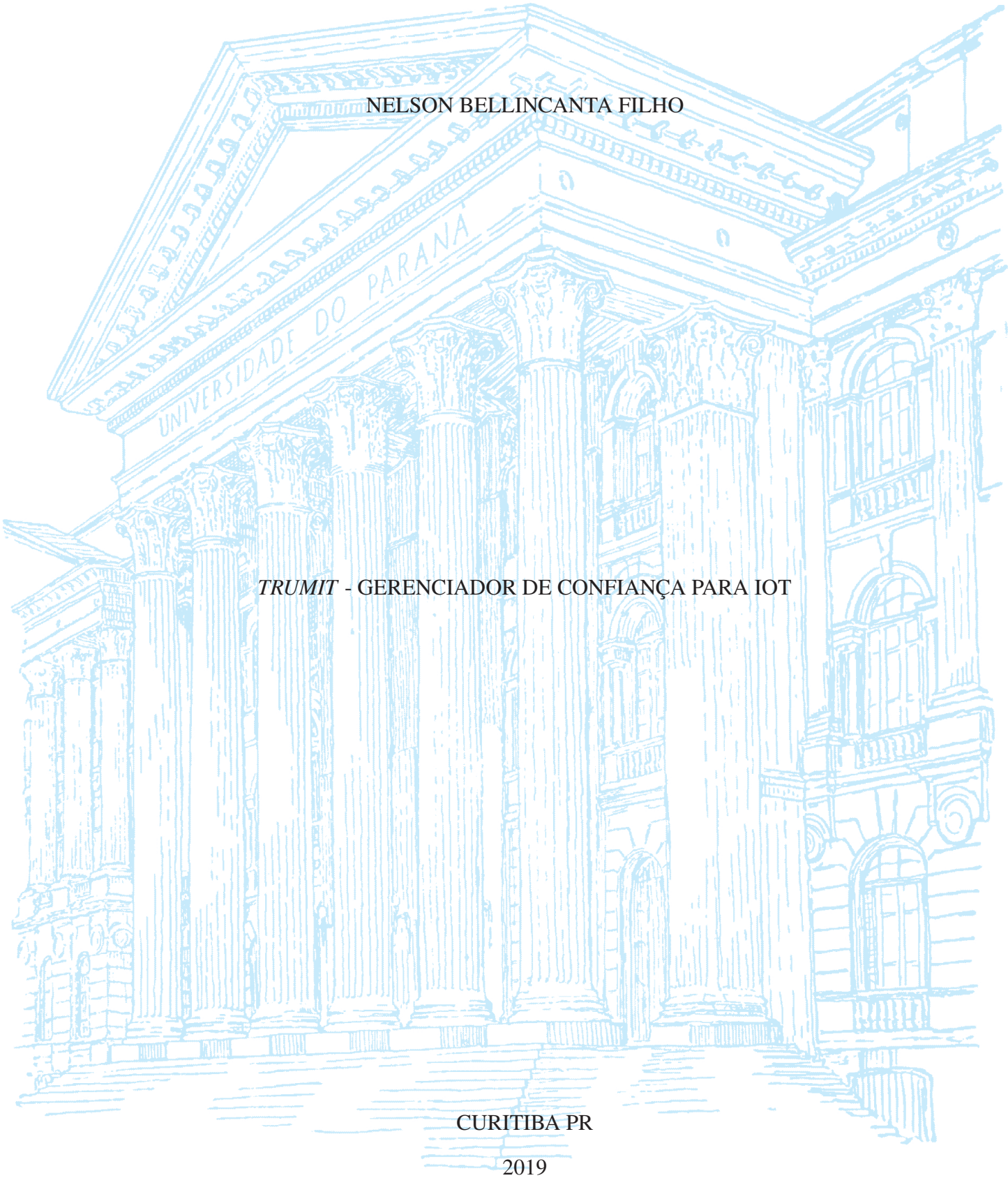
UNIVERSIDADE FEDERAL DO PARANÁ

NELSON BELLINCANTA FILHO



TRUMIT - GERENCIADOR DE CONFIANÇA PARA IOT

CURITIBA PR

2019

NELSON BELLINCANTA FILHO

TRUMIT - GERENCIADOR DE CONFIANÇA PARA IOT

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: Luiz Carlos Pessoa Albini.

CURITIBA PR

2019

Catalogação na Fonte: Sistema de Bibliotecas, UFPR
Biblioteca de Ciência e Tecnologia

B444t Bellincanta Filho, Nelson
Trumit - gerenciador de confiança para IOT [recurso eletrônico] / Nelson Bellincanta Filho. – Curitiba, 2019.

Dissertação - Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-Graduação em Informática, 2019.

Orientador: Luiz Carlos Pessoa Albini.

1. Internet das coisas. 2. Computadores - Medidas de segurança. 3. Internet - Controle de acesso. I. Universidade Federal do Paraná. II. Albini, Luiz Carlos Pessoa. III. Título.

CDD: 004.678

Bibliotecária: Vanusa Maciel CRB- 9/1928

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 **NELSON BELLINCANTA FILHO** intitulada: **TRUMIT - Gerenciador de Confiança para IoT**, sob orientação do Prof. Dr. LUIZ CARLOS PESSOA ALBINI, 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, 17 de Setembro de 2019.

LUIZ CARLOS PESSOA ALBINI
Presidente da Banca Examinadora (UNIVERSIDADE FEDERAL DO PARANÁ)

ALESSANDRO BRAWERMAN
Avaliador Externo (SETOR DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA)

MARCOS DIDONET DEL FABRO
Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

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

A minha esposa e filhos.

AGRADECIMENTOS

Á minha esposa que com seu amor incondicional nunca desistiu de mim, mesmo quando eu já tinha desistido. Apenas nós sabemos o quão difícil foi esta jornada. Obrigado por me trazer até aqui, você é o amor da minha vida. Aos meus filhos Eric, Maria Eduarda (Duda) e Igor, vocês são a melhor coisa que fiz nessa vida. Sem vocês não teria conseguido. Obrigado por serem a minha família, amo muito cada um de vocês.

As novas amizades que fiz em Curitiba, em especial ao Ivan Luiz Pedroso Pires sempre disponível para tirar dúvidas ou tomar um café e ao Renan Greca pelos conhecimentos compartilhados.

Ao Frank Uez pela infraestrutura disponibilizada, ao Rafael Gil Freques pelas tentativas de ajuda nesta dissertação e ao Dr. Thiago Moreira pela paciência e atenção.

