Controle da Disseminação em Agrupamentos Dinâmicos de Dados Para Rede IoT Densa Contra o Ataque de Injeção de Dados Falsos

Carlos Pedroso[1], **Aldri Santos**[1] **(Orientador)**

[1]Núcleo de Redes Sem-Fio e Redes Avançadas (NR2) – PPGInf – UFPR

{capjunior,aldri}@inf.ufpr.br

Abstract. *The growth of IoT has made possible the creation of increasingly personalized services, that often deal with massive amounts of data. However, as IoT grows, its threats are even greater. Among the threats to dense IoTs, the false data injection attacks (FDI) stand out as being one of the most aggressive, especially on the service of data clustering. This dissertation proposes an intrusion detection mechanism, called CONFINIT, against FDI attacks on the data dissemination service in IoT dense. It combines strategies of watchdog surveillance and collaborative consensus for the detection of attackers, guaranteeing the authenticity of the data collected by th devices. An evaluation on the NS-3 simulator has shown that CONFINIT achieves detection rate of 99% for IDF attackers, an average accuracy of 0.84 , and low rates of false positive and negatives. In addition, it has increased the capacity of clustering by up to 30%, proving its effectiveness in supporting the availability of the service.*

Resumo. *O crescimento da IoT vem possibilitando a criação de serviços cada vez mais personalizados, entre eles destacam-se os serviços que lidam com massiva quantidade de dados. Entre as ameaças às IoT densas estão os ataques de injeção de dados falsos (IDF) por serem um dos mais agressivos sobre o serviço de agrupamento de dados. Esta dissertação propôs um mecanismo de detecção de intrusão contra ataques IDF, chamado CONFINIT, sobre o serviço de disseminação de dados em IoT densa. Ele combina estratégias de vigilância watchdog e consenso colaborativo para a detecção de atacantes, garantindo a autenticidade dos dados coletados pelos dispositivos. Uma avaliação no simulador NS-3 demonstrou que o CONFINIT alcança 99% de taxa de detecção de atacantes IDF, uma acurácia média de 0,84, e baixas taxas de falsos negativos e positivos. Além disso, ele aumentou em até 30% a capacidade de agrupamentos formados, comprovando sua eficácia para apoiar a disponibilidade do serviço.*

1. Introdução

A Internet das coisas (IoT) possibilita a conexão de diferentes tipos de objetos físicos, através de tecnologias como as redes de sensores sem fio (RSSF), RFID, GPS e NFC, entre outras. Os objetos que compõem a IoT possuem várias características como identidade, atributos físicos, heterogeneidade, e muitos deles usam interfaces inteligentes para estabelecerem comunicações entre si, além de apresentar alguma forma de mobilidade. A IoT faz parte da evolução de domínios densos e complexos como processos industriais, logística, segurança pública e cidades inteligentes. 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. Grande parte dos dispositivos estarão embarcadas nas industrias e maquinário industrial, criando s Internet das coisas industriais (IIoT) densas. A IIoT trata da conexão de diferentes dispositivos dentro de uma indústria, possibilitando que todos trabalhem de forma sincronizada e organizada.

Visto que as redes IoT são fundamentais para coletar, disseminar e lidar com o volume de dados exigido por diversas aplicações nas suas tomadas de decisões. Logo, tratar e disseminar esse grande volume de dados resultante da interação entre os vários dispositivos expõe as IoTs densas a diversas vulnerabilidades. Os ambientes IoT normalmente contam com dispositivos móveis e fixos e a infraestrutura varia conforme a interação ao longo do tempo. Além disso, parte desses dispositivos têm recursos imitados, como pouca energia, baixa capacidade de processamento e armazenamento; além de sofrerem perdas nos enlaces de conexão. Assim, a IoT torna-se alvo de inúmeras ameaças que violam atributos de segurança como integridade, autenticidade e disponibilidade de serviços. O ataque de injeção de dados falsos (IDF) é considerado um dos ataques de intrusão mais nocivo às redes de dados, devido à inconsistência das informações geradas e à imprevisibilidade do seu acontecimento [Sen and Madria 2017], tendo um comportamento arbitrário de uma falha bizantina. Em razão da sua complexidade, a detecção do ataque torna-se complexa e trabalhosa, pois normalmente os dispositivos maliciosos estão autenticados na redes e exercem suas funções padrão de coleta e disseminação de dados. Os ataques ocorrem em diferentes períodos e de forma contínua, desorientando a rede. Por característica, um ataque IDF pode alterar ou fabricar os dados, capturando ou usando outros dispositivos para injetar dados. Esse comportamento dificulta a identificação de dispositivos maliciosos e aumenta o tempo de mal funcionamento da rede, gerando inconsistência nos dados e prejudicando o desempenho da rede.

