

Provendo Agrupamento Seguro de Dados Similares em Redes IoT Contra Ataques de Injeção de Dados Falsos

Carlos Pedroso¹, Fernando Gielow¹, Michele Nogueira¹, Aldri Santos¹

¹Núcleo de Redes Sem-Fio e Redes Avançadas (NR2) – UFPR
Centro de Ciência de Segurança Computacional (CCSC) – UFPR
Caixa Postal 19.081 – 81.531-980 – Curitiba – PR – Brasil

→ acho que meu email .inf
(capjunior, aldri, fhgielow, }@inf.ufpr.br NÃO Existe Mais

1. Introdução

A Internet das coisas (IoT) possibilita a conexão de diferentes tipos de objetos físicos, através de tecnologias como redes de sensores sem fio (RSSF), RFID, GPS e NFC, entre outras. Os objetos IoT possuem várias características como identidade, atributos físico, heterogeneidade, e muitos deles usam interfaces inteligentes para estabelecerem comunicações entre si, ~~e podem possuir~~ [Gubbi et al. 2013]. A IoT faz parte da evolução de domínios densos e complexos como processos industriais, logística, segurança política e cidades inteligentes, visto que ela é fundamental para coletar, disseminar, e lidar com o volume de dados exigido por diversas aplicações nas suas tomadas de decisões [Minoli et al. 2017, Akpaku et al. 2018].

Contudo, **tratar e disseminar** esse grande volume de dados ~~atrelado~~^{ela} a interação entre diversos dispositivos consequentemente expõe a IoT **densa** a diversas vulnerabilidades. Os ambientes normalmente contam com dispositivos móveis e fixos ~~e~~^A infraestrutura ~~que~~ varia conforme a interação. Parte dos dispositivos têm recursos limitados, pouca

SOPREREM

energia, pouca capacidade de processamento e armazenamento, além de perdas nos links de conexão [Borgia 2014, Qiu et al. 2018]. Logo, a IoT ~~tem sido~~^é alvo de inúmeros tipos de ataques que ~~visam~~ viola~~m~~ atributos de integridade, autenticidade e privacidade dos serviços da rede [Yaqoob et al. 2017, Kouicem et al. 2018], prejudicando a operação das aplicações [Miorandi et al. 2012, Mendez et al. 2017]

Particularmente, entre as ameaças **internas** ao serviço de disseminação de dados na IoT que apoiam~~o~~ as aplicações, destaca-se o ataque de Injeção de Dados Falsos (IDF), considerado~~o~~ um dos ataques **de intrusão** mais nocivo à redes de dados devido à inconsistência das informações geradas e à imprevisibilidade do seu acontecimento [Sen and Madria 2017]. Em razão da sua complexidade, a detecção do ataque torna-se complexa e trabalhosa, ~~isso porque~~^{Pois} normalmente os dispositivos maliciosos estão autenticados na redes e exercem suas funções padrão de coleta e disseminação de dados. Muitas vezes os ataques podem ocorrer~~em~~ em diferentes períodos e penitência de-
sorientando a rede. Por característica, um ataque IDF pode alterar ou fabricar os dados, ~~O atacante pode capturar~~ o dispositivo ou usar~~o~~^{Não} outros dispositivos para injetar dados. Essa ação prejudica o desempenho da rede e quebra atributos de segurança como, pri-
vacidade, integridade e autenticidade [Botta et al. 2016, Chattopadhyay and Mitra 2018]. Esse comportamento dificulta a identificação de dispositivos maliciosos, aumenta o tempo de mal funcionamento da rede e gera ~~uma~~ inconsistência nos dados. Desta forma, torna-
se imprescindível identificar e excluir os dispositivos maliciosos da rede. **Este trabalho**
foca nas duas formas de ataque citadas acima. ~~→ NÃO FICAM CLARAS AS~~

? Interni-
Tentes?