A UFPR e ao Programa de Pós-graduação em Informática por proporcionar mais esta conquista em minha vida pessoal e profissional. Aos professores do departamento de informática da UFPR pelos conhecimentos repassados e pela sua dedicação a essa que se não é a mais importante das profissões é com certeza a base de todas. Aos técnicos administrativos da pós-graduação pelo atendimento cordial e celeridade nas solicitações e acesso às informações. Aos demais funcionários de UFPR que juntos colaboram para que a UFPR possa ser o orgulho de todos nós. Agradeço também á Capes por suportar a pesquisa nas universidades do Brasil.

Ao professor Albini, que acreditou em mim, me aceitando como seu orientando e que mesmo com tantos imprevistos, sempre esteve disposto a encontrar a melhor solução. Agradeço também aos professores Alessandro Braweman e Marcos Didonet Del Fabro por aceitarem a ser a banca da defesa da minha Dissertação e por contribuir com sugestões, ideias e novas visões que enriqueceram esta dissertação.

Muito obrigado!

"I’m still alive."
(Eddie Vedder)

RESUMO

A *Internet of Things - IoT* pretende unificar diferentes objetos inteligentes do mundo real sob uma infraestrutura comum, possibilitando a coleta de informações e o controle dos mesmos. A interação entre esses objetos de forma unificada e sob uma infraestrutura comum, irá gerar uma quantidade significativa de dados, os quais devem ser armazenados, processados e distribuídos de forma segura. Desta forma, é necessário garantir que estes objetos possuam um certo nível de confiança entre si. Contudo, avaliar a confiança em uma rede complexa como a *IoT* é uma tarefa desafiadora e é um tópico que tem recebido grande atenção da comunidade de segurança. Este fato, se deve à heterogeneidade e à limitação de recursos computacionais dos dispositivos que compõe o ambiente *IoT*. Para superar este desafio, diversas soluções de gerenciamento de confiança para *IoT* foram propostas e cada uma delas apresenta ganhos significativos para o gerenciamento de confiança para *IoT*. Entretanto, o estudo do gerenciamento de confiança para *IoT* ainda se encontra em desenvolvimento e novos direcionamentos devem ser propostos visando a integração dos dispositivos de forma confiável e considerando as características da *IoT*. Diante deste contexto, este trabalho propõe um novo modelo de confiança, denominado *TRUMIT* para gerenciar as relações de confiança entre dispositivos em um ambiente *IoT*. O modelo proposto é totalmente descentralizado e distribuído, desta forma, os dispositivos de uma rede *IoT* podem identificar rapidamente quais outros dispositivos são confiáveis ou não. Como uma rede *IoT* é altamente dinâmica, nesta abordagem, cada dispositivo cria, de forma auto-organizada sua rede de confiança, obtendo as informações necessárias para avaliar a confiabilidade dos demais dispositivos. Assim, o valor de confiança é calculado localmente, diminuindo o número de interações entre os dispositivos. As informações de confiança são obtidas através de observações diretas e indiretas. Inicialmente são coletadas as informações dos dispositivos conectados diretamente. Com o decorrer do tempo, são obtidas as informações de confiança dos dispositivos que não estão conectados diretamente, através de recomendações. As recomendações são adicionadas a rede de confiança, desta forma, quando houver uma interação direta no futuro, os dispositivos possuirão um certo nível de confiança entre si, sem mesmo terem interagido diretamente em outro momento. Em sua avaliação, o modelo proposto, demonstrou a capacidade de convergência e resiliência a nós maliciosos, garantido assim a confiabilidade entre os dispositivos.

Palavras-chave: *IoT*, gerenciamento de confiança, confiança direta, recomendações.

ABSTRACT

The Internet of Things - IoT intends to unify different real world intelligent objects under a common infrastructure, allowing the collection of information and control of them. Interaction between these objects unified and under a common infrastructure, will generate a significant amount of data, which must be stored, processed and distributed safely. Thus, it is necessary to ensure that these objects have a certain level of trust with each other. However, assessing trust in a complex network such as IoT is a defiant task and a topic that has received wide attention from the security community. This fact, is due to the heterogeneity and the limited computational resources of the devices that make up the IoT environment. To overcome this challenge, several trust management solutions for IoT have been proposed, and each has significant gains for trust management for IoT. However, the study of trust management for IoT is still under development and new directions should be proposed aiming at the integration of devices reliably and considering the characteristics of IoT. Given this context, this paper proposes a new trust model called TRUMIT to manage trust relationships between devices in an IoT environment. The proposed model is fully decentralized and distributed, in this way the devices on an IoT network can quickly identify which other devices are reliable or unreliable. Because an IoT network is highly dynamic, in this approach, each device create in a self-organized way its trusted network, obtaining the information it needs to assess the reliability of other devices. Thus, the confidence value is calculated locally, decreasing the number of interactions between the devices. The reliable informations is obtained through direct and indirect observations. Initially information is collected from directly connected devices. Over time, the reliable informations is obtained from devices that are not directly connected through recommendations. The recommendations are added to the trust network, in this way, when there is direct interaction in the future, devices will have a certain level of trust with each other without even interacting directly at another time. In his evaluation, the proposed model demonstrated the ability of convergence and resilience to malicious nodes, thus ensuring the reliability among the devices.

Keywords: IoT, trust management, direct trust, recommendations.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

2G	Second-generation Cellular Technology
3G	Third-generation Cellular Technology
4G	Fourth-generation Cellular Technology
AI	Artificial Intelligence
API	Application Programming Interface
bps	Bits per second
DINF	Departamento de Informática
DHT	Dristributed Hash Table
DSL	Digital Subscriber Line
EXI	eEfficient XML Interchange
GHz	Gigahertz
GSN	Global Sensor Networks
HPHC	High Processing and High Connectivity
HTTP	Hypertext Transfer Protocol
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IoT	Internet of Things
IR	Infrared
ISM	Scientific and Medical (ISM) Band Specifications
ITU	International Telecommunication Union
Km	Quilômetro
LPHC	Low Processing and High Connectivity
LPLC	Low Processing and Low Connectivity
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
M2M	Machine-to-Machine
MAC	Media Access Control
MANET	Mobile Ad Hoc Network
Mbps	Megabits per second
MHz	Megahertz
MTU	Maximum Transmission Unit
NFC	Near Field Communication
OWL	Web Ontology Language
P&G	Procter & Gamble