Apesar de várias abordagens na literatura terem sido empregadas para tratar ataques IDF, seja em RSSF, *Smart Grids* [Li et al. 2017] ou IoT [Yang et al. 2017]. Elas têm falhado ou não são adequadas ao contexto de IoT densa, visto que geram alto consumo de recursos, não checam os dados, e poucas consideram uma detecção colaborativa. Uma abordagem efetiva e prática são os esquemas de filtragem em rotas, que tem sido constantemente aplicados em RSSF, e usam a verificação de relatório em dispositivos intermediários entre a origem e o destino, descartando pacotes com qualquer tipo de inconsistência. As técnicas de detecção colaborativas têm sido usadas para lidar com ataques IDF nas *Smart Grids*, onde cada dispositivo desempenha duas funções, as suas funções-padrão e a de agente colaborativo de detecção. Os sistemas de detecção de intrusão (IDS) são mecanismos normalmente robustos para lidar com os ataques em diferentes contextos, podendo ser baseados em dispositivos ou rede. Entretanto, eles podem gerar alto consumo de recursos dependendo da escala da rede, além de gerar novas vulnerabilidades. Logo, torna-se fundamental ao desenvolvimento da IoT que os mecanismos sejam capazes de detectar e isolar a presença de ameaças de forma distribuída garantindo maior robustez aos serviços de agrupamento e disseminação de dados.

A dissertação apresentou um mecanismo para a mitigação do ataque de injeção de dados falsos sobre o serviço de disseminação de dados de redes IoT densas. O mecanismo, chamado CONFINIT (***CON****sensus Based Data* ***FI****lteri****N****g for* ***IoT***), busca detectar e isolar da rede IoT dispositivos maliciosos que apresentem má conduta ao serviço de

disseminação de dados a fim de prover a autenticidade dos dados e a disponibilidade do serviço. Ele combina as estratégias de vigilância (*watchdog*) para o monitoramento entre participantes e consenso colaborativo para a tomada de decisão sobre a existência de dispositivos maliciosos. Uma avaliação do CONFINIT no simulador NS-3 alcançou uma taxa de detecção de 99% de ataques IDF, uma acurácia média de 0,81, até 3,2% de falsos negativos e até 3,6% de falsos positivos. Ele proveu um aumento em até 30% no número de agrupamentos formados livres de atacantes, melhorando a disponibilidade do serviço.

Este artigo está organizado da seguinte forma: A Seção 2 apresenta o CONFINIT e seu funcionamento. A Seção 3 detalha a avaliação do sistema e os resultados. A Seção 4 apresenta as conclusões da pesquisa.

2. CONFINIT: Um Mecanismo para Mitigação de Ataques IDF em redes IoT

O sistema CONFINIT atua no serviço de agrupamento executando numa estrutura de rede IoT densa no contexto industrial, como ilustra a Figura 1 e descrito a seguir, sendo composta por nós heterogêneos, que podem ou não possuir mobilidade. Além disso, assume-se que a comunicação entre os agrupamentos estabelecidos ocorre através dos nós líderes. A arquitetura do CONFINIT, retratada na Figura 2, é composta pelos módulos **Gerência Agrupamentos** e **Gerência de Falhas**, que atuam de maneira conjunta para garantir a disseminação segura de dados na rede IoT [1].