2 FORMAS.

Apesar de diferentes técnicas ~~já~~ s~~ão~~ empregadas para lidar com os ata-
ques IDF, sejam no contexto de RSSF [Lu et al. 2012, Kumar and Pais 2018], Smart
Grid [Li et al. 2017] ou IoT [Yang et al. 2017], ~~mas~~ têm falhados ou não atende~~o~~^{ao}
contexto de IoT densa, visto que elas geram alto consumo de recursos, não checam
os dados além de poucas consideram a detecção colaborativa. Dentre as técnicas
existentes, ~~a~~ mais empregadas são: esquemas de filtragem em rota, métodos colaborati-
vos e os sistemas de detecção de intrusão (IDS). Os esquemas de filtragem em rotas são
constantemente aplicados em RSSF, usam a verificação de relatório em nós intermediá-
rios entre origem e destino, descartando pacotes com qualquer tipo de inconsistência. Os
relatórios são endossados para garantir sua autenticidade, entretanto, eles não consideram
alteração dos dados coletados. Os métodos colaborativos são alternativa para lidar com
ataque~~s~~ IDF nas Smart Grid, cada dispositivo desempenha duas funções, as suas padrões
e a de agente colaborativo de detecção. Contudo, o consumo de recurso dos dispositivos
aumenta consideravelmente. Os IDS são alternativas robustas para lidar com os ataques
em diferentes contextos, podem~~o~~^{Não} ser baseados em dispositivos ou rede. Entretanto, podem
gerar alto consumo de recursos e gerar novas vulnerabilidades. Desta forma, torna-se ne-
cessário desenvolver mecanismos capazes de detectar e isolar a presença de ameaças de
forma distribuída para o serviço de agrupamento e protegendo a disseminação de dados.

Este trabalho propõe um mecanismo para mitigação do ataque de Injeção de da-
dos falsos sobre o serviço de disseminação de dados de redes IoT. O mecanismo chamado
CONFINIT (CONsensus Based Data FIltErinG for IoT), busca detectar e isolar da rede
IoT dispositivos maliciosos que apresentem comportamento malicioso ao sistema. O me-
canismo utiliza~~am~~ agrupamentos por similaridade para lidar com densidade e mobili-
dade dos dispositivos. Ele combina as técnicas de Watchdog e Consenso para tomada~~s~~ de

decisão sobre os dispositivos. O CONFINIT foi avaliado por simulações e os resultados demonstram sua capacidade de detectar dispositivos maliciosos e isolá-los da rede.

O restante do artigo está composto da seguinte forma: a Seção 2 apresenta os trabalhos relacionados. A Seção 3 apresenta e descreve o funcionamento do CONFINIT. A Seção 4 descreve o método de avaliação e o desempenho do mecanismo juntamente com resultados obtidos. A Seção 5 conclui o artigo e apresenta direcionamentos futuros.

2. Trabalhos Relacionados

A demanda por serviço de disseminação de dados seguro em redes densas contra diversas formas de ataques de intrusão tem sido o foco de diferentes trabalhos [Lu et al. 2012, Kumar et al. 2016, Yang et al. 2017, Cervantes et al. 2018, Bostami et al. 2019]. Em geral, o uso de Sistemas de detecção de Intrusão (IDS) viabiliza identificar, localizar e mitigar comportamentos de **má conduta de diversas naturezas** [Kumar et al. 2016]. Particularmente, os ataques maliciosos de IDF sobre o serviço de disseminação de dados das IoT densas tornam-se ~~muito~~ danosos ~~ao bom comportamento da~~ rede devido ao grande volume de dados gerados **pelos dispositivos e da sua importância à tomada de decisões dos objetos** pelas aplicações.

Em [Yang et al. 2017] os autores propuseram um IDS baseado em detecção de anomalias através do uso de *Watchdog* para mitigação do ataque de injeção de dados falsos. Usando os dados coletados de vigilância ambiental da IoT, eles tentam predizer eventos naturais. Para isso eles utilizam monitoramento Hierárquico Bayesiano Espacial-Temporal (HBT) para retratar as características dos dados coletados. Logo após, usa-se uma estratégia de decisão ~~baseada em~~ estatística em um teste de probabilidade sequencial para identificar atividades maliciosas. Entretanto, o modelo HBT apresenta ~~um~~ alto consumo energético, juntamente com ~~seu~~ teste probabilístico ~~empregado~~ que sobrecarrega a rede, além de os dispositivos serem estacionários. Em [Cervantes et al. 2018] os autores apresentam uma IDS para mitigação de ataques *sinkhole* e *selective forwarding* no roteamento de redes IoT densas. Para isso a rede é organizada em *clusters* e os nós classificados em três categorias. Eles usam uma estratégia *Watchdog* em níveis para monitorar a relação entre encaminhamento e dados recebidos, com isso é possível calcular o números de transmissões e definir quais nós apresentam comportamento malicioso. Apesar disso, computar a confiança entre participantes com base na quantidade de dados recebidos e transmitidos não exclui a possibilidade do nó alterar os dados coletados.