P2P	Peer-to-peer
PPGINF	Programa de Pós-Graduação em Informática
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RDF	Resource Description Framework
RFC	Request for Comments
RFID	Radio-frequency identification
RSSI	Received Signal Strength Indicator
SEMAN	SEcure Middleware for Ad hoc Mobile Networks
SASL	Simple Authentication and Security Layer
SCADA	Supervisory Control and Data Acquisition
SN	Sensor Networks
TCP	Transmission Control Protocol
TRUMIT	Trust Manager for IoT
UDGM	Unit Disk Graph Medium
UDP	User Datagram Protocol
UFPR	Universidade Federal do Paraná
UMTS	Universal Mobile Telecommunications System
Wi-Fi	Wireless Fidelity
WPAN	Wireless Personal Area Network
WSAN	Wireless Sensor and Actuator networks
WSN	Wireless Sensor Networks

LISTA DE SÍMBOLOS

α Parâmetro de confiança direta e indireta

Δ Intervalo entre as trocas de informação

Σ Somátorio

SUMÁRIO

1 INTRODUÇÃO

Desde seu início, a *Internet* passou por muitas transformações, do tradicional vínculo e compartilhamento de computadores e documentos, até uma plataforma para a realização de negócios e conexão de pessoas através das mídias sociais. Agora um novo paradigma denominado *Internet* das Coisas (*Internet of Things - IoT* termo em inglês) permitirá que bilhões ou até trilhões de objetos heterogêneos denominados de ”coisas” possam interagir uns com os outros por meio da *Internet*, a qualquer momento e em qualquer lugar. Esta interação irá permitir que esses objetos coletem e compartilhem informações, para coordenarem decisões, que auxiliem a execução de tarefas do cotidiano (Ngu et al., 2017; Al-Fuqaha et al., 2015; Kumar et al., 2016; Pawar e Ghumbre, 2016).

No entanto, as informações coletadas e processadas por estes objetos estão propensas a fatores que as tornam pouco confiáveis. Esses fatores podem estar relacionados a problemas técnicos ou de comportamento. Questões técnicas, como as condições do ambiente de implantação e o comprometimento da transmissão, são investigadas e abordadas por diversos pesquisadores. Esses problemas técnicos se concentram em detalhes de como verificar a autenticidade de um objeto e determinar quais as permissões o objeto possui. As técnicas utilizadas incluem criptografia, ocultação de dados, assinaturas digitais, protocolos de autenticação e métodos de controle de acesso (Suárez-Albela et al., 2018; Ali e Awad, 2018; Cui et al., 2018; Azzedin e Ghaleb, 2019).

Por outro lado, problemas relacionados ao comportamento dos objetos de *IoT* começaram recentemente a chamar a atenção da comunidade de pesquisa, uma vez que, o objetivo da *IoT* é permitir que diferentes objetos coletem e compartilhem informações vitais, incluindo informações do corpo humano e de medições ambientais. Essas medições monitoram não apenas seus ambientes, mas também executam efetivamente tarefas e influenciam processos de tomada de decisão em outros ambientes. Em um ambiente tão complexo como a *IoT*, não é possível presumir que todos os dispositivos sejam confiáveis, honestos e precisos. Assim, se esses objetos agirem de maneira mal-intencionada, poderão ocorrer catástrofes nos ambientes de *IoT*. Além disso, esses objetos afetam de perto a vida humana e consequências desastrosas podem ser impostas pela injeção de informações falsas (Mahalle et al., 2013; Fremantle e Scott, 2017; Billure et al., 2015; Kumar et al., 2016; Al-Fuqaha et al., 2015; Azzedin e Ghaleb, 2019).

No entanto, o tratamento de problemas relacionados ao comportamento dos objetos é uma tarefa desafiadora, devido ao ambiente heterogêneo, de grande escala e dinâmico como a *IoT*. A confiança de comportamento lida com uma noção mais ampla de confiabilidade de um objeto. Assim, um objeto malicioso pode fornecer as informações erradas ou não fornecer informação alguma (Bandyopadhyay et al., 2011; Al-Fuqaha et al., 2015; Bauer et al., 2016; Razzaque et al., 2016; Kumar et al., 2016; Ngu et al., 2017; Guo et al., 2017; Chelloug e El-Zawawy, 2017; Azzedin e Ghaleb, 2019).

Desta forma, a criação de ambientes confiáveis de *IoT* é de grande importância para obter todos os benefícios que este novo paradigma tem a oferecer. Além disso, a criação de ambientes confiáveis de *IoT* mitiga danos irrecuperáveis e inesperados para criar sistemas inteligentes, eficientes, estáveis e flexíveis orientados por sensores inteligentes e, consequentemente garante que os serviços tenham o desempenho esperado.

Diante deste contexto, um sistema de gerenciamento de confiança descentralizado e distribuído pode garantir a confiabilidade entre os objetos em um ambiente *IoT*, fornecer suporte à interoperabilidade às diversas aplicações e serviços que funcionam nesses objetos e resiliência a

outros objetos maliciosos (Guo et al., 2017; Ngu et al., 2017; Palade et al., 2017; de Jesus Júnior e Moreno, 2016; Tiburski et al., 2016; Albuquerque et al., 2016).

Para solucionar este problema, diferentes propostas foram apresentadas pela comunidade acadêmica e são discutidas e analisadas no Capítulo 3. No entanto, há muito a ser estudado, especialmente no que diz respeito a esquemas capazes de lidar com as restrições inerentes aos objetos de *IoT*, resiliência a nós maliciosos, instabilidade e comportamentos dinâmicos dos objetos. Assim, é proposto no Capítulo 4 o *TRUMIT*, uma solução para o gerenciamento de confiança para *IoT*, capaz de avaliar a confiança dos objetos em um ambiente *IoT*, considerando as características de um ambiente *IoT*, conforme verificado no Capítulo 2.

1.1 OBJETIVOS

O objetivo principal deste trabalho é a proposta do *TRUMIT - Trust Manager for IoT*, como uma solução para o gerenciamento de confiança entre dispositivos *IoT*. Para atingir o objetivo esperado, formam determinadas as seguintes atividades:

- Estudar os conceitos e fundamentos da *IoT*;
- Compreender o funcionamento de um sistema de gerenciamento de confiança para *IoT*;
- Realizar a revisão da literatura e identificar o estado da arte do gerenciamento de confiança para *IoT*;
- Classificar as soluções de gerenciamento de confiança existentes, de acordo com os requisitos analisados na seção 2.6.1 do Capitulo 2;
- Definir as funcionalidades do *TRUMIT*;
- Definir os cenários para a avaliação do *TRUMIT*;
- Coletar e analisar os resultados da avaliação do *TRUMIT*;
- Apresentar as conclusões e apontar os direcionamentos para novas pesquisas.

