IoT. Inicialmente, apresentaram-se os modelos de rede e de disseminação onde o CONFINIT pode atuar, bem como seus componentes. Em seguida, descreveu-se o modelo de ataque IDF e como ele atua no modelo de rede proposto. Então, detalhou-se cada componente da arquitetura CONFINIT para lidar com o ataque. Ao final, detalhou-se o funcionamento do CONFINIT e como ele atua para garantir a disseminação de dados segura em redes IoT densa.

5 AVALIAÇÃO

Este capítulo apresenta uma avaliação da eficácia do CONFINIT na mitigação de ataques IDF contra a disseminação de dados em uma rede IoT. A avaliação considera os resultados obtidos a partir do funcionamento do mecanismo no ambiente de simulação onde ele foi implementado e através das métricas definidas com a finalidade de avaliar a performance do mecanismo. As métricas buscam comprovar a eficácia do CONFINIT na formação de agrupamentos e mitigação do ataque, para garantir uma disseminação de dados segura. A Seção 5.1 descreve a implementação do CONFINIT. A Seção 5.2 apresenta os cenários, suas configurações, e as métricas usadas na avaliação. A Secção 5.3 descreve a validação do CONFINIT juntamente com o protocolo DDFC. A Seção 5.4 apresenta uma análise do comportamento do sistema, e a Seção 5.5 faz uma discussão dos resultados obtidos.

5.1 IMPLEMENTAÇÃO

O CONFINIT foi implementado e avaliado através do simulador de eventos discreto em redes NS- 3 (*Network Simulator 3*) (Consortium, 2001). Este simulador tem sido amplamente usado em estudo de novas soluções em diferentes tipos de redes. O NS-3 é uma ferramenta de código livre baseada nas linguagens C++ e Python. O código-fonte do NS-3 permite realizar modificações em diferentes tipos de protocolos conforme a necessidade do usuário. Em relação a outros simuladores, NS-3 oferece a maior diversidade de redes, coleta de dados relacionada ao seu funcionamento; e as métricas de avaliação podem ser implementadas juntamente com o código de simulação. Além disso, o NS-3 tem suporte aos principais protocolos de comunicação de rede. Essa facilidade possibilita a avaliação em diferentes contextos de redes, inclusive redes IoT.

A versão do NS-3 utilizada foi a 3.28, onde foi implementada uma versão do protocolo de agrupamento DDFC (Gielow et al., 2015), visto que o protocolo DDFC foi inicialmente desenvolvido em uma versão mais antiga do NS-3 a 3.14. Assim, foram necessárias adequações de código para que ele funcionasse na versão mais atualizada do simulador. Além disso, a classe node foi modificada, para incorporar informações dos nós e a lista de suspeitos. Esses novos métodos foram adicionados na classe sem que eles interferissem nos já existentes. Também implementou-se o modelo de ataque IDF baseados no trabalho de (Deng et al., 2016). Neste modelo o atacante busca alterar os dados de uma matriz de leituras de energia e dois tipos de dados são inseridos: um que visa uma pequena alteração e outro que altera completamente o dado coletado. Para melhor se adequar ao cenário desenvolvido, optou-se pela variação dos dados manipulados pelo atacante. Desta maneira, são selecionados randomicamente os nós para atuarem como atacantes IDF dentro da rede. Os atacantes têm total conhecimento sobre os dados trafegados na rede, facilitando sua interação com a rede na manipulação dos valores coletados. Assim, considera-se que os atacantes conseguem manipular os dados ao alterar, falsificar ou mesmo inserir valores distintos aos coletados. Além disso, um nó que em um primeiro momento é considerado suspeito, não necessariamente torna-se um atacante. Isso ocorre pelo fato que um nó poder apresentar apenas uma falha de funcionamento, e essa falha não ser decorrente e um ataque. Logo, chegou-se o mais próximo do comportamento real do ataque IDF.

5.2 CENÁRIOS E MÉTRICAS

As simulações foram realizadas em um mesmo cenário, com diferentes cargas de trabalho. A carga de trabalho é definida conforme o número de nós e porcentagem de ataques efetuados contra a rede. Eles foram em diferentes formas, sem que para cada quantidade de nós presentes na rede, uma porcentagem de ataque foi efetuada. Essas variações nos permitiu observar o comportamento do CONFINIT e seus diferentes comportamentos. Desta forma, pode-se dizer que foram definidos três cenários com diferentes configurações. Assume-se que todos os nós presentes na rede são autenticados, e passaram um controle de acesso prévio.] Nesse controle de acesso prévio, são checadas informações como a identificação do nó, tipo de dados, tipo de informação que ele pode ter acesso, e autorizações. Por fim, diante dos resultados obtidos, a análise dos dados foi realizada através da ferramenta R (Foundation 2018), versão 3.4.4, pelo software RStudio (RStudio, 2018) versão 1.1.414. Os resultados obtidos das simulações correspondem à média de 35 simulações efetuadas para cada cenário, com um intervalo de confiança de 95%.

O cenário desenvolvido visa criar um ambiente mais próximo ao de uma indústria, onde os dispositivos IoT estão sobre os objetos industriais representando o modelo de uma rede IIoT. Esses objetos podem ser variados conforme o tipo de indústria avaliada e seu tipo de função. O objetivo é usar leituras reais, assim, o ambiente de simulação foi baseado na coleta de dados de sensores de pressão de gás coletados em 2008. A coleta desses dados buscou identificar diferentes padrões de comportamento a fim de analisar seus desvios. Os dados utilizados foram coletados e disponibilizados pelo laboratório UCI *Machine Learning Repository* (UCI, 2013) e os *datasets* estão disponíveis no site para análises. A base de dados são de sensores de pressão de gás. Com a utilização desse *dataset* buscou-se chegar a um ambiente mais próximo ao real.

O meio de comunicação adotado pelos dispositivos é o padrão IEEE 802.15.14, utilizado pelo IETF para o chamado 6LoWPAN. O uso do 6LoWPAN foi definido por ser o mais adequado a dispositivos de baixa capacidade, pois o encapsulamento e mecanismo de compressão do cabeçalho possibilita o encaminhamento de pacotes IPV6 com mensagens de 127 *bytes*. Além disso, o protocolo UDP (do inglês, *User Datagram Protocol*) foi escolhido como protocolo de transporte. Desta forma, os dispositivos disseminam seus dados em busca de dispositivos destino com o objetivo de simular uma aplicação industrial em tempo real de uma rede IoT. O ambiente industrial corresponde a um cenário inteligente (*smart industry*), construído em um região de *200m x 200m*. Neste cenário, para cada simulação assume-se uma quantidade de nós fixos, 50, 75 e 100 que estão distribuídos de forma a representar o comportamento dos objetos industriais. Eles operam por *1200s*. Em cada rodada de simulação foram definidos o total de 2%, 5% e 10% de atacantes inseridos na rede buscando deteriorá-la. O raio de transmissão ficou definido em *100m*. A definição do raio de transmissão levou em conta a proporção da área de cobertura para ser definido e não comprometer os resultados obtidos, pois uma maior cobertura poderia interferir na formação dos agrupamentos e do consenso. Os limiar de similaridade foi definido com o valor 3 e o limiar de consenso foi defindo com o valor 5. A definição desses limiares ocorre com base nos valores de leituras obtidos pelo *dataset*. Cabe ressaltar que esse valores podem ser variar de acordo com o tipo de dados e o modelo de aplicação. A área definida buscou representar uma ambiente IoT industrial denso. Pelo *dataset* de dados não disponibilizar o tamanho da área nem um modelo de planta, as definições foram aferidas com base nos trabalho (Cervantes et al., 2018; Kumar e Pais, 2018), além de considerar a classificação apresentada no Capítulo 2 subseção 2.1.2. Com a classificação de trabalhos foi possível determinar o tamanho e quantidade de dispositivos que uma área deve conter para ser definida como densa. Logo, a Figura 5.1 ilustra um modelo de planta industrial com diversos tanques e válvulas de gás, onde os dispositivos

estão sobre os objetos e criam uma interface entre o meio físico e o digital. Esse modelo foi retirado do site bibliocad[1] e adaptado para se adequar ao modelo industrial denso proposto neste trabalho. Esse site oferece diversas bibliotecas de plantas e blocos de CAD e BIM de forma gratuita para que possam ser utilizadas.

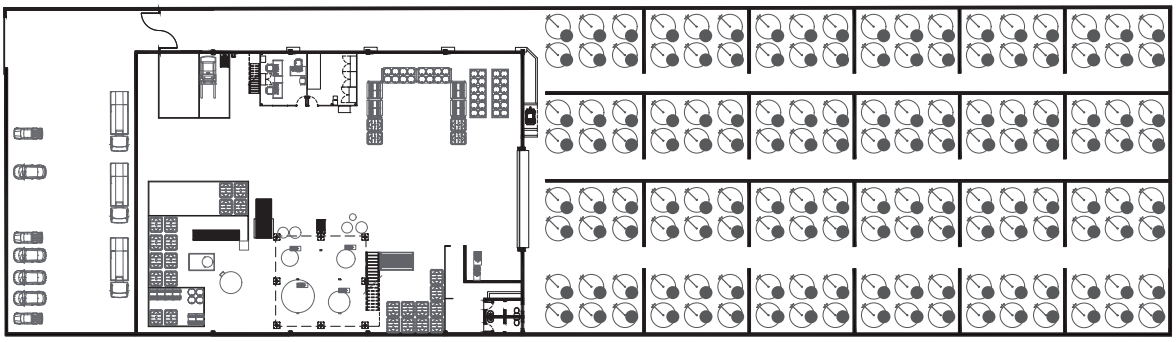


Figura 5.1: Cenário base da simulação

A Figura 5.2 apresenta uma abstração da rede representada através de um grafo. A geração do grafo ocorre pelas relações entre os dispositivos IIoT, onde cada dispositivo representa um vértice e a adjacência entre eles são as arrestas. Com esse modelo, os dispositivos criam relações e estabelecem os agrupamentos com base na similaridade de leituras de dados entre eles e também elegem líderes para esses agrupamentos. Logo, essa representação visa modelar uma rede IoT densa em um contexto industrial.