Um método frequentemente utilizado contra os ataques IDF em RSSF ~~são os~~ esquemas de filtragem em rota [Lu et al. 2012, Yu and Guan 2010, Wang et al. 2014]. Em [Lu et al. 2012] os autores propõem um esquema de autenticação cooperativa para filtrar dados falsos em RSSF, cada nó requer um número fixo de vizinhos para gerenciar a autenticação, que baseia-se no roteamento de vizinhos. Os nós são autenticados de forma distribuída ao longo do roteamento dos dados até a estação base. O esquema adota a técnica de bit comprimido visando não sobrecarregar o canal, tornando-o adequado para filtrar dados injetado já que a autenticação ocorre ponto-a-ponto. Além disso, o uso de um protocolo de roteamento evita que dispositivos maliciosos comprometam outros dispositivos. Entretanto, a proposta gera uma alta sobrecarga na rede e não identifica os dispositivos comprometidos. Em [Yu and Guan 2010], os autores apresentam um esquema de filtragem dinâmica em rota para lidar com dados falsos e ataque DoS em RSSF. Cada nó tem

um conjunto de chaves de autenticação usada para endossar relatórios. A autenticação é garantida por um grupo de nós escolhidos antes da rede funcionar. Cada nó disponibiliza sua chave aos nós encaminhadores que devem divulgar suas chaves, o que permite que os encaminhadores verificar todos os relatórios. Porém, esta solução gera sobrecarga na rede devido a constante troca de chaves entre os dispositivos, o que limita o seu funcionamento em redes densas.

Uma maneira de alcançar uma detecção colaborativa é através do uso de *Consenso* entre dispositivos de uma rede [Colistra et al. 2014]. 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. Para isso, são realizadas análises em cada ponto de coleta de dados usando um classificador Bayes. Ao final, a análise é realizada de forma redundante, paralelo ao nível de cada ponto de coleta de dados, o que evita o ponto único de falhas. O fato de utilizar o consenso de forma distribuída facilita a tomada de decisão colaborativa. Contudo, o custo computacional de comunicação entre os participantes pode sobrecarregar a rede e diminuir a efetividade do sistema. Em [Kailkhura et al. 2015], os autores desenvolvem um algoritmo robusto de consenso apoiado em média ponderada distribuída. O algoritmo visa permitir uma adaptação a regras locais estipuladas pela rede. Para isso, foi desenvolvida uma técnica de aprendizagem para estimar parâmetros operacionais ou peso de cada nó. Assim, torna-se possível automatizar regras locais de fusão ou atualização para mitigar ataques. O trabalho foi proposto para funcionar em uma rede distribuída, apesar disso, os autores não consideraram a dinamicidade como fator de impacto, o que facilita as ações maliciosas.

Assim, faz-se necessário o desenvolvimento de soluções capazes de atuar de forma distribuída e sejam capazes de identificar e isolar a presença de dispositivos maliciosos em redes IoT densas. Essas soluções ao preservar a segurança dos dispositivos de maneira não devem interferir no seu funcionamento padrão ou gerar sobrecargas adicionais. Além disso, deve-se atender normalmente as características de uma IoT densa.

3. Um Mecanismo para Mitigação de Ataques IDF em IoT Densa

Este seção apresenta o mecanismo CONFINIT (*CONsensus Based Data FIltErinG for IoT*) para mitigação de ataques de injeção de dados falsos sobre o serviço de disseminação de dados em redes IoT densas voltadas ao ambiente da indústria 4.0. Ele baseia-se no monitoramento entre participantes para detectar anomalias na rede e utiliza-se da técnica de consenso colaborativo para tomada de decisão. O objetivo é garantir a autenticidade dos dados disseminados na rede IoT para apoiar a toma de decisões das aplicações sobre os serviços disponibilizados.

Inicialmente, detalha-se as características da rede IoT massiva, onde o serviço de agrupamento de dados executa, e do comportamento dos nós atacantes. Em seguida, define-se a arquitetura do mecanismo, realçando o papel de cada componente, de modo a identificar e isolar os nós atacantes atuando no agrupamento.

3.1. Modelo da Rede e do Sistema

- descrever as características da rede (caracterização da rede IoT)

- descrever as características do atacante (caracterização do atacante no serviço)

3.2. Modelo da Rede e do Sistema

Esta subseção contextualiza a estrutura da rede IoT densa empregada no trabalho, o modelo de ataque a ser aplicado sobre o serviço de disseminação de dados. Assume-se uma rede IoT densa ~~no ambiente~~ no contexto industrial. Ela é composta por nós heterogêneos, que podem ou não apresentar ~~mobilidade~~ mobilidade. O modelo de comunicação assume que a comunicação entre os agrupamento ocorre através dos nós líderes de cada agrupamento.