1.2 ESTRUTURA DO TRABALHO

O restante deste documento está organizado da seguinte maneira. O Capítulo 2 apresenta o embasamento teórico necessário para o entendimento desta dissertação. O Capítulo 3 apresenta o estado da arte dos sistemas de gerenciamento de confiança para *IoT*. Em seguida, o Capítulo 4 apresenta o *TRUMIT*, descrevendo seu modelo, notação e funcionalidades. O Capítulo 5 apresenta a análise dos resultados coletados da avaliação do modelo proposto e, por fim, o Capítulo 6 contém as considerações finais e sugestões de trabalhos futuros.

2 INTERNET DAS COISAS (IOT)

O termo ”Internet das Coisas” foi utilizado pela primeira vez em 1999 por *Kevin Ashton* em uma apresentação realizada aos executivos da *Procter & Gamble (P&G)*, onde vinculou a tecnologia *RFID* com a cadeia de suprimentos da *P&G* e à *Internet*, visando apenas obter a atenção dos executivos. Desta forma *Ashton* resumiu uma importante visão que se tornou sinônimo de tudo que está sendo conectado à rede das redes (Ashton, 2011).

O conceito de *IoT* pressupõe a conexão de qualquer dispositivo eletrônico à *Internet*, de modo a dotá-los de inteligência necessária para detectar e trocar informações entre si e coordenarem decisões por meio da coleta de dados físicos, processamento e respostas através de atuadores eletromecânicos. Isso inclui telefones celulares, cafeteiras, máquinas de lavar roupas, lâmpadas, dispositivos portáteis, geladeiras, além de uma infinidade de dispositivos construídos com sensores e com capacidade de conexão (Fig. 2.1). Unificando assim todos os dispositivos eletrônicos sob uma infraestrutura comum e permitindo o controle das coisas que compõem o mundo real, bem como, com informações sobre o estado dessas coisas (Albuquerque et al., 2016; Weber e Boban, 2016; Al-Fuqaha et al., 2015; de Jesus Júnior e Moreno, 2016; Madakam et al., 2015; Khan et al., 2012).

Figura 2.1: Visão geral *IoT* (Khan et al., 2012).

2.1 CARACTERÍSTICAS

A *IoT* pode ser vista como uma combinação de diversas tecnologias, as quais se complementam no sentido de viabilizar a integração dos objetos do ambiente físico ao mundo virtual. Dentro deste contexto, redes de sensores (*SNs - Sensor Networks*), redes de sensores sem fio (*WSNs - Wireless Sensor Networks*) , redes de sensores e atuadores sem fio (*WSANs - Wireless Sensor and Actuator networks*), redes *RFID* (*Radio-frequency identification*), redes *M2M* (*Machine-to-Machine*) e *SCADA* (*Supervisory Control and Data Acquisition*), são componentes essenciais da *IoT*, e uma série de características da *IoT* são herdadas de um ou mais desses componentes. As principais características da *IoT* são (Razzaque et al., 2016; Bhuvaneswari, 2017; Santos et al., 2016):

- Dispositivos heterogêneos: os dispositivos *IoT* são compostos por diferentes tipos de sensores ou atuadores, ou ambos que suportam conexão com a *Internet* por diferentes interfaces de comunicação;
- Recursos limitados: grande parte dos dispositivos *IoT* possuem recursos computacionais limitados, tais como, processamento, memória, conexão e energia;
- Interação espontânea: ocorre à medida que o dispositivo se move ou se aproxima do alcance de comunicação de outros dispositivos, levando à geração espontânea de eventos, normalmente no ambiente *IoT* uma interação significa que um evento é gerado na maioria das vezes sem intervenção humana;
- Rede de grande escala e grande número de eventos: em um ambiente *IoT*, milhares de dispositivos, ou coisas, podem interagir uns com os outros, produzindo uma grande quantidade de eventos como comportamento normal.
- Rede dinâmica e sem infraestrutura: os dispositivos são livres para se mover arbitrariamente e não dependem de nenhuma infraestrutura para suportar as suas operações.
- Contexto: um grande número de sensores irá gerar grandes quantidades de dados, que não terão valor até que sejam analisados, interpretados e entendidos.
- Inteligência: se refere à capacidade dos objetos de se auto-organizarem, compartilhando informações, dados e recursos, reagir e agir de acordo com situações e mudanças no ambiente.
- Diversidade de aplicações: a *IoT* pode oferecer seus serviços em diversos domínios de aplicações, tais como, transporte e logística, cuidados de saúde, ambientes inteligentes (casa, escritório), cidades, industrial, pessoal e social.
- Coleta de informações: as aplicações *IoT* coletam informações sobre as atividades realizadas por seus dispositivos.

2.2 ELEMENTOS

A *IoT* permite a comunicação de diversos objetos denominados de coisas através da *Internet*. Para fornecer esta funcionalidade, a literatura destaca seis elementos envolvidos neste processo (Yen e Tsai, 2010; Al-Fuqaha et al., 2015; Pandya e Champaneria, 2015; Madakam et al., 2015; Pawar e Ghumbre, 2016; Santos et al., 2016).

Figura 2.2: Elementos da *IoT* (Al-Fuqaha et al., 2015).

Conforme pode ser verificado na Figura 2.2, inicialmente o elemento de identificação deve identificar os objetos de forma única para então conectá-los à *Internet*, sendo considerado um dos elementos mais importantes para a *IoT*. Tecnologias como *RFID*, *NFC* (*Near Field Communication*) e endereçamento *IP* podem ser empregados para identificar os objetos. O

processo de identificação também é capaz de nomear e combinar os serviços de acordo com a sua demanda, diferenciando o *ID* do objeto de seu endereço *IP*.

Após a identificação do objeto, o sensoriamento, consiste na coleta de informações por parte dos objetos sobre o contexto ao seu redor bem como, armazenar ou encaminhar essas informações para a nuvem, ou banco de dados, onde as informações coletadas serão analisadas para realizar ações específicas com base nos serviços necessários. No caso dos atuadores, os objetos podem manipular o ambiente ou reagir de acordo com as informações obtidas.