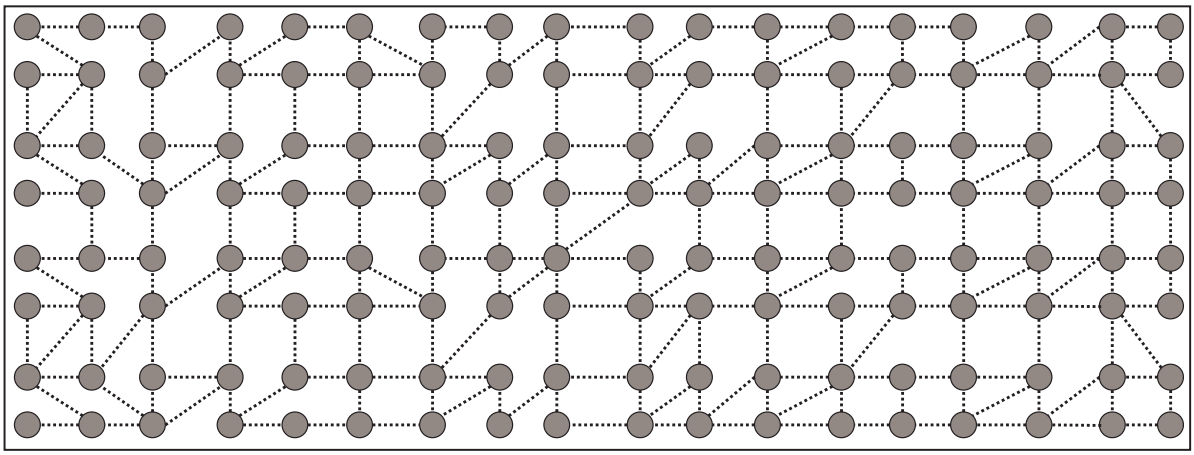


Figura 5.2: Grafo gerado a partir da interação entre dispositivos

A avaliação do CONFINIT ocorreu a partir da análise dos resultados obtidos em simulação por métricas definidas previamente. Elas buscam refletir seu comportamento ao longo do processo de formação de agrupamentos, detecção e isolamento de ataques IDF contra a rede. As métricas escolhidas para avaliar o mecanismo, foram definidas com base nos trabalhos de (Yang et al., 2017; Ferdowsi e Saad, 2019). Essas métricas buscam validar a eficácia e eficiência da detecção, exclusão e o desempenho (custo) e o impacto que o mecanismo representar na rede IoT. Para isso, um conjunto de métricas são descritas e explicadas. A métrica de eficiência considerada é o ***Número de Agrupamentos Formados***, ela avalia quantos agrupamentos são

[1]https://bit.ly/2Z0dUJa

formados ao longo do tempo de simulação em relação a quantidade de nós disponíveis na rede. As métricas de eficácia são descritas abaixo:

- ***Taxa de detecção*** (T_{det}) calcula os ataques de injeção de dados falsos identificados corretamente pelo mecanismo, a partir do consenso entre os participantes. O cálculo da (T_{det}) entende a razão entre o total de detecção (det_{ni}), e a quantidade de ataques inseridos, (A_{ins}), (Eq 5.1). Esta métrica apresenta resultado de valores que podem variar de 0% a 100%, assim quando o valor da taxa for mais próximo de 100% maior será a eficácia do mecanismo.

$$T_{det} = \frac{\sum det_{ni}}{A_{ins}} \tag{5.1}$$

- ***Acurácia*** (R_a) indaga a precisão na detecção do mecanismo, correspondendo ao total do que foi detectado do ataque (det_{ni}), a identificação correta de nós legítimos da rede, (det_{nl}), dividido pelo total de ataques detectados na rede (T_{det}) mais (det_{ni}), (T_{fp}) e (T_{fn}) (Eq 5.2). A (R_a), também resulta em valores discretos, entre 0 e 1, quanto mais próximo de 1 mais precisa é acurácia.

$$R_a = \frac{\sum det_{ni} + \sum det_{nl}}{T_{det} + det_{ni} + T_{fn} + T_{fn}} \tag{5.2}$$

- ***Taxa de Falsos positivos*** (T_{fp}) define a quantidade de vezes que o mecanismo identificou um ataque de injeção de dados falsos quando o mesmo não existia. Seu cálculo se dá através da divisão entre quantidade de detecção, (det_{ni}), é pelo total de interações feitas à rede. (T_{int}), (Eq 5.2).

$$T_{fp} = \frac{\sum det_{ni}}{T_{int}} \tag{5.3}$$

- ***Taxa de Falsos Negativos*** (T_{fn}) calcula o percentual de nós identificados de forma errada como não intrusos. Ela é obtida pela Eq 5.4, onde X é o total de interação, i.e. envio de mensagens de controle e T_{det} a taxa de detecção do ataque.

$$T_{fn} = |X| - T_{det} \tag{5.4}$$

5.3 COMPARAÇÃO DE DESEMPENHO DDCF X CONFINIT

Esta seção apresenta uma avaliação de desempenhos a fim de investigar a atuação do módulo de formação de agrupamentos do CONFINIT. Para isso, utilizou-se o protocolo DDFC para comparação, pois o módulo de formação de agrupamentos do CONFINIT utiliza os mesmos princípios. Ambos são avaliados em relação disponibilização de dados, considerando o número de agrupamentos formados em um cenário de rede IoT densa. Os resultados foram obtidos a partir de 35 simulações para cada cenário; e os gráficos apresentam intervalos de confiança de 95%. Os resultados dividem-se conforme o número de nós presentes na rede.

Os agrupamentos formados por ambos os mecanismos são avaliados conforme a variação de nós presentes na rede (50, 75 e 100). Assim, buscou-se investigar o comportamento dos mecanismos na presença de variações de participantes. Os gráficos da Figura 5.3 apresentam o desempenho do CONFINIT e DDFC na formação dos agrupamentos. É possível observar

que ambos sistemas apresentam um comportamento muito semelhante em relação a formação dos agrupamentos, o que é refletido pelo número de agrupamentos formados por ambos. Essa semelhança acontece devido ao fato do módulo de agrupamentos do CONFINIT ser baseado no DDFC, onde ambos usam a similaridade de leituras como parâmetro para definir os nós que podem ou não participar de alguma agrupamento. Cabe ressaltar que os mecanismo de defesa do CONFINIT não interferem na formação dos agrupamentos visto que a avaliação não inseriu nenhum tipo de ataque. O comportamento dos mecanismo manteve-se estável mesmo variando o número de participantes na rede, essa conduta reforça que ambos são escalares, e podem funcionar perfeitamente com diferentes variações de quantidade de nós na rede.

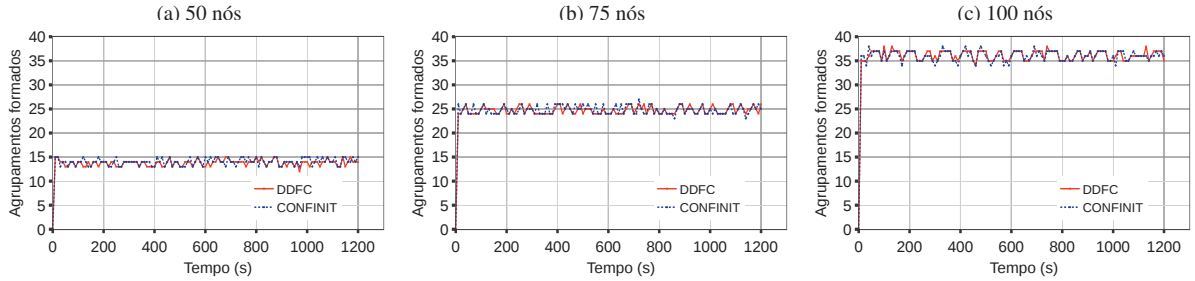


Figura 5.3: Número de agrupamentos formados os longo do tempo DDFC e CONFINIT

No. de nós	DDFC	CONFINIT
50	13	14
75	24	24
100	36	35

Tabela 5.1: Média de agrupamentos formados

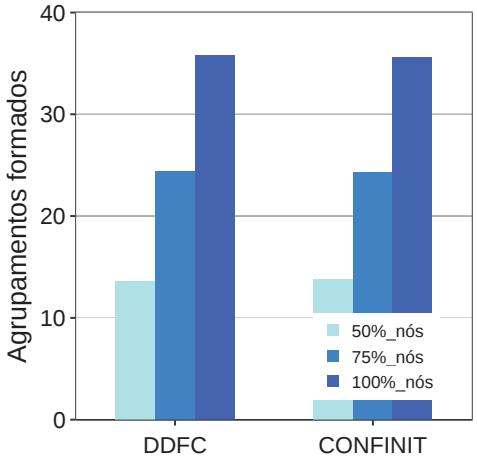


Figura 5.4: Media de agrupamentos DDFC e CONFINIT

Para melhor sintetizar a análise dos resultados sobre o número de agrupamentos, o gráfico da Figura 5.4 apresenta os valores acumulados que ambos os mecanismos obtiveram. Nota-se que os resultados são muito semelhantes, isso *era esperado visto que o CONFINIT é uma extensão do DDFC e utiliza os mesmos princípios. Os valores obtidos de agrupamentos formados podem ser observados na tabela 5.1, nela estão a quantidade de nós inseridos na rede e quanto em médica DDFC e CONFINIT alcançaram. É possível perceber que o número médio de agrupamento é praticamente o mesmo. Isso ocorre devido à quantidade não ser determinística de nós por agrupamentos, ou seja, não existe um número fixo de integrantes por agrupamentos. Com esse comportamento o número de agrupamentos reflete nos dados a serem disponibilizados, pois mais agrupamentos não necessariamente significa mais nós participantes.