Modelo de Rede: Representa uma rede IoT densa formada pelo conjunto N de n nós denotados por $N = \{n_1, n_2, n_3, \dots, n_n\}$, onde $n_i \in N$. Cada nó n_i tem um endereço físico exclusivo (Id) que o identifica na rede. A transmissão de nó ocorre através do meio sem fio mediante a um canal assíncrono com perda de pacotes devido a ruídos e posição dos nós. Os nós são compostos de diferentes recursos, como tamanho da memória, armazenamento e bateria. Além disso, todos os nós atuam na mesma faixa de transmissão e formam os agrupamentos. Todos os nós começam como nós isolados e buscam por vizinhos para formarem os agrupamentos, eles podem integrar ou não agrupamentos. Os que não fazem parte de nenhum agrupamento podem ser detectado como nó atacante. Os nós podem atuar na rede de duas formas: como nós comum, e nós líder. Os comuns são os que integram os agrupamentos e enviam suas mensagens em direção aos líderes. Os nós líderes ~~são~~ são responsáveis por receber as informações e disponibilizá-las. A Figura 1 ilustra o modelo de rede densa na IoT.

Essa figura está muito cópia do Christian. Melhor ter um único plano com tamanho maior, e assim construir os agrupamentos através de linhas. Parecido um pouco com a Figura 6 do link abaixo

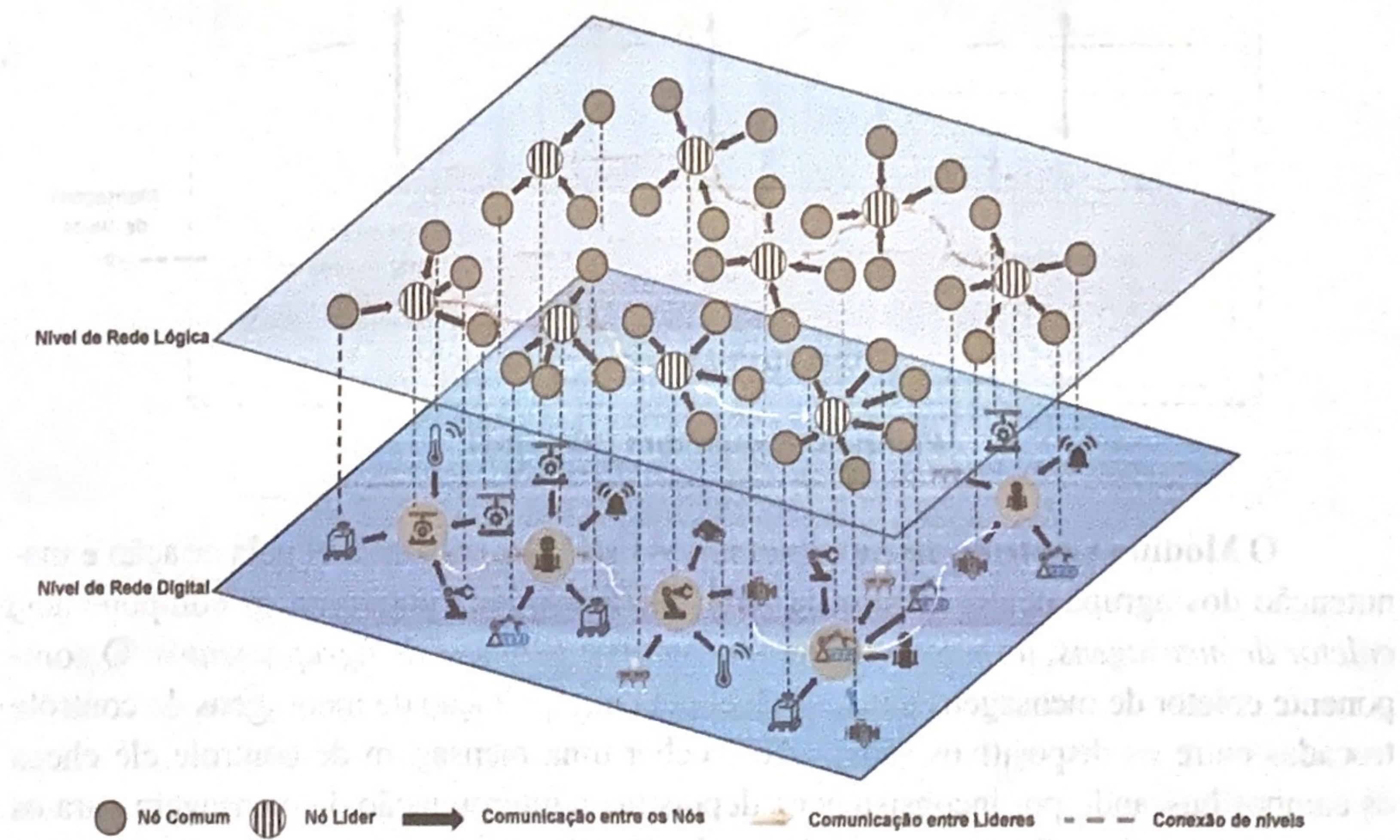


Figura 1. Modelo de Rede

Modelo da Ameaça: o ataque de injeção de dados falsos (IDF) é um tipo de ataque de intrusão de má-conduta, que tem por características a adulteração, falsificação e fabricação de dados coletados por dispositivos IoT. A execução do ataque IDF ~~por~~ ocorrer ~~por~~