Assim como o elemento de identificação, a comunicação também é um dos processos fundamentais para a *IoT*, pois, por meio dela é possível conectar objetos heterogêneos em conjunto para fornecer serviços inteligentes. As tecnologias de comunicação mais utilizadas na *IoT* são: *RFID*, *Wi-Fi*, *NFC*, *Bluetooth*, *ZigBee*, *6LoWPAN*, *Z-wave* e *LTE-Advanced*.

O elemento de computação, representa a unidade de processamento, que possibilita aos objetos a capacidade de computar dados. O microprocessador e o microcontrolador são alguns dos elementos computacionais comumente usados.

Os serviços em *IoT* são classificados em quatro classes, sendo o serviço relacionado à identidade, responsável por identificar os objetos do mundo real para o mundo virtual. O serviço de agregação de informações, é responsável por coletar e sumarizar dados brutos obtidos dos objetos inteligentes que precisam ser processados e enviados para as aplicações. O serviço de conhecimento colaborativo, atua sobre os serviços de agregação de informações e usa os dados obtidos para tomar decisões e reagir em conformidade. O serviço ubíquo, que visa prover serviços de colaboração e inteligência em qualquer momento e em qualquer lugar que eles sejam necessários.

Por fim, o elemento de semântica, refere-se à capacidade de extrair o conhecimento de modo inteligente de diferentes objetos para fornecer os serviços necessários. A extração de conhecimento inclui descobrir e usar recursos e informações de modelagem. Além disso, inclui reconhecer e analisar dados para dar sentido à decisão certa para fornecer o serviço exato. Para tanto, podem ser usadas diversas tecnologias tais como, *Resource Description Framework* (*RDF*), *Web Ontology Language* (*OWL*) e *Efficient XML Interchange* (*EXI*).

2.3 ARQUITETURA DOS DISPOSITIVOS *IOT*

De acordo com a (ITU, 2012), um dispositivo de *IoT* é um equipamento com os recursos obrigatórios de comunicação e recursos opcionais de detecção, atuação, captura, armazenamento e processamento de dados. Tais dispositivos, coletam vários tipos de informações e as fornecem às redes de informação e comunicação para processamento posterior. Alguns dispositivos também executam operações com base nas informações recebidas das redes de informação e comunicação.

A (ITU, 2019) categoriza os dispositivos de *IoT* como: dispositivos de transporte de dados, dispositivos de captura de dados, dispositivos de detecção e atuação e dispositivos gerais. Essa categorização diz respeito à maneira pela qual um dispositivo interage com mundo real. Os dispositivos de transporte e captura de dados são responsáveis pela leitura/gravação de dados de/para objetos físicos. Exemplos desses dispositivos incluem leitores de infravermelho (IR), leitores de cartão, leitores de código de barras, etc. Os dispositivos de detecção e atuação podem detectar ou medir informações relacionadas ao ambiente e convertê-las em sinais eletrônicos digitais. Um dispositivo geral, possui recursos incorporados de processamento e comunicação e pode incluir equipamentos e dispositivos para diferentes domínios de aplicação da *IoT*.

Com base nessa categorização, a (ITU, 2019) classifica os dispositivos de acordo com os recursos de poder de processamento e comunicação. Esses recursos, definem como o dispositivo se comunica e interage com outros dispositivos em um ambiente *IoT*; são eles que limitam

ou potencializam o funcionamento dos dispositivos. Assim, a capacidade de processamento define como os dispositivos podem executar tarefas computacionais e executar algoritmos. Por ouro lado, os recursos de comunicação definem como os dispositivos podem se conectar às redes de comunicação. Ao correlacionar tais classificações a (ITU, 2019) definiu um modelo de referência de arquitetura para dispositivos de baixo processamento e baixa conectividade (LPLC), dispositivos de baixo processamento e alta conectividade (LPHC) e dispositivos de alto processamento e alta conectividade (HPHC).

O modelo de referência para dispositivos de baixo processamento e baixa conectividade (LPLC), considera que em alguns casos, os dispositivos *IoT* simplesmente agem como uma interface para coletar dados de objetos físicos ou do ambiente e/ou executar operações em objetos físicos ou no ambiente. Assim, esses dispositivos não possuem recursos de processamento suficientes para tomar decisões ou executar algoritmos complexos; eles também não têm recursos de conectividade suficientes para se conectar diretamente às redes de comunicação. Por esses motivos, é necessário um *gateway* para atuar como intermediário entre esses dispositivos e a *IoT*. Conforme pode ser verificado na Figura 2.3, a entidade funcional de detecção/atuação/captura de dados é responsável por fornecer funções para ler dados de sensores, gravar dados em atuadores e capturar dados de dispositivos portadores de dados ou suporte de dados conectados a objetos físicos; a entidade funcional de manipulação de mensagens é responsável por fornecer funções para enviar e receber mensagens, usando um protocolo da camada de aplicação, também pode fornecer uma máquina de estado para lidar com as mensagens recebidas; a entidade funcional de acesso ao *gateway* fornece funções para gerenciamento de comunicação com o *gateway*; por fim, entidade a funcional de gerenciamento de hardware, fornece funções para acessar o hardware (sensores e/ou atuadores, interfaces de comunicação física, periféricos de hardware como temporizadores, conversores de analógico para digital, etc.).

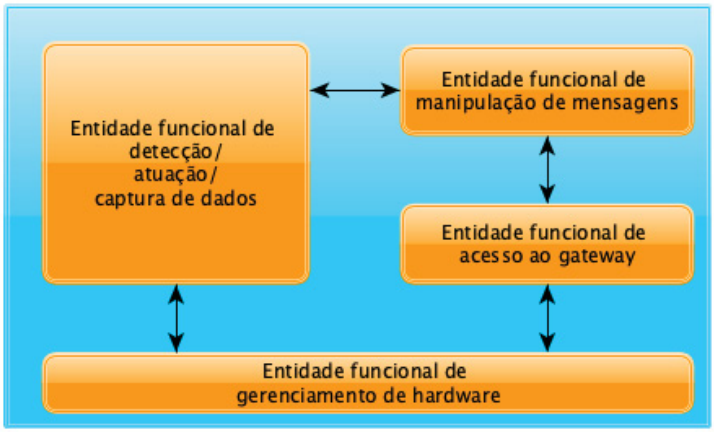


Figura 2.3: Arquitetura *LPLC*.
Adaptado de (ITU, 2019).