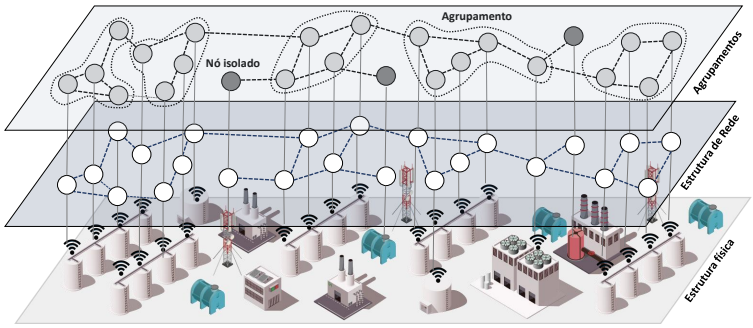

Figura 1. Exemplo de uma rede IoT densa

O **Módulo Gerência de Agrupamentos (MGA)** controla a formação e manutenção dos agrupamentos dentro da rede. Ele estabelece os agrupamentos com base em um limiar de similaridade de leituras dos dispositivos (nós) próximos e determina quando eles estão aptos para formar um agrupamento. Assim, ao receber uma mensagem de dados (explicado a seguir), ele verifica a identificação, a quantidade de vizinhos e as leituras desses vizinhos. O MGA possui os componentes *Controle de Similaridade (CS)*, *Coordenação de Agrupamento (CA)* e *Disseminação de Leitura Sensoriadas (DL)*. O componente CS atua como **watchdog** ao monitorar o recebimento e fazer a interpretação das mensagens trocada 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 cuida da eleição dos líderes. O componente DL é responsável por disseminar sua leitura, a leitura dos vizinhos e o número de vizinhos. Desta forma, ao receberem a mensagem os nós saberão se fazem parte 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

[1] Detalhes dos módulos, algoritmos e equações do CONFINIT encontram-se na dissertação.

os participantes. Assim, cada nó da rede mantém uma visão local, evitando sobrecarregar 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 carregam consigo.

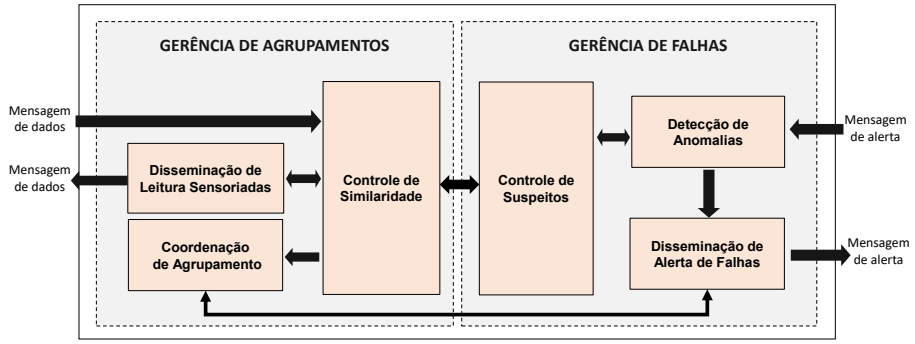

Figura 2. Arquitetura CONFINIT

O **Módulo Gerência de Falhas (MGF)** atua na segurança da disseminação de dados entre os nós da rede IoT tal 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 CS 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. A **filtragem colaborativa** tem como objetivo identificar os nós maliciosos que buscam fazer parte da disseminação de dados através da formação de agrupamentos. Ela ocorre toda vez que um nó é detectado como atacante. Essas interações são ilustradas na Figura 3,