Muita repetição de "dispositivo", daí pra entender mais é pra "fazer" de se Ler

de duas formas com o mesmo objetivo. Na primeira forma, o dispositivo é capturado por outro dispositivo, que ~~mais~~ manipula o dispositivo, seja alterando ou fabricando seus dados. Na segunda forma, o próprio dispositivo altera, fábrica e manipula seus dados. Assume-se que o ataque IDF inicia-se após vulnerabilidades serem deixadas por outros ataques. [Yang et al. 2017, Yaqoob et al. 2017]. O atacante explora essas vulnerabilidades dificultando a identificação dos dispositivos, como ilustrado na Figura 2.

Figura 2. Modelo de ataque IDF

3.3. Arquitetura CONFINIT

A arquitetura do CONFINIT é composta por dois módulos **Controle de Agrupamentos** e **Detecção de Falhas** como ilustrado na Figura 3. Ambos os módulos trabalham de maneira conjunta e paralela para garantir a segurança da rede. O módulo agrupamentos organiza a rede em *cluster*, e o módulo detecção de falhas é responsável por monitorar os dispositivos da rede, detectar e isolar dispositivos maliciosos.

Vamos conversar sobre a figura da arquitetura depois.

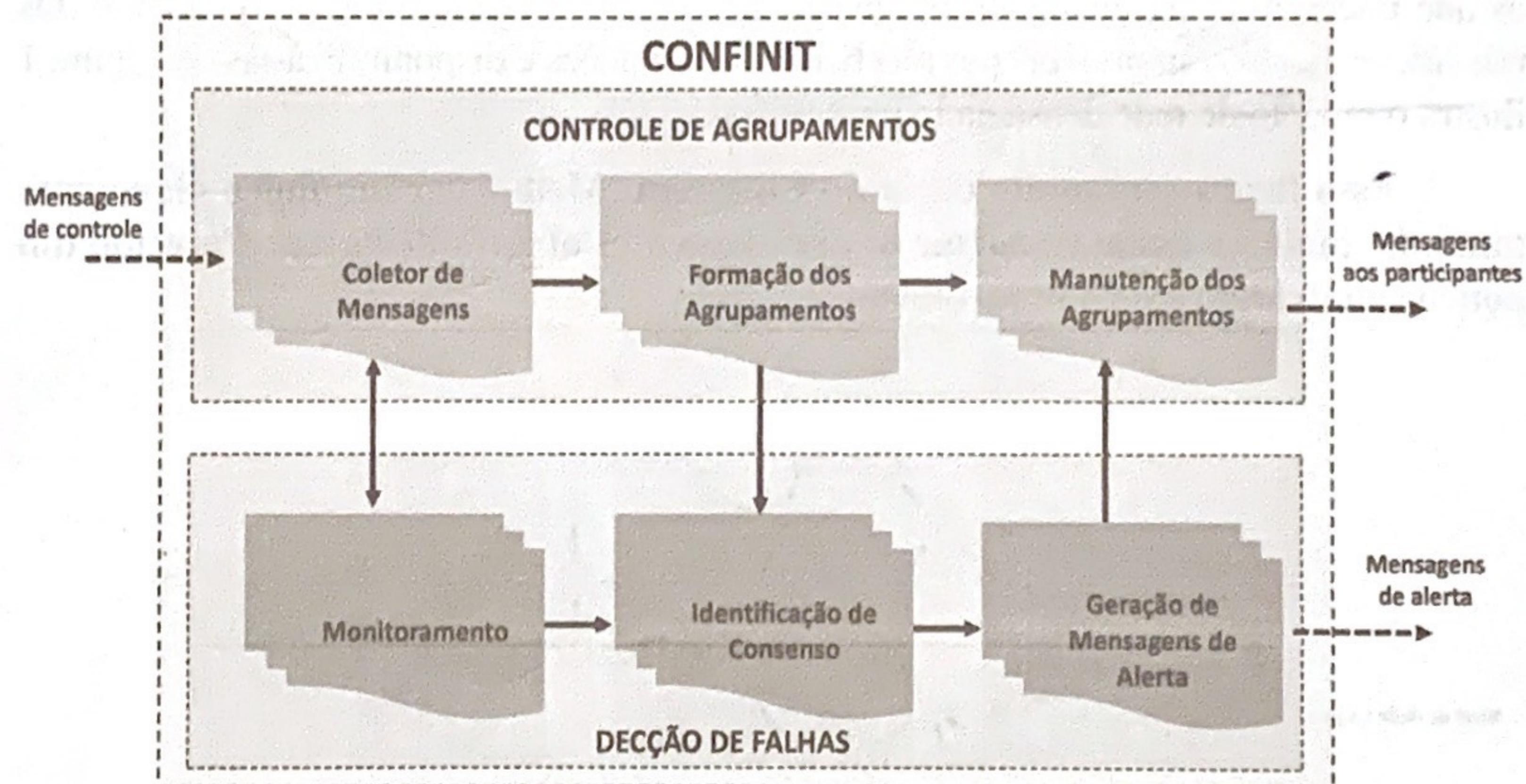


Figura 3. Arquitetura CONFINIT

O Módulo Controle de Agrupamentos (MCA) é responsável pela criação e manutenção dos agrupamentos dentro da rede. Para isso ele conta com os componentes *coletor de mensagens*, *formação de agrupamentos* e *gerência de agrupamentos*. O componente coletor de mensagens é responsável pela interpretação de mensagens de controle trocadas entre os dispositivos (nós). Ao receber uma mensagem de controle ele checa os campos buscando por inconsistências, depois faz a interpretação da mensagem para os outros componentes. O componente formação de agrupamentos é responsável pela organização da rede em agrupamentos ~~na rede~~, considera ~~mais~~ o valor de leitura coletada pelos nós comparando-as com os vizinhos. O componente gerência de agrupamento é encarregado de manter a formação dos agrupamentos, ele mantém uma lista com os participantes que é atualizada quando um nó entra ou sai do agrupamento. Esse procedimento ocorre de

identifica os nomes próprios dos módulos. Se sa com negativo, tipo ou o que for.

PARA SUPORTAR