O modelo de referência de dispositivos de baixo processamento e alta conectividade (LPHC), considera que estes dispositivos possuem recursos de conectividade suficientes para se comunicar diretamente com a *Internet*. Portanto, não há necessidade de *gateways* mediando a comunicação entre os dispositivos e as aplicações ou serviços em nuvem. No entanto, estes dispositivos ainda não possuem recursos de processamento suficientes para tomar decisões ou executar algoritmos complexos. Conforme pode ser verificado na Figura 2.4, neste modelo são adicionadas duas novas entidades em relação ao modelo de referência *LPLC*. A entidade funcional da interface de serviço/aplicação, fornece funções para interagir com o serviço em

nuvem da *IoT* ou aplicação *IoT*, enviar e receber mensagens para o serviço em nuvem da *IoT* ou aplicação *IoT*, registrar/autenticar o dispositivo, etc; a entidade funcional de gerenciamento de conectividade, fornece funções para o gerenciamento de conectividade entre o dispositivo e a rede de comunicação.

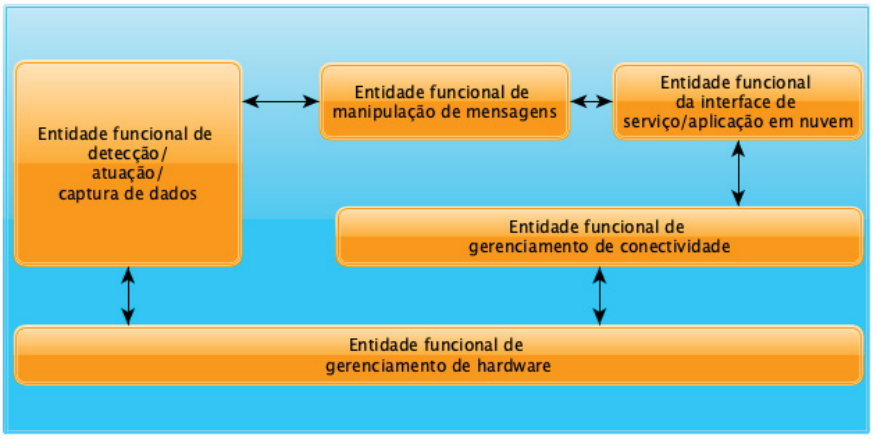


Figura 2.4: Arquitetura *LPHC*.
Adaptado de (ITU, 2019).

Por fim, o modelo de referência de dispositivos de alto processamento e alta conectividade (HPHC), considera que estes dispositivos não possuem apenas alta capacidade de conectividade, tornando-os capazes de se conectar diretamente a aplicações e serviços em nuvem, mas também possuem capacidade de processamento suficientemente alta para tomar decisões e executar algoritmos complexos (por exemplo, algoritmos relacionados à inteligência artificial (AI)). Esses dispositivos são autônomos; eles tomam decisões sobre suas próprias funções e também podem coordenar outros dispositivos. Conforme pode ser verificado na Figura 2.5, neste modelo são adicionadas cinco novas entidades em relação ao modelo de referência *LPHC*. A entidade funcional do mecanismo de execução de aplicações, fornece funções para instalar, excluir, atualizar e executar aplicações nos dispositivos, também fornece aos aplicativos acesso a outras entidades funcionais. A entidade funcional de gerenciamento de dispositivos, fornece funções para gerenciar outros dispositivos conectados ao dispositivo e ao próprio dispositivo. A entidade funcional de compartilhamento de informações, fornece funções como interação dispositivo a dispositivo (troca de dados entre dispositivos), descoberta de serviço, monitoramento de serviço e interoperabilidade de descoberta de serviço. A entidade funcional de análise de dados, fornece funções para processamento de dados e decisão autônoma executando análises e algoritmos de *AI*. Por fim, a entidade funcional de armazenamento de dados, fornece funções de armazenamento e recuperação de dados.

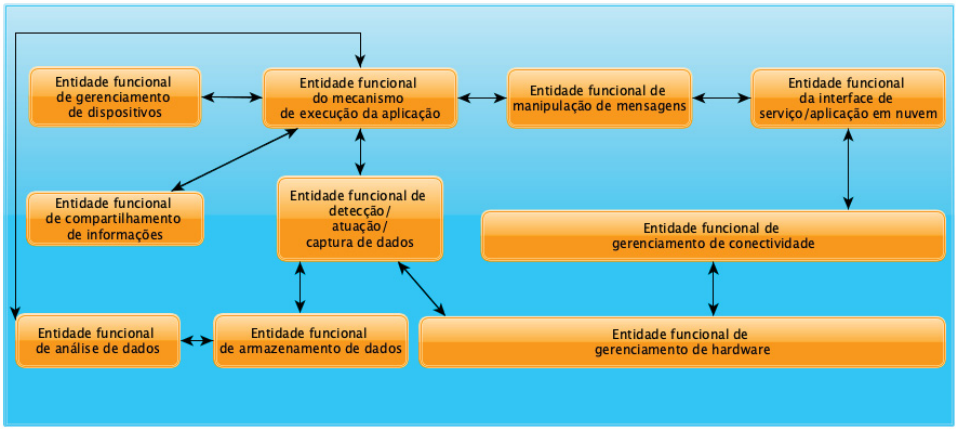


Figura 2.5: Arquitetura *HPHC*.
Adaptado de (ITU, 2019).

2.4 MODELOS DE COMUNICAÇÃO

A *RFC* 7452 (Tschofenig et al., 2015), define quatro padrões de comunicação para o ambiente *IoT*. Sendo que mais de um padrão pode ser utilizado em um mesmo dispositivo *IoT*. Os padrões definidos pela *RFC* 7452 são:

- Comunicação dispositivo-dispositivo: neste padrão de comunicação, os dispositivos comunicam-se diretamente uns com os outros (Fig. 2.6). Estes dispositivos se comunicam em vários tipos de redes, incluindo rede *IP* ou *Internet*. Muitas vezes, esses dispositivos usam protocolos de comunicação como *Bluetooth, Z-Wave, ZigBee ou 6LoWPAN* para estabelecer comunicações diretas;

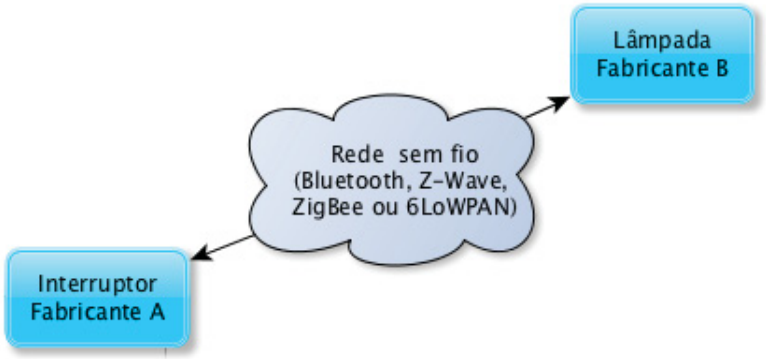


Figura 2.6: Comunicação dispositivo-dispositivo.
Adaptado de (Singh e Gaur, 2017).