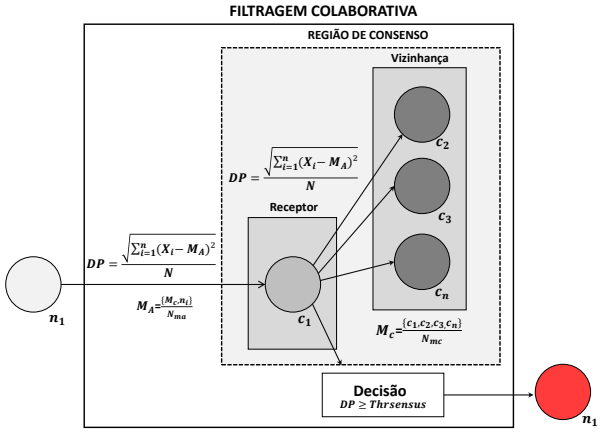

Figura 3. Funcionamento da filtragem no CONFINIT

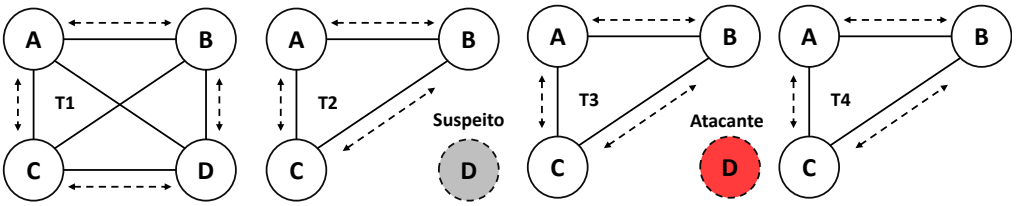

Figura 4. Formação de consenso entre os nós

A Figura 4 ilustra um exemplo 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. No instante *T2*, apenas os nós (**A, B, C**) agrupam-se, visto que eles respeitam o limiar de similaridade. Entretanto, o nó **D** por não respeitar este limiar, num primeiro momento, é classificado como suspeito. No instante *T3*, o nó **D** envia novamente mensagens de controle a fim de fazer parte do agrupamento e, então, o conjunto formado pelos nós **(A, B e C)**, ao executar o cálculo, classifica o nó **D** como atacante, visto que ele novamente possui leituras distintas em relação ao conjunto. Em *T4* apenas os nós honestos participam do agrupamento. Assim, a segurança da rede é mantida pelos próprios participantes sem a necessidade de entidade externas.

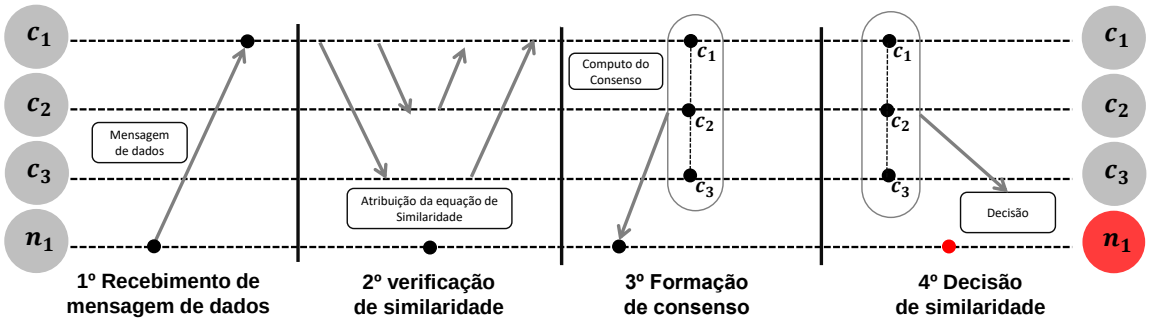

Figura 5. Interações entre as entidades do CONFINIT

A Figura 5 ilustra o processo de interação com base na formação dos agrupamentos e na filtragem colaborativa. 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 de formação de consenso colaborativo entre um conjunto de dispositivos.

2.1. Funcionamento

A formação de agrupamento ocorre de maneira dinâmica em cada nó da rede. As interações entre os nós realizam-se sob grandezas de espaço e tempo, assim as mensagens de dados são enviadas e recebidas pelos nós que estão dentro do raio de transmissão do emissor. Cada nó envia em *broadcast*, sua leitura, as leituras dos seus vizinhos, e a quantidade de vizinhos. Quando a mensagem é recebida, o nó receptor a interpreta, verificando seus campos e realizando o cálculo da similaridade. Se o limiar de similaridade é respeitado, o nó em questão passa a compor o agrupamento. Entretanto, se o limiar não for respeitado ele passa a integrar a lista de suspeito em um primeiro momento.

A Figura 6 retrata um exemplo do funcionamento do mecanismo na formação dos agrupamentos e eleição dos líderes. As arestas sólidas indicam os nós que estão dentro do raio de transmissão um do outro e podem trocar mensagens. 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. Assim, considera-se um limiar de similaridade = 3 para formação dos agrupamentos. Cada instante *T* corresponde a um troca de mensagem entre os nós para formar os agrupamentos e eleger os líderes. Com o controle de agrupamentos operando desta maneira, cada nó mantém atualizada suas informações através da troca de mensagens. Essa estrutura determina quais nós da vizinhança são vistos como membros do mesmo agrupamento, garante uma melhor escalabilidade à rede; além de ajudar a classificar nós com leituras divergentes, facilitando assim a identificação de atacantes pelo módulo de controle de falhas.