5.4 ANÁLISE DO CONFINIT

Esta seção apresenta a avaliação do comportamento e do desempenho do mecanismo CONFINIT quanto aos parâmetros e métricas apresentados em relação a mitigação e disponibilidade dos dados em uma rede IoT densa conforme classificação, para mais detalhes ver Subseção 2.1.2. Os resultados foram obtidos a partir de 35 simulações para cada cenário. Assim, são mostrados nos gráficos intervalos de confiança de 95%. Os resultados apresentados são divididos conforme os cenários avaliados.

5.4.1 Disponibilidade dos agrupamentos

A disponibilidade dos agrupamentos pelo CONFINIT reflete a viabilização dos dados a serem acessados pelas aplicações. Essa disponibilidade é refletida no número de agrupamentos formados, onde mais agrupamentos significa mais dados disponibilizados pelos dispositivos as aplicações.

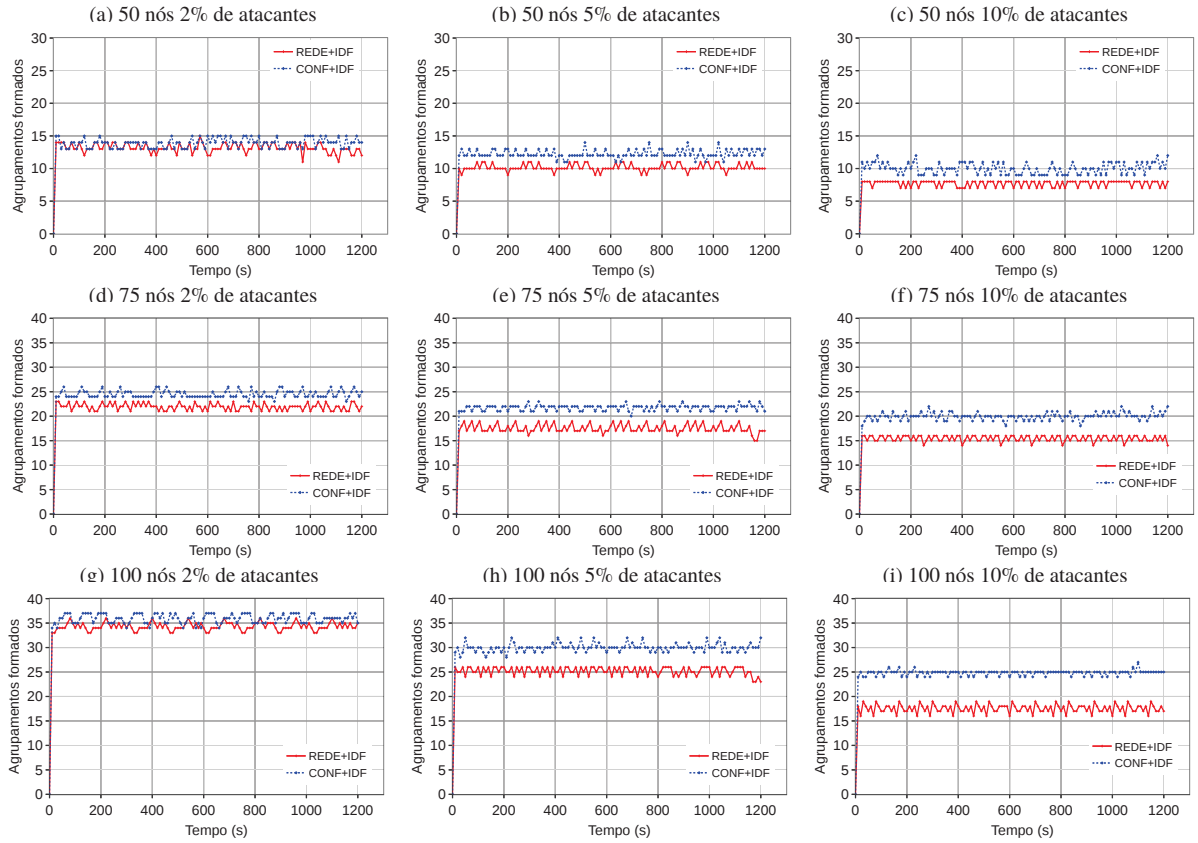


Figura 5.5: Número de agrupamentos formados ao longo do tempo

Dessa forma, a avaliação sobre os agrupamentos considera quantos agrupamentos são formados ao longo do tempo de simulação. Sendo assim, a disponibilização de agrupamentos foi analisada em dois momentos. No primeiro avaliou-se a presença do ataque IDF na rede sem os mecanismos de defesa do CONFINIT, essa avaliação buscou apresentar qual o comportamento da rede em relação ao ataque e como ele interfere na formação dos agrupamentos. No segundo momento, a disponibilidade dos agrupamentos foi avaliada com a presença do ataque e também do CONFINIT, juntamente com seus mecanismos de defesa a fim de comparar ambos os comportamentos. Os gráficos a seguir sintetizam as relações acima citadas, eles são separados considerando o número de dispositivos inseridos na rede (50, 75 e 100) e também a porcentagem

de atacantes (2%, 5% e 10%). Os gráficos da Figura 5.5 apresentam os números de agrupamentos formados ao longo do tempo em relação à quantidade de nós e número de atacantes. Observa-se que a proporção de agrupamentos varia conforme os parâmetros relacionados, assim quanto menor o número de ataques maior é a formação dos agrupamentos. Em relação ao ataque IDF, constatou-se que ele tem impacto direto na formação dos agrupamentos, porém como era esperado, com 10% o número de agrupamentos tem perda considerável e um impacto mais acentuado em relação aos ataques de 2% e 5%. Em alguns casos, o número de agrupamentos sem a presença do CONFINIT chegou a resultar em queda de até 35% na disponibilidade dos dados. Este comportamento afeta a quantidade de dados disponibilizados e, consequentemente, interfere na tomada de decisões. A precisão na formação dos agrupamentos considera o fato do cenário ser estático, isto é, não sofrer com mudanças quanto à posição dos nós. Porém, as leituras apresentam uma variação, quanto aos seus valores de dados coletados. Isto fica evidente nas baixas variações no número de agrupamentos formados ao longo do tempo. Além disso, considera-se a quantidade não determinista de nós por agrupamentos, ou seja, não existe um número fixo de integrantes por agrupamento. Dessa fora, considerando que o ambiente industrial, é importante garantir que os dados estejam disponíveis, pois as aplicações necessitam de diferentes tipos de informações para tomada de decisão em relação ao qualidade da produção, funcionamento de sistemas e qualidade do ambiente, logo esses dados devem ser facilmente acessados.

5.4.2 Eficácia da segurança

A eficácia da detecção do CONFINIT na presença de ataques IDF foi avaliada conforme as métricas selecionadas para ilustrar como a atuação do mecanismo contribui para a segurança da rede. Desta forma, a taxa de detecção (T_{det}), a acurácia (R_a), os falsos positivos (T_{fp}) e os falsos negativos (T_{fn}) foram aplicados e seus resultados podem ser constatados a seguir. Os gráficos da Figura 5.6 apresentam a taxa de detecção (T_{det}) obtida pelo CONFINIT em relação ao número de dispositivos na rede e porcentagem de atacantes inseridos. Observa-se que o mecanismo alcançou um taxa média de 97% de detecção para o ataque IDF. Esse valor representa que em diversos casos o mecanismo foi eficaz em manter a segurança da rede. Além disso, em algumas situações foi possível chegar a uma taxa de 100% conforme o número nós. Essa variação

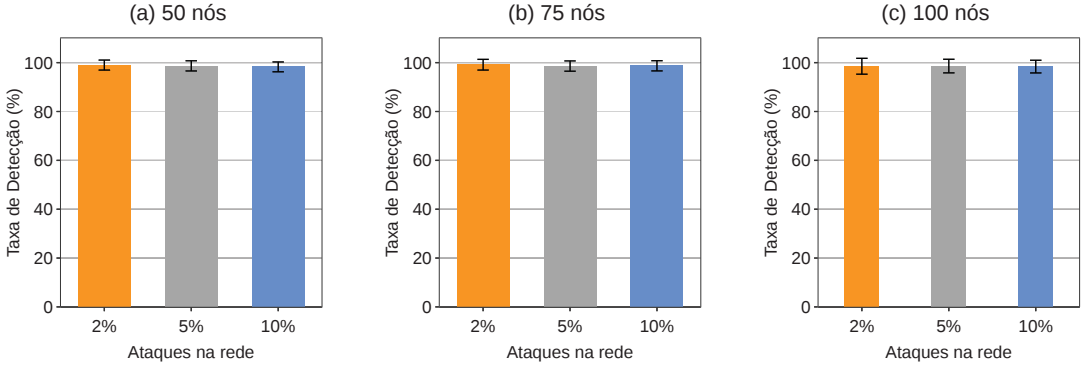


Figura 5.6: Taxas de detecção (T_{det}) para 50, 75 e 100 nós na rede

na taxa detecção acontece devido a densidade da rede, ou seja, quanto mais denso mais eficiente é a detecção de atacantes. Essa efetividade deve-se ao fato da vigilância entre os participantes empregada pela estratégia *watchdog* ser constante. Ela avalia todas as mensagens trocadas entre os participantes a fim de identificar comportamentos anômalos entre os participantes. Esse modelo de vigilância contribui para manter a rede segura pelos próprios dispositivos. Atrelados a esse modelo está a formação de consenso colaborativo que garante uma melhor decisão sobre as ações de atacantes. O consenso atua diretamente na avaliação sobre um dispositivo em

questão, ela utiliza a colaboração entre os participantes para trabalhar de forma distribuída entre todos na rede. O emprego das duas estratégias busca manter a segurança da rede de forma distribuída entre todos que participam dela, os resultados apresentados reforçam a eficácia dessa atuação. A junção dessas estratégias colabora para filtragem colaborativa e aumenta o número de agrupamentos formados, garantindo a disponibilidade apensas de dados verificados. Também observa-se que a taxa de detecção não é influenciada pela variação relacionada à quantidade de nós e porcentagem de ataques, pois o CONFINIT manteve-se estável em todas as variações e demonstrou alta capacidade em lidar com ataque IDF em um ambiente de IoT densa.