- Comunicação dispositivo-nuvem: neste padrão de comunicação os dispositivos conectam-se diretamente a um provedor de serviços para troca de dados (Fig. 2.7). Esta abordagem aproveita os mecanismos de comunicação existentes, como conexões *Ethernet* ou *WLAN* para estabelecer a conexão entre o dispositivo e a rede *IP*, que finalmente se conecta ao serviço da nuvem;

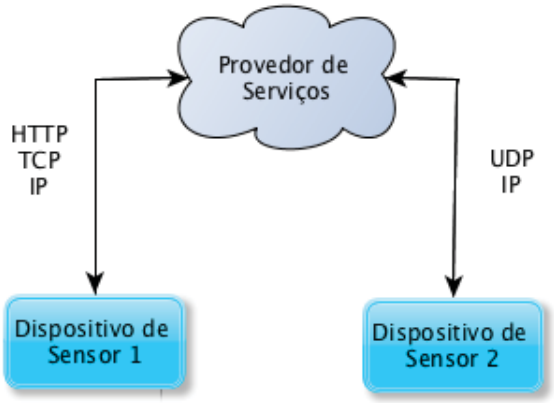


Figura 2.7: Comunicação dispositivo-nuvem.
Adaptado de (Singh e Gaur, 2017).

- Comunicação dispositivo-gateway: neste padrão de comunicação os dispositivos se conectam a um *gateway* para ter acesso à *Internet* (Fig. 2.8).

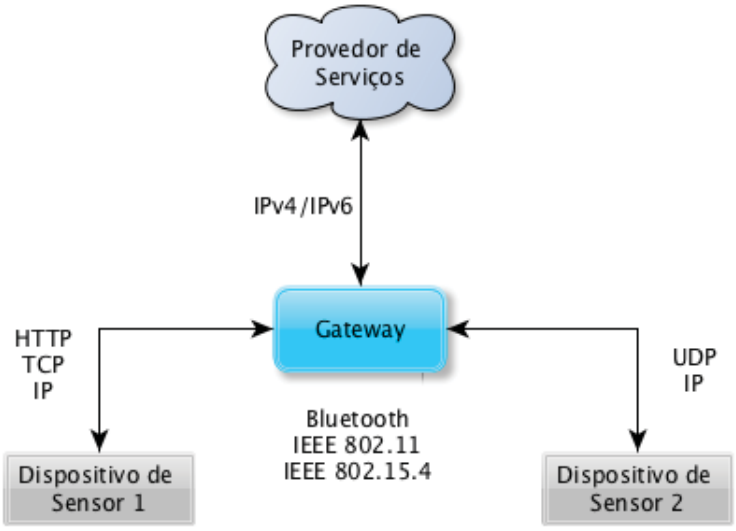


Figura 2.8: Comunicação dispositivo-gateway.
Adaptado de (Singh e Gaur, 2017).

- Comunicação para compartilhamento de dados *back-end*: este padrão refere-se a uma arquitetura de comunicação que permite a exportação e a análise de dados para um serviço na nuvem em combinação com outras fontes de dados (Fig. 2.9).

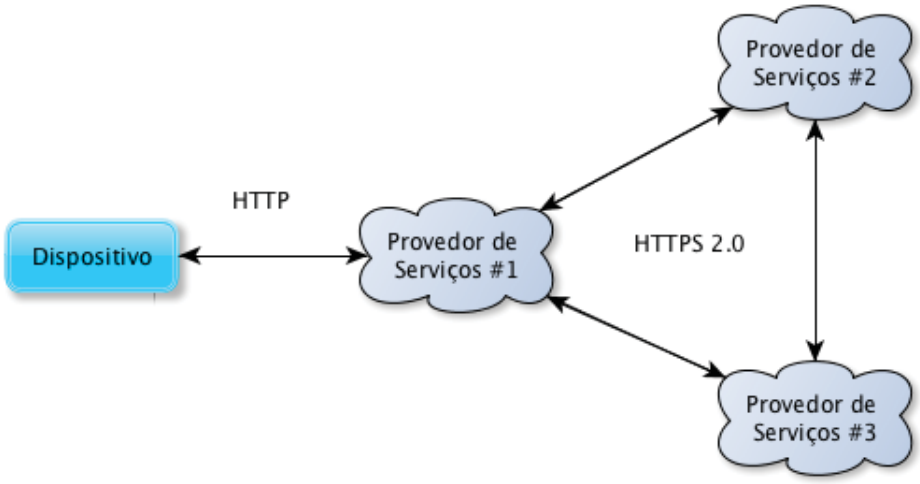


Figura 2.9: Compartilhamento de dados *back-end*.
Adaptado de (Singh e Gaur, 2017).

2.5 TECNOLOGIAS DE COMUNICAÇÃO

As tecnologias de comunicação em um ambiente *IoT* conectam dispositivos heterogêneos para fornecer serviços específicos. Diferentes tecnologias de comunicação sem fio podem ser usadas para conectar estes dispositivos. A escolha de uma ou alguma forma de combinação destas tecnologias deve considerar fatores como, aplicação, alcance, requisitos de dados, segurança, demanda de energia e duração da bateria (Dragomir et al., 2016; Samie et al., 2016; Samuel, 2016; Al-Sarawi et al., 2017). As principais tecnologias de comunicação sem fio para *IoT* são descritas a seguir.

2.5.1 Celular

A tecnologia *Celular* é adequada para dispositivos com fonte de energia própria que necessitam enviar dados para longas distâncias, podendo aproveitar as capacidades de comunicação de alta velocidade das tecnologias *3G/4G*. Esta tecnologia possui um alto consumo de energia em comparação as outras tecnologias. No entanto, a sua utilização em locais afastados e baixa mobilidade podem compensar esse gasto. No Brasil, a frequência utilizada para o *3G* é de 1900MHz e 2100MHz (*UMTS*), já o padrão *4G* (*LTE*) utiliza a frequência 2500MHz. A taxa de transferência no padrão *3G* é de 1$Mbps$ e no padrão *4G* pode alcançar até 10$Mbps$ (Pandya, 2015).