forma continua devido a dinamicidade da rede IoT e dos participantes. Além disso, ele funciona localmente em cada nó, o que facilita a tomada de decisão.

O Módulo Detecção de Falhas (MDF) garante a segurança da disseminação de dados entre os nós da rede IoT de modo que apenas leituras autenticas sejam disseminadas. Ele consiste dos componentes *Monitoramento*, *Identificação* e *Isolamento*. O componente *Monitoramento* verifica o comportamento dos nós com relação a troca de mensagens de controle. Ele utiliza uma combinação de *Watchdog* que monitora os nós que não conseguem participar do agrupamento. O componente *Detecção* emprega uma técnica de *Consenso* colaborativo entre os nós para detectar os ataques IDF. O consenso é a concordância e uniformidade de opiniões que os nós estabelecem por meio de troca de informações entre eles. O componente *Isolamento* opera para isolar os nós atacantes e informar aos demais membros sobre ~~esse~~ ameaças. Assim, quando é detectado um ataque, os nós que detectaram propagam uma mensagem de alerta para que os líderes do agrupamento dissemitem a mensagem pela rede. Os dados propagados na mensagem de alerta consistem do Id e leitura individual do atacante.

3.3.1. Formação dos agrupamentos

A IoT é composta por uma diversidade de dispositivos, logo o desafio de gerenciar e controlar esses dispositivos torna-se uma tarefa que exige esforços. Desta maneira, o módulo agrupamentos organiza a rede com base nos líderes para a criação da topologia da rede. A técnica de agrupamento é muito utilizada na organização de dispositivos (nós) na rede, melhorando o fluxo de dados, aumentando a escalabilidade, prolongando a vida útil da rede, viabilizando uma melhor comunicação entre os dispositivos. Inicialmente todos os nós da rede começam livres transmitindo e coletando mensagens de controle dos nós vizinhos para composição dos agrupamentos. As transmissões das mensagens de controle são realizadas em *broadcast*, afim de serem escutadas pelos nós em busca de vizinhos. As mensagens trocadas são compostas por informações como (*Id*) do nó emissor, leitura individual L_{ind} , número de vizinhos do nó N_{viz} , leitura agregada L_{agr} , e nível de energia N_{ener} . Entretanto, caso alguma das informações não seja recebida pelo nó receptor, o mesmo descarta a mensagem automaticamente.