Para melhor corroborar com os resultados obtidos pela taxa de detecção do CONFINIT, a avaliação da acurácia é apresentada. Os gráficos da Figura 5.7 demonstram os resultados alcançados pelo mecanismo com base na métrica de acurácia. Deve-se destacar que os valores obtidos da acurácia são discretos e variam de 0 a 1: quanto mais próximo de 1 mais acurado é o mecanismo. O CONFINIT obteve valores para acariciá entre 0,71 e 0,98 o que mostra sua eficácia na detecção. Nota-se que com 100 nós a variação ficou menor que com 75 e 50. Isso é decorrência da filtragem colaborativa, que atua melhor com mais nós presentes na rede. Deve-se destacar que esse valores são favorecidos pelo fato dos nós serem fixos colaborando para uma alta taxa de detecção com baixa variação em relação ao número de nós na rede e atacantes inseridos. Nota-se também que independente do número de nós, variação de resultados é baixa, ou seja, o CONFINIT mantém-se estável e alcança alta eficácia contra o ataque. A alta precisão do mecanismo ocorre pela utilização das estratégias de segurança serem mantidas de maneira continua e distribuída pelos próprios participantes da rede. Esse modelo garante uma maior segurança para a rede. Essa precisão reflete na disponibilidade dos agrupamentos, pois quanto mais precisa a detecção menos dispositivos maliciosos são capazes de participar dos agrupamentos e consequentemente menos dados maliciosos são disseminados as aplicações.

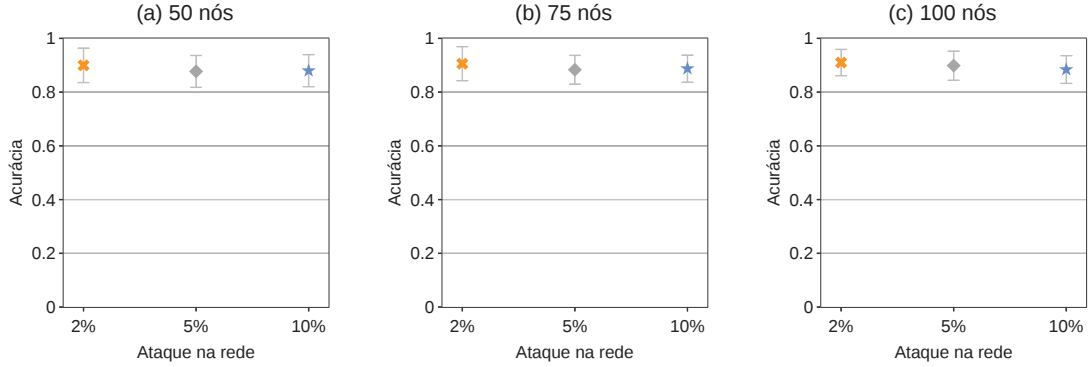


Figura 5.7: Acurácia (R_a) para 50, 75 e 100 nós na rede

Avaliar falsos positivos e falsos negativos representa entender como os resultados tendem a ser influenciados. Como redes sem fio, que envolvem o comportamento de diferentes entidade, essas relações são fundamentais para entender e avaliar diferentes comportamentos. A variações espaciais e temporais devem ser consideradas como parte de avaliações, pois influenciam diretamente relações entre participantes. Nesse sentido, falsos positivos podem ocorrer, assim como falsos negativos e a identificação correta torna-se parte do sistema, pois elas são importantes para mensurar erros na classificação de atacantes pelos mecanismos de segurança. Os falsos positivos retratam os nós legítimos considerados como ameaças e assim impossibilitados de participar dos agrupamentos. Os falsos negativos representam atacantes classificados como nós legítimos e assim não considerados como ameaças a rede e podem participar dos agrupamentos.

Os gráficos da Figura 5.8 apresentam o desempenho do CONFINIT em relação as taxas de falsos negativos na presença do ataque IDF. O CONFINIT obteve uma taxa média de falsos

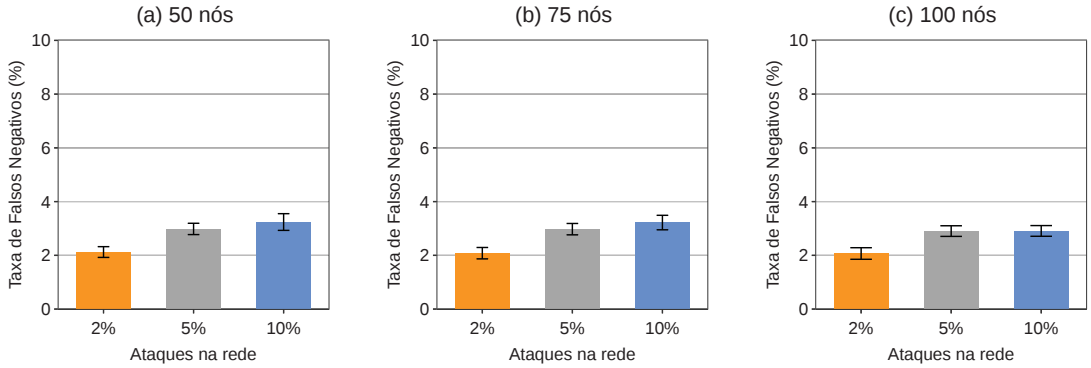


Figura 5.8: Taxas de falsos negativos (T_{fn}) para 50, 75 e 100 nós na rede

negativos variando de 2% para 2% de atacantes e 3,2% para 10% de atacantes. A diferença média entre os cenários ficou em 1,2%, representando uma baixa variação entre eles. Isso demonstra que poucos nós atacantes não são detectados pelo CONFINIT independentemente da quantidade de nós presentes na rede. Além disso, quanto maior a inserção de atacantes na rede a taxa de falsos negativos tende a crescer. Isso acontece pelo fato da vigilância ser colaborativa e, em alguns casos, pode ser comprometida por algum atacante presente. A falha na detecção de um atacante pode acontecer quando há um erro no cálculo da similaridade, e o nó é indicado como suspeito; e portanto a fase de consenso acaba por identificar de maneira errada esse nó como atacante. Assim, os nós da rede podem demorar a identificar um atacante e comprometer a detecção.

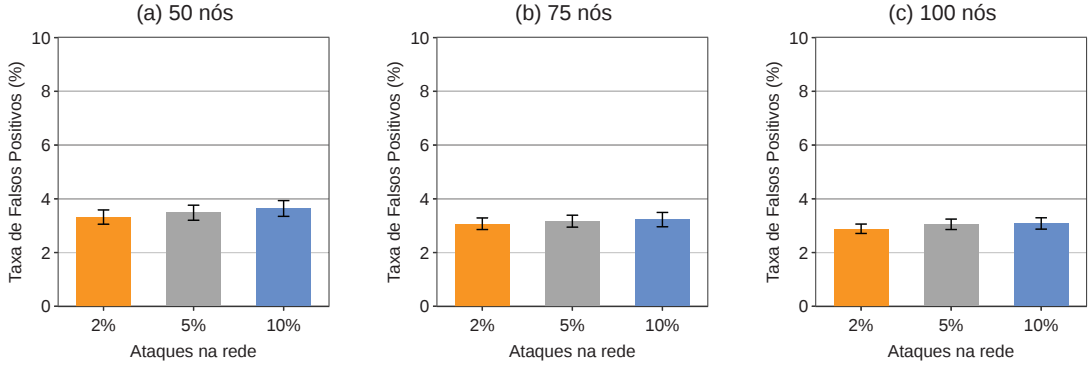


Figura 5.9: Taxas de falsos positivos (T_{fp}) para 50, 75 e 100 nós na rede

As taxas de falsos positivos podem ser observadas pelos gráficos da Figura 5.9. O CONFINIT obteve uma taxa média variando de 2,8% para 2% de atacantes e 3,6% para 10% de atacantes. A diferença média percentual entre os cenários ficou em 0,8%, apresentando uma baixa variação entre eles. Essa baixa variação ocorre devido ao nós serem estáticos, facilitando a detecção correta de atacantes. Esses valores, quando destacados, reforçam a tese de baixa taxa de falsos positivos, entretanto reforçam a necessidade de alguns ajustes serem feitos para melhorar parte do mecanismo. Esses ajustes seriam importantes pois dependendo da aplicação é importante que todos os participantes da rede consigam disponibilizar seus dados. Porém, ajustes assim estão relacionados os tipos de dados coletados e a forma como são disponibilizados. As detecções erradas também podem ser decorrentes de erro no monitoramento cálculo do consenso entre os participantes, que podem identificar um nó legítimo como atacante baseado pequenos desvios nos valores de leitura. Logo, num primeiro momento, eles são considerados suspeitos, porém conforme as novas interações e a troca de mensagens entre os nós vão acontecendo, os novos cálculos identificam os nós corretos. Nota-se também que o número de nós presentes na rede não tem tanta influência nos resultados, pois a variação de um cenário para outro é muito

pequena. Entretanto cabe ressaltar que quanto maior for o número de dispositivos participantes na rede maior tende a ser a taxa de falsos positivos resultante. Além disso, quanto menor for o número de atacantes presentes mais eficaz é a detecção que automaticamente garante menores taxa de falsos positivos ao mecanismo.