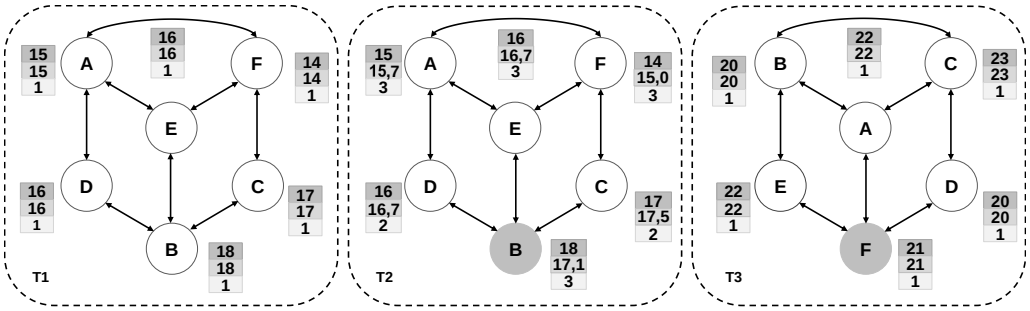

Figura 6. Formação dos agrupamentos

A detecção de falhas atua considerando a formação dos agrupamentos. Assim, os nós que não respeitam o limiar de similaridade passam a integrar uma lista de suspeitos em um primeiro momento. A classificação dos nós que não fizeram parte do agrupamento tem início na mensagem de controle, que sem os campos devidamente preenchidos são descartadas. Na formação dos agrupamentos, um nó que está próximo fisicamente de seus vizinhos em determinado instante e apresenta leituras distintas não respeitando o limiar de similaridade, pode ser considerado um nó suspeito em um primeiro momento. Assim, ele passa à integrar a lista de suspeitos, a qual contém nós que apresentaram um comportamento anômalo, mas não necessariamente são atacantes. Quando o nó em questão passa a integrar a lista de suspeitos e tenta participar do agrupamento, e novamente não consegue devido à leituras distintas, ele é classificado como atacante. Logo, seu (Id) é inserido em uma lista que contém todos os (Ids) das ameaças. Em seguida, o líder do agrupamento envia uma mensagem aos outros líderes avisando sobre a ameaça tal que, caso ele tente se agrupar em outro momento, não consiga.

A Figura 7 exemplifica a detecção de um ataque, onde cada instante *T* corresponde à um processo de agrupamento e os nós que satisfazem o limiar de similaridade passam a formar um agrupamento. Assim, no instante *T1* os nós **(A, B, D, E, F)** têm seus valores de leitura individual variando entre 14 a 18, respeitando o limiar de similaridade entre eles. Entretanto, o nó **C** apresenta um valor de 45 para sua leitura, o que diverge muito em relação aos seus vizinhos espaciais, logo, não respeita o limiar de similaridade. Desta forma, o nó **C** não pode fazer parte do agrupamento nesse momento. No instante *T2* o nó **C** novamente tenta agrupar-se, mas como seu (Id) já consta na lista de suspeitos, é feito um consenso entre os participantes com base em suas leituras e comparadas às do nó

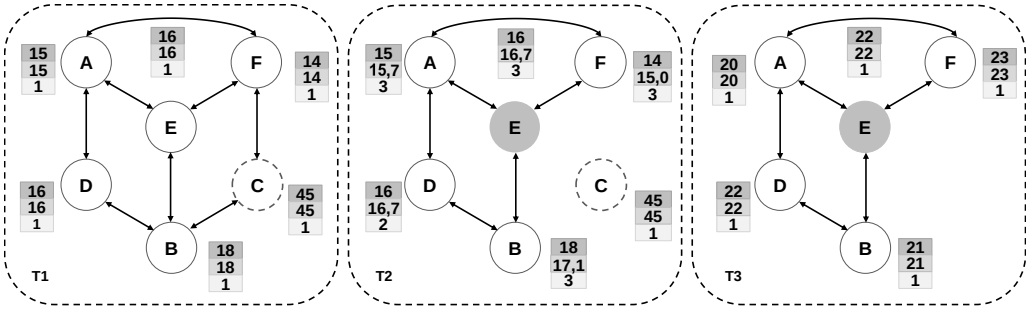

Figura 7. Detecção de falhas e consenso

C. Logo, constata-se que **C** é um atacante, não podendo integrar nenhum agrupamento. No instante *T3*, retirou-se o nó **C** da rede e é disseminada uma mensagem de alarme direcionada aos líderes com o (Id) do atacante em questão.