~~Assim~~, as informações são encaminhadas ao componente formação dos agrupamentos, responsável pelo cálculo da similaridade entre os nós. ~~Assim, ele~~

O componente formação de agrupamento realiza a comparação de similaridade entre os nós com base nos valores das leituras, quantidade de vizinhos e leituras agregadas desses vizinhos. Devido a suas características, a melhor forma de chegar à similaridade de dados é através da comparação de leituras, assim a equação de similaridade é baseada em [Gielow et al. 2015], onde X representa a leitura atual do nó e Y a leitura com a qual ela está sendo comparada com a finalidade de satisfazer o limiar de similaridade. A Equação 1 calcula a similaridade entre dois nós.

$$Y - \frac{X + \sum_{v \in SNeigh} (NeighR[v].aR * NeighR[v].nR)}{1 + \sum_{v \in SNeigh} (NeighR[v].nR)} \quad CThresh \quad (1)$$

Não foi definido no texto

** Estamos assumindo forte correlação espacial então? Pás nem sempre a não similaridade de nós próximos indica um ataque. Este escopo deve ser definido antes, não no meio do desenvolvimento.

Paralelo a formação dos agrupamentos, o processo de eleição dos líderes ocorre com base na quantidade de vizinhos com relação aos nós que estão fazendo parte do agrupamento. Após esse processo, o nó líder dissemina uma mensagem aos nós que fazem parte do agrupamento que ele é líder. Caso exista no agrupamento nós com mesmo número de vizinhos, o nó com maior nível de energia (NE) será eleito o líder. Por exemplo, no cálculo do NE_i , do nó n_i é preciso saber o total de energia restante TE_{ri} , que possui o nó (n_i). A Equação 2 determina o valor calculado para TE_{ri} onde TE_i é o total de energia do nó n_i e TE_{ci} é o total de energia consumida pelo nó n_i . Este cálculo define o total de energia que ainda resta ao nó n_i . Isso garante a melhor definição do nó líder.

total?

$$TE_{ri} = TE_i - TE_{ci} \quad (2)$$

A Equação 3 estabelece o cálculo de NE do nó n_i , que é obtido com o TE_{ri} resultante da Equação 2. O segundo parâmetro da equação é o TE_{ci} .

$$NE_i = \frac{TE_{ri}}{TE_{ci}} \quad (3)$$

O consumo de energia deve ser eficiente em todos os aspectos do mecanismo para melhorar o tempo de vida da rede. A preservação de energia entre os nós é fator fundamental para sobrevivência das redes IoT. Logo, otimizar a rede em forma de agrupamento auxilia na economia de energia. No CONFINIT, a energia é considerada na escolha de um nó como líder, no caso de ter dois ou mais líderes no mesmo agrupamento. A manutenção dos agrupamentos ocorre quando um dos participantes falha ou deixa o agrupamento. Assim, cada nó mantém uma lista de vizinhos atualizada a medida que um nó queira participar ou deixar o agrupamento. Essa atualização ocorre periodicamente com a troca de mensagens entre os participantes devido à mobilidade da rede.

3.4. Detecção de Falhas

Na formação dos agrupamentos, os nós que não atendem ao limiar de similaridade de leituras em um primeiro momento são considerados suspeitos, e passam a integrar uma lista **de suspeitos**. Essa lista mantém o *Id* desse nó e sua leitura. Uma vez inserido na lista, o nó que detectou **ações** envia uma mensagem em broadcast tal que os outros nós possam atualizar sua lista com as informações. O Consenso passa a atuar de forma efetiva após a primeira interação entre os nós, porque é necessário um histórico de interações. Em um segundo momento, o mesmo nó tenta fazer parte do agrupamento novamente, quando é recebida a mensagem de controle o nó que recebeu a mensagem confere as informações e identifica que o nó está na lista de suspeitos. Assim, ele compara a leitura **nós** juntamente com as leituras dos seus vizinhos. A Equação 4 define a formação do Consenso colaborativo entre os nós participantes para identificação de atacantes. Ela é derivada da equação do desvio padrão, onde o conjunto $V = (x_i, x_{i+1}, \dots, x_n)$ representa os vértices a serem comparados.

$$\sqrt{(x_i - x_{i+1})^2} \leq \text{limiar} \quad (4)$$

Após computado os valores entre os nós, chega-se a um consenso sobre o comportamento do nó em questão, se o mesmo é ou não um atacante. Caso ele seja determinado

o mesmo nota ** da página 7.

ESSA NÃO É
UMA CONCLUSÃO
INTUITIVA.
REFERÊNCIA?

em algumas Redes a Leitura atípica e sustamente a Leitura mais
válida. em uma Rede p/ detecção de incêndios, descartar uma Lei-
tura muito alta por estar fora do limiar mataria o propósito
da rede. É necessário definir melhor o escopo deste trabalho.