5.5 DISCUSSÃO

Os resultados obtidos por simulação demonstraram a eficácia e a eficiência do CONFINIT na detecção e mitigação do ataque IDF e a garantia de disponibilidade de apenas dados legítimos serem disseminados pela rede. Assim, são utilizados parâmetros e métricas que foram definidos e descritos na Seção 5.2, sendo que todas as variações buscou-se o mesmo objetivo de avaliar a eficiência do mecanismo. Em todo processo de simulação foi constatado que a disponibilidade dos dados sempre ocorreu de forma controlada, reforçando a atuação do CONFINIT na formação dos agrupamentos e segurança da rede. Assim, a disponibilização dos agrupamentos atuou visando manter agrupados apenas nós classificados como honestos e o controle de falhas atuou na identificação de atacantes e seu isolamento. Assim, sempre que um nó era identificado como atacante ele era avaliado pelos nós vizinhos, que formavam um consenso colaborativo com o intuito de avaliar a condição do nó em relação a sua vizinhança. Caso ele fosse definido como atacante era isolado da rede e as informações sobre ele eram disseminadas pela rede a fim de evitar novas tentativas de participar de algum agrupamento. Dessa forma simples, a segurança é mantida pelos próprios participantes da rede de forma distribuída e escalável.

A avaliação da taxa de detecção obtida pelo CONFINIT mostrou que é possível lidar com a dinamicidade e densidade da rede de ao mesmo tempo manter a segurança diante de ataques IDF. Também reforça que um monitoramento e decisão colaborativos são capazes de manter a segurança da rede de forma satisfatória, possibilitando o crescimento da rede em número de participantes. Quando trata-se de redes sem fio com varias relações entre diferentes entidades, a presença de falsos positivos e falsos negativos são constante e devem ser consideradas. Isso ocorre pelo fato do mecanismo ser empregado em todos os participantes, ou seja, a colaboração pode ser benéfica no sentido de detecção, porém quando não se utiliza de forma tão precisa erros são ocasionados. Esses erros podem ser caracterizados com as taxa de falsos positivos e falsos negativos e tendem a ser minimizados quando aplicados na precisão que o mecanismo apresenta. Isso ocorre devido ao monitoramento acontecer de forma distribuída entre os nós, onde eles podem identificar um nó incorretamente que possibilita o surgimento de problemas na disponibilização dos dados.

A colaboração entre os nós está atrelada diretamente a relação de similaridade que ambos partilham, nesse caso similaridade de leituras que os nós partilham mediante a troca de mensagens entre eles. Essa relação é ligada diretamente ao monitoramento, das mensagens trocadas, pois são elas que determinam quando um nó pode ou não fazer parte do agrupamento. Assim, caso um agrupamento seja formado apenas por nós maliciosos, pode ser acarretado o problema de conluio e assim levar a falhas na interpretação dos dados. Entretanto, nesse primeiro momento não foi avaliado esse comportamento de ataque. Esse problema reforça que para uma detecção colaborativa ocorrer, ela necessita de um grupo de dispositivos honestos capazes de avaliar e decidir sobre uma ameaça em questão. Nota-se que essa é uma estrutura altamente capaz de manter a disponibilidade de dados frente a ataques IDF que uma vez bem ajustada aos padrões da aplicação tende a ser eficiente na disponibilização dos dados e eficaz na segurança contra atacantes.

5.6 RESUMO

Este capítulo apresentou a metodologia de avaliação e a validade dos resultados obtidos pelos mecanismo CONFINIT, a fim de mensurar sua eficiência e eficácia em garantir a disseminação de dados em redes IoT densa. Os resultados obtidos são reforçados através das métricas definidas e demonstram a capacidade do CONFINIT em mitigar o ataque IDF e garantir a disponibilidade e autenticidade do serviço de disseminação de dados. A disponibilidade dos agrupamentos formados pelos dispositivos foi verificada. Os cenários foram avaliados de modo que o mecanismo pudesse ser testado em diferentes situações impostas por diferentes cargas de trabalho. Além disso, os resultados foram discutidos e analisados para melhor entender o mecanismo. O CONFINIT mostra uma alternativa viável para lidar com ataques IDF na disseminação de dados em uma rede IoT densa em um contexto industrial.

6 CONCLUSÕES

A Internet das Coisas (IoT) tem evoluído rapidamente e transformando-se em realidade. Esse desenvolvimento vem acontecendo pela integração de diferentes tipos de dispositivos, padronização de novas tecnologias de comunicação e agregação de novas conceitos. Essa evolução tem permitido ampliar vários domínios de aplicação, onde destaca-se o industrial. A IoT quando aplicada no contexto industrial caracteriza-se por ser denominada Internet das coisas industriais (IIoT), que compreende os objetivos inseridos em uma indústria. A IIoT trabalha com interface do meio físico para o digital, disponibilizando as informações coletadas pelos objetivos. Entretanto, por ser um domínio onde a quantidade de informações geradas representa um grande volume de dados a ser interpretado pela aplicação. Porém, questões relacionadas a segurança da rede ainda necessitam de definições, representando um desafio para a implementação da IIoT. Esses desafios estão ligados principalmente com a disponibilidade e autenticidade dos dados disseminados, pois quando comprometidos podem gerar irregularidade nas interpretações por parte das aplicações. Ataques como o IDF aproveitam-se de vulnerabilidades encontradas na rede para lançar ataques capazes de modificar, falsificar ou injetar novos dados nos dispositivos, desta forma quebrando atributos de segurança.

A literatura tem apresentado diversas abordagens que buscam lidar com os ataques IDF em diferentes contextos de rede. Todavia, a grande maioria dos trabalhos são propostos para RSSF, e apenas um apresentado para contexto IoT. Desta forma, os trabalhos encontrados foram categorizados através das técnicas por eles utilizados. Dentre as técnicas destacam-se as filtragens em rota, as baseadas em agrupamentos, que são as mais relevante para lidar com o ataque e encaixam-se no escopo do trabalho. Essas abordagens mostram vantagens e desvantagem ao serem aplicadas. Entre as desvantagens encontra-se o problema de distribuição de chaves, não verificação dos dados, usar de um modelo centralizado para detecção, além de não identificarem a fonte do ataque. Logo, detectou-se a necessidade de novas soluções com eficácia na detecção de ataques IDF a partir da identificação da fonte com base em suas informações num contexto de rede IoT massiva. Assim, levantou-se os trabalhos que empregam monitoramento entre os participantes e aqueles que apresentassem abordagens de consenso colaborativo.

A fim de lidar com esse problema, este trabalho propôs o mecanismo CONFINIT (***CON****sensus Based Data* ***FI****lteri****N****g for* ***I****o****T***) para mitigação de ataques de injeção de dados falsos sobre o serviço de disseminação de dados em rede IoT densa voltada ao ambiente da indústria 4.0. Ele baseia-se na vigilância (monitoramento *Watchdog*) entre participantes para detectar anomalias na rede e usa uma técnica de Consenso Colaborativo para tomada de decisão. O uso dessas duas estratégias fortalece o modelo de filtragem colaborativa, trazendo precisão e dinamicidade para o CONFINIT. O objetivo é garantir a autenticidade dos dados disseminados na rede IoT para apoiar a tomada de decisões das aplicações. Para isso, os nós aplicam uma estratégia de monitoramento *watchdog* para detectar e isolar nós atacantes na rede ao informar sua presença ao nós lideres de agrupamentos.

Uma avaliação da eficácia do CONFINIT, realizada através do simulador NS-3, teve como objetivo analisar e determinar a sua capacidade em mitigar ataques IDF no serviço de disseminação de dados. O CONFINIT obteve uma taxa de detecção de 97% e em alguns casos chegou a 100% para certos cenários. Os resultados alcançados demonstram que ele é adequado para lidar com o ataque IDF em redes IoT densa voltada ao contexto industrial. Particularmente, esse resultado é corroborado pelos baixos valores de taxas de falso positivo e falso negativo apresentados, contribuindo para a alta taxa de acertos pelo mecanismo. Esse modelo de segurança

colabora para disponibilidade dos agrupamentos formados. Assim, o número de agrupamentos tende a subir e sempre se manter estável, garantindo uma maior disponibilidade dos dados gerados pelos dispositivos IoT. Esses dados disponíveis favorecem o acesso de aplicações assegurando um tomada de decisão mais precisa sobre serviços com base nos dados analisados.

Para que o serviço de disseminação de dados possa funcionar corretamente em uma rede IoT massiva, ele deve ser livre de ameaças que busquem degradar sua disponibilidade. Desta forma, conclui-se que para garantir uma disseminação segura frente a ataques como o IDF deve-se fornecer mecanismo capazes de detectar e isolar o ataque. Esse objetivo foi alcançado pelo CONFINIT, visto que ele contra a disseminação de dados através da formação de agrupamentos seguros e disponibilizando os dados para que as aplicações possam acessá-los. Esse controle ocorre na forma de que apenas os dados dos agrupamentos são disponibilizados, ou seja, para que um atacante consiga disseminar seus dados ele deve participar de um agrupamento. Dessa maneira, este trabalho contribui com um estudo das principais abordagens empregadas na literatura para lidar com o ataque, explorar como as abordagens de consenso colaborativo e vigilância *watchdog* podem ser alternativas robustas para lidar com o ataque IDF.