3. Avaliação

O CONFINIT foi implementado e avaliado no simulador NS-3, versão 3.28 [1]. O cenário analisado representa um o ambiente de uma indústria densa de maquinários, no qual os dispositivos IoT estão embarcados sobre os objetos industriais caracterizando uma rede IIoT. A análise leva em conta leituras reais obtidas a partir da coleta de dados de sensores de pressão de gás disponibilizada pelo laboratório UCI Machine Learning Repository, e foram definidos um limite de similaridade de 3 e de consenso de 5 com base no tipo de dados obtidos neste *dataset*. O cenário considera uma rede composta por 50, 75, e 100 nós distribuídos aleatoriamente em uma área retangular de *200m x 200m* operando por *1200s* com um raio de transmissão de *100m*. As percentagens de atacantes de IDF analisados foram 2%, 5% e 10%. A comunicação entre os dispositivos ocorre através do protocolo IPv6, sendo estabelecida uma rede *ad-hoc* no padrão IEEE 802.15.4. As métricas de avaliação usadas para mensurar o desempenho do CONFINIT, foram: ***Taxa de detecção*** (T_{det}), ***Acurácia*** (R_a), ***Taxa de Falsos positivos*** (T_{fp}) e ***Taxa de Falsos Negativos*** (T_{fn}). Todos os resultados são a média de 35 simulações, com um intervalo de confiança de 95% e são apresentados em pontos percentuais. Abaixo são apresentados os resultados referentes a (T_{det}), os demais resultados estão no texto da dissertação.

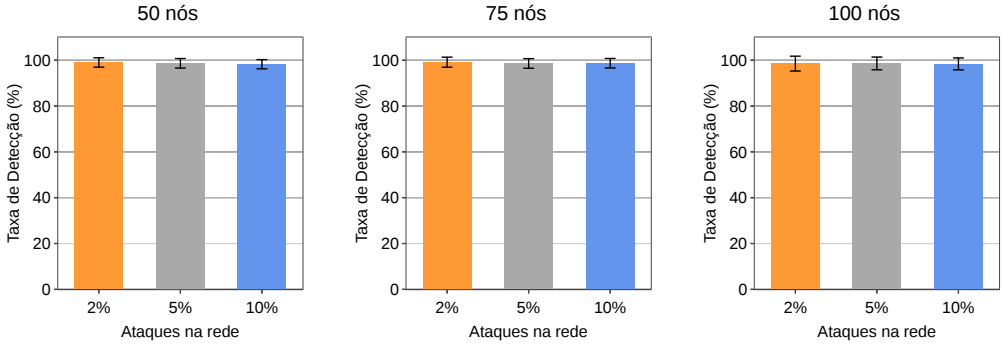

Figura 8. Taxas de detecção (T_{det}) para 50, 75 e 100 nós na rede

Os gráficos da Figura 8 apresentam a taxa de detecção (T_{det}) obtida pelo CONFINIT em relação ao número de dispositivos na rede e porcentagem de atacantes inseridos.

[1] Código disponível no github https://bit.ly/2S7JLDp

O mecanismo alcançou um taxa média de 97% de detecção para o ataque IDF, mostrando 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 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 das estratégias coopera para a filtragem colaborativa e aumenta o número de agrupamentos formados, garantindo a disponibilidade apenas de dados verificados. 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 mostrou alta capacidade em lidar com ataque IDF num ambiente de IoT densa.

4. Conclusão

Este artigo apresentou o mecanismo CONFINIT para mitigação de ataque de injeção de dados falsos em redes IoT densas. Este mecanismo ao organizar a rede em agrupamentos lida com a densidade dos dispositivos levando em conta a similaridade de leituras entre eles. O CONFINIT, através de *watchdog* e consenso colaborativo, vigia o comportamento dos dispositivos IoT com relação as suas informações de leitura, a fim de determinar dispositivos maliciosos, e prover a autenticidade dos dados e a disponibilidade do serviço. Os resultados a partir do emprego de dados reais de uma rede densa demonstraram a sua eficácia do na detecção e mitigação de dispositivos atacantes e a garantia de disponibilidade de apenas dados legítimos. As contribuições desta pesquisa de dissertação resultaram na publicação [Pedroso et al. 2019].

Referências

Li, B., Lu, R., Wang, W., and 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.

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.

Pedroso, C., Gielow, F., Santos, A., and Nogueira, M. (2019). Mitigação de Ataques IDFs no Serviço de Agrupamento de Disseminação de Dados em Redes IoT Densas. In *Anais SBSeg 2019*, Porto Alegre, RS, Brasil. SBC.

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

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