Ó Propósito

como um atacante, uma mensagem é propagada em broadcast aos participantes. Caso o cálculo fique dentro do limiar de similaridade o ele ainda continua sem fazer parte do agrupamento no momento, mas pode vir a fazer em outro momento, se em um segundo momento ele apresentar leituras dentro do limiar e não tiver nenhuma restrição. Logo, quando ele consegue participar do agrupamento seu Id é retirados da rede. Vale salientar que os históricos são mantidos por um determinando tempo, isso ocorre devido a dinamicidade da rede. A Figura ?? ilustra um exemplo de consenso entre participantes, mostrando a identificação e exclusão de um nó da rede.

Mul escrito.
Revisar

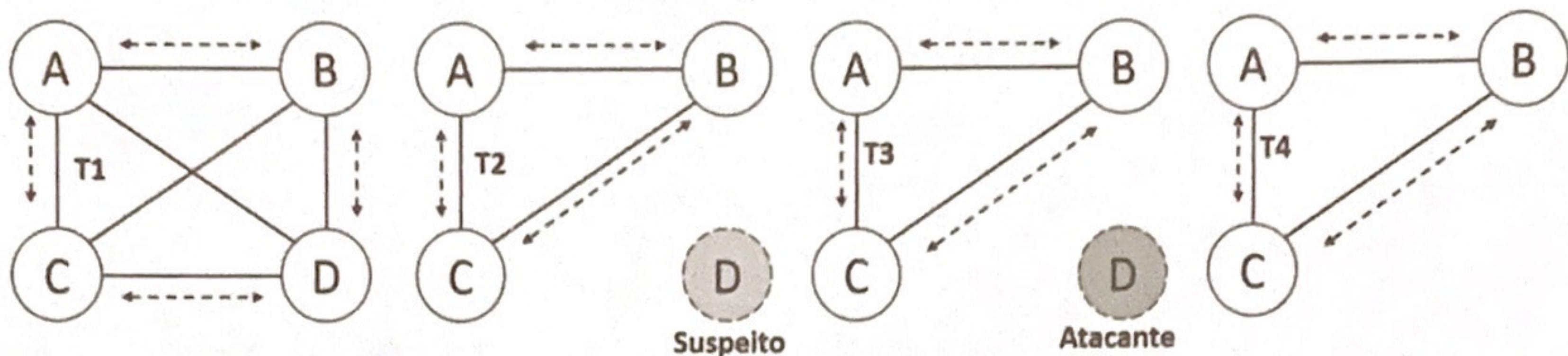


Figura 4. Formação dos Consenso entre os nós

Na Figura, as setas pontilhadas significam a existência de comunicação entre os nós (A, B, C, D) no instante T_1 , garantindo assim a troca de mensagem de controle entre eles. Já no instante T_2 , apenas os nós (A, B, C) agrupam-se visto que eles respeitam o limiar de similaridade, entretanto o nó D não respeita o limiar, então em um primeiro momento é classificado como suspeito. No instante T_3 , o nó D envia novamente mensagens de controle para tentar fazer parte do agrupamento, assim o conjunto formado pelos nós (A, B e C) que executam o cálculo da Equação 4, e classificam o nó D como atacante, já que ele novamente apresenta leituras distintas dos demais nós. Por fim, no instante T_4 apenas os nós honestos estão fazendo parte da rede. Desta forma, a segurança da rede pode ser mantida pelos próprios participantes sem a necessidade entidade externa, o que representa o ponto único de falha.

3.5. Funcionamento

4. Avaliação

Não revisei a Seção 4. Pois
ainda é incompleta.

Esta seção apresenta uma avaliação sobre a eficácia do CONFINIT diante de ataques de injeção de dados falsos. O CONFINIT foi implementado no simulador NS-3, versão 3.28. Este simulador foi escolhido em razão da possibilidade de representar um ambiente de massiva escala de objetos IoT num cenário IIoT com as características da redes. Além disso, o protocolo de agrupamento XXX usado para agrupar os dados foi implementado neste simulador [XX]. Além disso, o comportamento de ataques IDFs foi implementado.

O cenário analisado leva em conta um ambiente de redes de Indústria IoT (IIoT) 4.0 representando uma fábrica XX. Nela os dispositivos IoT estão localizados sobre os objetos A, B, C em uma área XxY metros. Cada objeto transmite dados através do padrão IEEE XXX, onde eles estabelecem agrupamento de modo a facilitar a busca dos dados para a tomadas de decisão. Os nós arbitrariamente apresentam um comportamento malicioso. A quantidade de nós comportamento malicioso consiste de x%, Y%, e z% do total de nós da rede. O tempo de simulação é de xxx segundo. Os nós estabelecem agrupamento a partir do protocolo XXX. A consulta sobre as informações da rede é feita por uma unidade central.