6.1 TRABALHOS FUTUROS

A evolução da pesquisa desta dissertação possibilita a investigação de novas questões a serem avaliadas, visto que o constante desenvolvimento da IoT que pode ser explorado em diferentes frentes. Assim, grande parte dessa demanda dos sistemas e serviços exigem preocupação com a segurança dos dados gerados pelas aplicações. Manter esses dados seguros torna-se uma tarefa de constante evolução, pois ao mesmo tempo que os mecanismos de segurança avançam os atacantes também. Portanto, os mecanismos ou protocolos para IoT devem ser robustos e adaptáveis frente à dinamicidade da IoT e suas características de infraestrutura. A IoT vem ampliando seu escopo de atuação e promovendo o surgimento de novas aplicações em diferentes setores. Logo, a disseminação deve-se manter segura seja qual for o contexto da IoT. Desta forma, pretende-se desenvolver novas investigações sobre a presente pesquisa, pois acredita-se que muitos questionamentos e análises ainda podem ser realizados sobre o CONFINIT observando diferentes aspectos do funcionamento e qualidade das ações. Abaixo, detalha-se de modo mais claro as questões a serem investigadas:

1. **Resiliência para aplicações de grande volume de dados:** desenvolvimento de estudo e análise do funcionamento do CONFINIT em diferentes aplicações que lidam com um grande volume de dados, e esses dados apresentam variações em relação ao seu fluxo, divulgação e tipo de dados. Além disso, conforme a aplicação outras questões podem ser avaliadas, como mobilidade, consumo energético e outros tipos de ataques.

2. **Eficiência energética sobre qualquer situação de funcionamento:** analisar o impacto do CONFINIT na questão de consumo de recursos, buscando identificar pontos que possam contribuir para melhorias em relação consumo de recursos dos dispositivos que possam torná-lo mais eficiente em relação aos outros mecanismos de segurança. E consequentemente melhorar a inteligência do mecanismo na tomada de decisão pode contribuir para um número maior de atacantes detectados.

3. **Robustez a comportamentos de má conduta em coluio:** avaliar o CONFINT conta o ataque IDF em conluio que representa uma ameaça ainda mais relevante contra redes orientadas a dados com a IoT. A atuação do ataque IDF em conluio representa um grande desafio, pois trata-se de uma forma sincronizada entre diferentes dispositivos

para atacar simultaneamente a rede. Por fim, explorar a atuação do CONFINIT em outros aspectos de linhas de defesa, como a preventiva, pode ser uma alternativa mais robusta para lidar com diferentes tipos de ataques contra a IoT como *Sybil*, *black hole*, *Sinkhole*, *Selective Forward* e *DDoS*.

Referências

Adat, V. e Gupta, B. (2018). Security in internet of things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, 67(3):423–441.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. e Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376.

Al-Qurishi, M., Rahman, S. M. M., Hossain, M. S., Almogren, A., Alrubaian, M., Alamri, A., Al-Rakhami, M. e Gupta, B. (2018). An efficient key agreement protocol for sybil-precaution in online social networks. *Future Generation Computer Systems*, 84:139–148.

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

Alduais, N., Abdullah, J., Jamil, A. e Audah, L. (2016). An efficient data collection and dissemination for iot based wsn. Em *IEEE Information Technology, Electronics and Mobile Communication Conference (IEMCON), Annual*, páginas 1–6. IEEE.

Almas Shehni, R., Faez, K., Eshghi, F. e Kelarestaghi, M. (2017). A new lightweight watchdog-based algorithm for detecting sybil nodes in mobile wsns. *Future Internet*, 10(1):1.

Alrajeh, N. A., Khan, S. e Shams, B. (2013). Intrusion detection systems in wireless sensor networks: a review. *International Journal of Distributed Sensor Networks*, 9(5):167575.

Arış, A., Oktuğ, S. F. e Voigt, T. (2018). Security of internet of things for a reliable internet of services. Em *Autonomous Control for a Reliable Internet of Services*, páginas 337–370. Springer.

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

Augustine, J., Pandurangan, G. e Robinson, P. (2013). Fast byzantine agreement in dynamic networks. Em *Proceedings of the 2013 ACM symposium on Principles of distributed computing*, páginas 74–83.

Avizienis, A., Laprie, J.-C., Randell, B. e Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on Dependable and Secure Computing*, 1(1):11–33.

Bandyopadhyay, D. e Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1):49–69.

Bennaceur, A., Tun, T. T., Bandara, A. K., Yu, Y. e Nuseibeh, B. (2018). Feature-driven mediator synthesis: Supporting collaborative security in the internet of things. *ACM Transactions on Cyber-Physical Systems*, 2(3):21.

Bertino, E. e Kantarcioglu, M. (2017). A cyber-provenance infrastructure for sensor-based data-intensive applications. Em *IEEE International Conference on Information Reuse and Integration (IRI)*, páginas 108–114. IEEE.

Bhuyan, M. H., Bhattacharyya, D. K. e Kalita, J. K. (2013). Network anomaly detection: methods, systems and tools. *IEEE Communications Surveys & Tutorials*, 16(1):303–336.

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

Botta, A., De Donato, W., Persico, V. e Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, 56:684–700.

Brust, M. R., Frey, H. e Rothkugel, S. (2008). Dynamic multi-hop clustering for mobile hybrid wireless networks. Em *Proceedings of the International conference on Ubiquitous Information Management and Communication*, página 130, New York, New York, USA. ACM Press.

Cai, H., Xu, B., Jiang, L. e Vasilakos, A. V. (2017). Iot-based big data storage systems in cloud computing: Perspectives and challenges. *IEEE Internet of Things Journal*, 4(1):75–87.

Carvin, D., Owezarski, P. e Berthou, P. (2014). A generalized distributed consensus algorithm for monitoring and decision making in the iot. Em *International Conference on Smart Communications in Network Technologies (SaCoNeT)*, páginas 1–6. IEEE.

Cervantes, C., Nogueira, M. e Santos, A. (2018). Mitigação de ataques no roteamento em iot densa e móvel baseada em agrupamento e confiabilidade dos dispositivos. Em *Simpósio Brasileiro de Redes de Computadores (SBRC)*, volume 36.

Cervantes, C., Poplade, D., Nogueira, M. e Santos, A. (2015). Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things. Em *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, páginas 606–611. IEEE.

Chen, B., Wan, J., Shu, L., Li, P., Mukherjee, M. e Yin, B. (2017). Smart factory of industry 4.0: Key technologies, application case, and challenges. *IEEE Access*, 6:6505–6519.

Chung, H., Iorga, M., Voas, J. e Lee, S. (2017). Alexa, can i trust you? *Computer*, 50(9):100.

Colistra, G., Pilloni, V. e Atzori, L. (2014a). The problem of task allocation in the internet of things and the consensus-based approach. *Computer Networks*, 73:98–111.

Colistra, G., Pilloni, V. e Atzori, L. (2014b). Task allocation in group of nodes in the iot: A consensus approach. Em *IEEE International Conference on Communications (ICC)*, páginas 3848–3853. IEEE.

Consortium, N.-. (2001). Ns-3 a discrete-event network simulator for internet system. `https://www.nsmam.org`. Acessado em 21-05-2018.

Da Cunha, M. J., de Almeira, M. B., Fernandes, R. F. e Carrijo, R. S. (2016). Proposal for an iot architecture in industrial processes. Em *IEEE International Conference on Industry Applications (INDUSCON)*, páginas 1–7. IEEE.

Da Xu, L., He, W. e Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 10(4):2233–2243.

Davis, J. J. e Clark, A. J. (2011). Data preprocessing for anomaly based network intrusion detection: A review. *Computers & Security*, 30(6-7):353–375.

Deng, R., Xiao, G., Lu, R., Liang, H. e Vasilakos, A. V. (2016). False data injection on state estimation in power systems—attacks, impacts, and defense: A survey. *IEEE Transactions on Industrial Informatics*, 13(2):411–423.

Dias, J. A., Rodrigues, J. J., Xia, F. e Mavromoustakis, C. X. (2015). A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks. *IEEE Transactions on Industrial Electronics*, 62(12):7929–7937.

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

Ferdowsi, A. e Saad, W. (2019). Generative adversarial networks for distributed intrusion detection in the internet of things. *arXiv preprint arXiv:1906.00567*.

Figueiredo, C. M., dos Santos, A. L., Loureiro, A. A. e Nogueira, J. M. (2005). Policy-based adaptive routing in autonomous wsns. Em *International Workshop on Distributed Systems: Operations and Management*, páginas 206–219. Springer.

Fleisch, E. (2010). What is the internet of things? an economic perspective. *Economics, Management & Financial Markets*, 5(2).

Furlaneto, S. S., Dos Santos, A. L. e Hara, C. S. (2012). An efficient data acquisition model for urban sensor networks. Em *2012 IEEE Network Operations and Management Symposium*, páginas 113–120. IEEE.

Gaona-García, P., Montenegro-Marin, C., Prieto, J. D. e Nieto, Y. V. (2017). Analysis of security mechanisms based on clusters iot environments. *International Journal of Interactive Multimedia & Artificial Intelligence*, 4(3).

Gielow, F., Jakllari, G., Nogueira, M. e Santos, A. (2015). Data similarity aware dynamic node clustering in wireless sensor networks. *Ad Hoc Networks*, 24:29–45.

Gielow, F., Nogueira, M. e Santos, A. (2014). Data similarity aware dynamic nodes clustering for supporting management operations. Em *2014 IEEE Network Operations and Management Symposium (NOMS)*, páginas 1–8. IEEE.

Gonçalves, N. M., dos Santos, A. L. e Hara, C. S. (2012). Dysto-a dynamic storage model for wireless sensor networks. *Journal of Information and Data Management*, 3(3):147–147.

Gonçalves, N. M., Dos Santos, A. L. e Hara, C. S. (2014). A policy-based storage model for sensor networks. Em *2014 IEEE Network Operations and Management Symposium (NOMS)*, páginas 1–8. IEEE.

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

Heinonen, H. (2018). Internet of things booming 15 trillion market. `ttps://medium.com/datadriveninvestor/internet-of-things-booming-15-trillion-market-88fde1da2113/`. Acessado em 12-04-2019.

Herrera-Viedma, E., Cabrerizo, F. J., Kacprzyk, J. e Pedrycz, W. (2014). A review of soft consensus models in a fuzzy environment. *Information Fusion*, 17:4–13.

Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.-L., Iorkyase, E., Tachtatzis, C. e Atkinson, R. (2016). Threat analysis of iot networks using artificial neural network intrusion detection system. Em *International Symposium on Networks, Computers and Communications (ISNCC)*, páginas 1–6. IEEE.

Hug, G. e Giampapa, J. A. (2012). Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks. *IEEE Transactions on Smart Grid*, 3(3):1362–1370.

Illiano, V. P. e Lupu, E. C. (2015). Detecting malicious data injections in event detection wireless sensor networks. *IEEE Transactions on Network and Service Management*, 12(3):496–510.

Itforum365 (2018). Internet das coisas será ainda maior do que onda dos celulares. `https://www.itforum365.com.br/tecnologia/internet-das-coisas-sera-ainda-maior-do-que-onda-dos-celulares/`. Acessado em 12-04-2018.

Jeba, S. A. e Paramasivan, B. (2012). False data injection attack and its countermeasures in wireless sensor networks. *European Journal of Scientific Research*, 82(2):248–257.

Jeba, S. A. e Paramasivan, B. (2013). Energy efficient multipath data transfer scheme to mitigate false data injection attack in wireless sensor networks. *Computers & Electrical Engineering*, 39(6):1867–1879.

Jun, C. e Chi, C. (2014). Design of complex event-processing ids in internet of things. Em *Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference on*, páginas 226–229. IEEE.

Kailkhura, B., Brahma, S. e Varshney, P. K. (2015). Consensus based detection in the presence of data falsification attacks. *arXiv preprint arXiv:1504.03413*.

Keally, M., Zhou, G. e Xing, G. (2010). Watchdog: Confident event detection in heterogeneous sensor networks. Em *Real-Time and Embedded Technology and Applications Symposium (RTAS)*, páginas 279–288. IEEE.

Khan, R., Khan, S. U., Zaheer, R. e Khan, S. (2012). Future internet: the internet of things architecture, possible applications and key challenges. Em *International Conference on Frontiers of Information Technology (FIT)*, páginas 257–260. IEEE.

Khatoun, R. e Zeadally, S. (2016). Smart cities: concepts, architectures, research opportunities. *Communications of the ACM*, 59(8):46–57.

Kim, H.-S., Ko, J., Culler, D. E. e Paek, J. (2017). Challenging the ipv6 routing protocol for low-power and lossy networks (rpl): A survey. *IEEE Communications Surveys & Tutorials*, 19(4):2502–2525.

Ko, J., Lu, C., Srivastava, M. B., Stankovic, J. A., Terzis, A. e Welsh, M. (2010). Wireless sensor networks for healthcare. *Proceedings of the IEEE*, 98(11):1947–1960.

Kouicem, D. E., Bouabdallah, A. e Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, 141:199–221.

Kraub, C., Schneider, M., Bayarou, K. e Eckert, C. (2007). Stef: A secure ticket-based en-route filtering scheme for wireless sensor networks. Em *International Conference on Availability, Reliability and Security, ARES 2007.*, páginas 310–317. IEEE.

Kumar, A. e Pais, A. R. (2017). En-route filtering techniques in wireless sensor networks: a survey. *Wireless Personal Communications*, 96(1):697–739.

Kumar, A. e Pais, A. R. (2018). Deterministic en-route filtering of false reports: A combinatorial design based approach. *IEEE Access*, 6:74494–74505.

Kumar, S. A., Vealey, T. e Srivastava, H. (2016). Security in internet of things: Challenges, solutions and future directions. Em *awaii International Conference on System Sciences (HICSS)*, páginas 5772–5781. IEEE.

Lee, I. e Lee, K. (2015). The internet of things (iot): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4):431–440.

Lee, J., Kao, H.-A. e Yang, S. (2014). Service innovation and smart analytics for industry 4.0 and big data environment. *Procedia Cirp*, 16:3–8.

Li, B., Lu, R., Wang, W. e Choo, K.-K. R. (2017). Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. *Journal of Parallel and Distributed Computing*, 103:32–41.

Li, G. e Znati, T. (2007). Reca: a ring-structured energy-efficient clustering architecture for robust communication in wireless sensor networks. *International Journal of Sensor Networks*, 2(1-2):34–43.

Li, S., Da Xu, L. e Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, 17(2):243–259.

Li, S., Oikonomou, G., Tryfonas, T., Chen, T. M. e Da Xu, L. (2014). A distributed consensus algorithm for decision making in service-oriented internet of things. *IEEE Transactions on Industrial Informatics*, 10(2):1461–1468.

Li, W., Song, H. e Zeng, F. (2018). Policy-based secure and trustworthy sensing for internet of things in smart cities. *IEEE Internet of Things Journal*, 5(2):716–723.

Lima, M. N., Dos Santos, A. L. e Pujolle, G. (2009). A survey of survivability in mobile ad hoc networks. *IEEE Communications surveys & tutorials*, 11(1):66–77.

Lin, J., Yang, X., Yu, W. e Fu, X. (2011). Towards effective en-route filtering against injected false data in wireless sensor networks. Em *IEEE Global Telecommunications Conference (GLOBECOM 2011)*, páginas 1–5. IEEE.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. e Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5):1125–1142.

Liu, Y., Ning, P. e Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 14(1):13.

Loureiro, A. A., Nogueira, J. M. S., Ruiz, L. B., Mini, R. A. d. F., Nakamura, E. F. e Figueiredo, C. M. S. (2003). Redes de sensores sem fio. Em *Simpósio Brasileiro de Redes de Computadores (SBRC)*, páginas 179–226. SBC.

Lu, R., Lin, X., Zhu, H., Liang, X. e Shen, X. (2012). Becan: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 23(1):32–43.

Lu, Y., Papagiannidis, S. e Alamanos, E. (2018). Internet of things: A systematic review of the business literature from the user and organisational perspectives. *Technological Forecasting and Social Change*, 136:285–297.

Luria, M., Hoffman, G., Megidish, B., Zuckerman, O. e Park, S. (2016). Designing vyo, a robotic smart home assistant: Bridging the gap between device and social agent. Em *IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN)*, páginas 1019–1025. IEEE.

Macedo, R., Santos, A., Ghamri-Doudane, Y. e Nogueira, M. (2016). A scheme for ddos attacks mitigation in idm systems through reorganizations. Em *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*, páginas 298–305. IEEE.

Mahmoud, R., Yousuf, T., Aloul, F. e Zualkernan, I. (2015). Internet of things (iot) security: Current status, challenges and prospective measures. Em *International Conference on Internet Technology and Secured Transactions (ICITST),*, páginas 336–341. IEEE.

Mannes, E., Nogueira, M. e Santos, A. (2012a). A bio-inspired scheme on quorum systems for reliable services data management in manets. Em *2012 IEEE Network Operations and Management Symposium*, páginas 278–285. IEEE.

Mannes, E., Nogueira, M. e Santos, A. (2012b). Reliable operational services in manets by misbehavior-tolerant quorum systems. Em *2012 8th international conference on network and service management (cnsm) and 2012 workshop on systems virtualiztion management (svm)*, páginas 343–349. IEEE.

Melo, R., Santos, A., Nogueira, M. e Mehdi, D. (2013). Modelagem e projeto de redes sem fio heterogêneas resilientes e sobreviventes. *Minicursos do XXXI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos (SBRC)*, páginas 1–50.

Mendez, D. M., Papapanagiotou, I. e Yang, B. (2017). Internet of things: Survey on security and privacy. *arXiv preprint arXiv:1707.01879*.

Meng, Z., Wu, Z., Muvianto, C. e Gray, J. (2016). A data-oriented m2m messaging mechanism for industrial iot applications. *IEEE Internet of Things Journal*, 4(1):236–246.

Miorandi, D., Sicari, S., De Pellegrini, F. e Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad hoc networks*, 10(7):1497–1516.

Mo, Y., Garone, E., Casavola, A. e Sinopoli, B. (2010). False data injection attacks against state estimation in wireless sensor networks. Em *IEEE Conference on Decision and Control (CDC)*, páginas 5967–5972. IEEE.

Molano, J. I. R., Lovelle, J. M. C., Montenegro, C. E., Granados, J. J. R. e Crespo, R. G. (2018). Metamodel for integration of internet of things, social networks, the cloud and industry 4.0. *Journal of ambient intelligence and humanized computing*, 9(3):709–723.

Mota, R., Riker, A. e Rosario, D. (2019). Adjusting group communication in dense internet of things networks with heterogeneous energy sources. Em *Anais do XI Simposio Brasileiro de Computacao Ubiqua e Pervasivasiva*. SBC.

Movahedi, Z. e Hosseini, Z. (2017). A green trust-distortion resistant trust management scheme on mobile ad hoc networks. *International Journal of Communication Systems*, 30(16):e3331.

Munir, A., Kansakar, P. e Khan, S. U. (2017). Ifciot: Integrated fog cloud iot: A novel architectural paradigm for the future internet of things. *IEEE Consumer Electronics Magazine*, 6(3):74–82.

Nadeem, A. e Howarth, M. P. (2013). A survey of manet intrusion detection & prevention approaches for network layer attacks. *IEEE Communications Surveys & Tutorials*, 15(4):2027–2045.

Ngu, A. H., Gutierrez, M., Metsis, V., Nepal, S. e Sheng, Q. Z. (2017). Iot middleware: A survey on issues and enabling technologies. *IEEE Internet of Things Journal*, 4(1):1–20.

Nordrum, A. (2018). Internet of Things forecast. https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated. Acessado em 12-04-2018.

Nunes, D. S., Zhang, P. e Silva, J. S. (2015). A survey on human-in-the-loop applications towards an internet of all. *IEEE Communications Surveys & Tutorials*, 17(2):944–965.

Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T. e Ladid, L. (2016). Internet of things in the 5g era: Enablers, architecture, and business models. *IEEE Journal on Selected Areas in Communications*, 34(3):510–527.

Palomares, I., Martinez, L. e Herrera, F. (2014). A consensus model to detect and manage noncooperative behaviors in large-scale group decision making. *IEEE Transactions on Fuzzy Systems*, 22(3):516–530.

Parwekar, P. (2011). From internet of things towards cloud of things. Em *International Conference on Computer and Communication Technology (ICCCT)*, páginas 329–333. IEEE.

Pedroso, C., Gielow, F., Santos, A. e Nogueira, M. (2019). Mitigação de ataques idfs no serviço de agrupamento de disseminação de dados em redes iot densas. *XIX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2019)*, páginas 1–50.

Perera, C., Zaslavsky, A., Christen, P. e Georgakopoulos, D. (2014). Sensing as a service model for smart cities supported by internet of things. *Transactions on Emerging Telecommunications Technologies*, 25(1):81–93.

Potluri, S., Diedrich, C. e Sangala, G. K. R. (2017). Identifying false data injection attacks in industrial control systems using artificial neural networks. Em *IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, páginas 1–8. IEEE.

Pourghebleh, B. e Navimipour, N. J. (2017). Data aggregation mechanisms in the internet of things: A systematic review of the literature and recommendations for future research. *Journal of Network and Computer Applications*, 97:23–34.

Rashid, B. e Rehmani, M. H. (2016). Applications of wireless sensor networks for urban areas: A survey. *Journal of network and computer applications*, 60:192–219.

Rault, T., Bouabdallah, A. e Challal, Y. (2014). Energy efficiency in wireless sensor networks: A top-down survey. *Computer Networks*, 67:104–122.

Roman, R., Alcaraz, C., Lopez, J. e Sklavos, N. (2011). Key management systems for sensor networks in the context of the internet of things. *Computers & Electrical Engineering*, 37(2):147–159.

Rossetti, G. e Cazabet, R. (2018a). Community discovery in dynamic networks: a survey. *ACM Computing Surveys (CSUR)*, 51(2):35.

Rossetti, G. e Cazabet, R. (2018b). Community discovery in dynamic networks: a survey. *ACM Computing Surveys*, 51(2):35.

Sadeghi, A.-R., Wachsmann, C. e Waidner, M. (2015). Security and privacy challenges in industrial internet of things. Em *ACM/EDAC/IEEE Design Automation Conference (DAC)*, páginas 1–6. IEEE.

Saeed, A., Butt, W. H., Kazmi, F. e Khan, M. A. (2018). Evaluation of clustering algorithms for wireless sensor and actor networks. Em *International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, páginas 883–889. IEEE.

Sanchez, L., Muñoz, L., Galache, J. A., Sotres, P., Santana, J. R., Gutierrez, V., Ramdhany, R., Gluhak, A., Krco, S., Theodoridis, E. et al. (2014). Smartsantander: Iot experimentation over a smart city testbed. *Computer Networks*, 61:217–238.

Sen, A. e Madria, S. (2017). Risk assessment in a sensor cloud framework using attack graphs. *IEEE Transactions on Services Computing*, 10(6):942–955.

Şensoy, M., Yilmaz, B. e Norman, T. J. (2016). Stage: Stereotypical trust assessment through graph extraction. *Computational Intelligence*, 32(1):72–101.

Sethi, M., Kortoci, P., Di Francesco, M. e Aura, T. (2015). Secure and low-power authentication for resource-constrained devices. Em *International Conference on the Internet of Things (IOT)*, páginas 30–36. IEEE.

Sethi, P. e Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, 2017.

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

Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T. e Uluagac, A. S. (2018). A survey on sensor-based threats to internet-of-things (iot) devices and applications. *arXiv preprint arXiv:1802.02041*.

Silva, B. N., Khan, M. e Han, K. (2018). Internet of things: A comprehensive review of enabling technologies, architecture, and challenges. *IETE Technical review*, 35(2):205–220.

Sisinni, E., Saifullah, A., Han, S., Jennehag, U. e Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics*, 14(11):4724–4734.

Sizemore, A. E. e Bassett, D. S. (2017). Dynamic graph metrics: Tutorial, toolbox, and tale. *NeuroImage*.

Slabicki, M., Premsankar, G. e Di Francesco, M. (2018). Adaptive configuration of lora networks for dense iot deployments. Em *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, páginas 1–9. IEEE.

Sundmaeker, H., Guillemin, P., Friess, P. e Woelfflé, S. (2010). Vision and challenges for realising the internet of things. *Cluster of European Research Projects on the Internet of Things, European Commision*, 3(3):34–36.

Talyansky, M. e Tumarkin, A. (2018). System and method for optimizing inter-node communication in content distribution network. US Patent 9,866,623.

Toulouse, M., Le, H., Phung, C. V. e Hock, D. (2016). Robust consensus-based network intrusion detection in presence of byzantine attacks. Em *Proceedings of the Seventh Symposium on Information and Communication Technology*, páginas 278–285. ACM.

Toulouse, M., Minh, B. Q. e Curtis, P. (2015). A consensus based network intrusion detection system. Em *International Conference on IT Convergence and Security (ICITCS)*, páginas 1–6. IEEE.

UCI, C. (2013). Estatisticas de acesso web. `https://archive.ics.uci.edu/ml/datasets/Gas+Sensor+Array+Drift+Dataset`. Acessado em 21-05-2018.

Uluagac, A. S., Beyah, R. A., Li, Y. e Copeland, J. A. (2010). Vebek: Virtual energy-based encryption and keying for wireless sensor networks. *IEEE Transactions on Mobile Computing*, 9(7):994–1007.

Vasseur, J.-P. e Dunkels, A. (2010). *Interconnecting smart objects with ip: The next Internet*. Morgan Kaufmann.

Vermesan, O. e Friess, P. (2013). *Internet of things: converging technologies for smart environments and integrated ecosystems*. River publishers.

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

Wang, J., Liu, Z., Zhang, S. e Zhang, X. (2014). Defending collaborative false data injection attacks in wireless sensor networks. *Information Sciences*, 254:39–53.

Wang, Y., Kung, L. e Byrd, T. A. (2018). Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. *Technological Forecasting and Social Change*, 126:3–13.

Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M. e Borriello, G. (2009). Building the internet of things using rfid: the rfid ecosystem experience. *IEEE Internet Computing*, 13(3).

Wu, M., Lu, T.-J., Ling, F.-Y., Sun, J. e Du, H.-Y. (2010). Research on the architecture of internet of things. Em *International Conference on Advanced Computer Theory and Engineering (ICACTE)*, volume 5, páginas V5–484. IEEE.

Yang, L., Ding, C., Wu, M. e Wang, K. (2017). Robust detection of false data injection attacks for data aggregation in an internet of things-based environmental surveillance. *Computer Networks*, 129:410–428.

Yang, X., Lin, J., Yu, W., Moulema, P.-M., Fu, X. e Zhao, W. (2015). A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems. *IEEE Transactions on Computers*, 64(1):4–18.

Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X. e Liu, W. (2011). Study and application on the architecture and key technologies for iot. Em *International Conference on Multimedia Technology (ICMT)*, páginas 747–751. IEEE.

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M. e Guizani, M. (2017). The rise of ransomware and emerging security challenges in the internet of things. *Computer Networks*, 129:444–458.

Ye, F., Luo, H., Lu, S. e Zhang, L. (2005). Statistical en-route filtering of injected false data in sensor networks. *IEEE Journal on Selected Areas in Communications*, 23(4):839–850.

Yu, Z. e Guan, Y. (2010). A dynamic en-route filtering scheme for data reporting in wireless sensor networks. *IEEE/ACM Transactions on Networking (ToN)*, 18(1):150–163.

Zanella, A., Bui, N., Castellani, A., Vangelista, L. e Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things journal*, 1(1):22–32.

Zarpelão, B. B., Miani, R. S., Kawakani, C. T. e de Alvarenga, S. C. (2017). A survey of intrusion detection in internet of things. *Journal of Network and Computer Applications*, 84:25–37.

Zhang, Q., Yu, T. e Ning, P. (2006). A framework for identifying compromised nodes in sensor networks. Em *2006 Secure, Communication and Workshops*, páginas 1–10. IEEE.

Zhang, Y., Yang, J., Vu, H. T. e Wu, Y. (2010). The design and evaluation of interleaved authentication for filtering false reports in multipath routing wsns. *Wireless Networks*, 16(1):125–140.

Zheng, P., Sang, Z., Zhong, R. Y., Liu, Y., Liu, C., Mubarok, K., Yu, S., Xu, X. et al. (2018). Smart manufacturing systems for industry 4.0: Conceptual framework, scenarios, and future perspectives. *Frontiers of Mechanical Engineering*, páginas 1–14.

Zhong, R. Y., Xu, X., Klotz, E. e Newman, S. T. (2017). Intelligent manufacturing in the context of industry 4.0: a review. *Engineering*, 3(5):616–630.

Zhou, P., Jiang, S., Irissappane, A., Zhang, J., Zhou, J. e Teo, J. C. M. (2015). Toward energy-efficient trust system through watchdog optimization for wsns. *IEEE Transactions on Information Forensics and Security*, 10(3):613–625.

Zhou, Y., Huang, T. e Wang, W. (2009). A trust establishment scheme for cluster-based sensor networks. Em *nternational Conference on Wireless Communications, Networking and Mobile Computing*, páginas 1–4. IEEE.

Zhu, D., Yang, X. e Yu, W. (2015). Spais: A novel self-checking pollution attackers identification scheme in network coding-based wireless mesh networks. *Computer Networks*, 91:376–389.