2.5.2 SigFox

A tecnologia *SigFox* é projetada para dispositivos com baixas velocidades de transferência de dados (de 10 a 1000 *bits* por segundo), oferecendo uma rede robusta, eficiente em termos de consumo de energia e escalável, podendo se comunicar com milhões de dispositivos operados por bateria em áreas de vários quilômetros quadrados. O raio de cobertura, em zonas urbanas

está entre 3*km* e 10*km* e em zonas rurais entre 30*km* e 50*km*. A taxa de tranferência varia entre 10*bps* e 1000*bps*. O *MTU* utilizado é de 96 *bytes* e opera na faixa de 900*MHz* (Raza et al., 2017).

2.5.3 LoRaWAN

A tecnologia *LoRaWAN* é projetada para fornecer comunicação de longa distância com consumo mínimo de energia para dispositivos com taxa de transmissão de dados que variam de 0,3 kbps a 50 kbps. Utiliza a frequência *ISM sub-GHz*, o que permite que as ondas penetrem grandes estruturas e superfícies com raio de 2*km* a 5*km* em meio urbano e 45*km* no meio rural. Utiliza frequências de 109 *MHz*, 433 *MHz*, 866 *MHz*, 915 *MHz*. O *MTU* adotado pelo padrão *LoRaWAN* é de 256 *bytes* (Mikhaylov et al., 2017).

2.5.4 6oLWPAN

O *6oLWPAN* é uma tecnologia de camada de rede que permite conectividade à *Internet* para dispositivos com restrição de recursos computacionais utilizando o protocolo *IPv6* em redes *IEEE 802.15.4* por meio do encapsulamento e fragmentação do cabeçalho de pacotes *IPv6* em frames *IEEE 802.15.4*. Utiliza a frequência de 2,4*GHz*, do padrão *IEEE 802.15.4* e está sendo adaptado e usado em uma variedade de outras mídias de rede, incluindo baixa potência de Sub-1*GHz RF*, *Bluetooth* Smart, controle de linha de energia (*PLC*) e *Wi-Fi* de baixa potência. O *MTU* utilizado por esta tecnologia é de até 256 *bytes* (Moinuddin et al., 2017).

2.5.5 *ZigBee*

O *ZigBee* é uma tecnologia de área pessoal sem fio (*WPAN*) de baixo consumo de energia e baixa taxa de transmissão de dados, desenvolvida para aplicações de monitoramento e controle. O *ZigBee* opera na frequência 2.4*GHz ISM*, mas é capaz de operar em outras duas frequências, 868*MHz* ou 915*MHz ISM*. Esta tecnologia possuiu taxa de transferência de até 250*Kbps* (Malhotra et al., 2015).

2.5.6 *Bluetooth Low Energy*

O *Bluetooth Low Energy* é uma tecnologia projetada para aplicações *IoT* de curto alcance, baixa largura de banda e latência, reduzindo significativamente o consumo de energia dos dispositivos e oferecendo uma infra-estrutura de conexão direta entre eles. Atualmente, o órgão *Bluetooth SpecialInteres Group* (*SIG)* é responsável por criar, testar e manter a tecnologia. Além disso, *Bluetooth* é uma das principais tecnologias de rede sem fio para *Personal Area Networks - PANs*, que é utilizada em *smartphones*, *headsets*, *PC's* entre outros. A tecnologia *Bluetooth* é dividida em, *Bluetooth Classic Basic Rate/Enhanced Data Rate* (*BR/EDR*), que são as versões 2.0 ou inferiores, o *Bluetooth High Speed* (*HS*), versão 3.0 e o *Bluetooth Low Energy* (*BLE*), versão 4.0 ou superior. A taxa de transferência desta tecnologia é de até 1*Mbps* (Rahman e Jain, 2015).

2.5.7 *RFID*

O *RFID* é a combinação das tecnologias baseadas em radiofrequência e de *microchip* para a identificação automática de objetos, pessoas, animais, veículos, entre outros. O *RFID* opera na frequência 13.56*MHz* e possuiu taxa de transferência de 4*Mbps* (Al-Sarawi et al., 2017).

2.5.8 *NFC*

O *NFC* é uma tecnologia de comunicação sem fio de curto alcance que permite interações bidirecionais simples entre os dispositivos a uma frequência de 13,56MHz e em distâncias de 10 cm a 1 m. O *NFC* possuiu uma taxa de transferência de 424*Kbps* (Timalsina et al., 2012).

2.5.9 *Z-Wave*

O *Z-Wave* é uma tecnologia de comunicação sem fio de baixa potência, para aplicações de controle remoto em ambientes comerciais e residenciais de pequeno porte. É otimizado para comunicação confiável e de baixa latência com taxa de transmissão de dados de até 100 Kbps, operando em uma frequência de 900*Mhz* (Samuel, 2016).

2.5.10 *Thread*

O *Thread* é uma nova tecnologia de rede *IP* com suporte ao protocolo *IPv6* baseado na tecnologia *6LowPAN*, para o ambiente de automação residencial. O *Thread* opera na frequência de 2.4*GHz* e possuiu taxa de transferência de até 250*Kbps* (Samuel, 2016).

2.5.11 *WiFi*

A tecnologia de comunicação *WiFi* permite a conectividade entre dispositivos eletrônicos através de um ponto de acesso ou em modo *ad hoc*. É a tecnologia de comunicação mais popular, estando presente em quase todos os lugares, fazendo parte do cotidiano das casas, escritórios, indústrias e até espaços públicos das cidades. O *WiFi* opera em frequências de 2.4 a 5 GHz e possui uma taxa de transferência de até 1*Gbps* (Robertazzi, 2017).

Tabela 2.1: Principais tecnologias de comunicação em *IoT*

	Tecnologia										
Características	Celular	SigFox	LoRaWAN	6oLWPAN	ZigBee	Thread	BLE	RFID	NFC	Z-Wave	WiFi
Padrão	2G,3G,4G e 5G	SigFox	LoRa	802.15.4	802.15.4	802.15.4	802.15.1	ISO / IEC	ISO 13157	ITU-T	802.11
Frequência	450-3600MHz	868-902MHz	109 - 915MHz	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz	13.56 MHz	13.56 MHz	900 MHz	2.4 - 5 GHz
Rede	WNAN	LPWAN	LPWAN	WPAN	WPAN	WPAN	WPAN	P2P	P2P	WPAN	WLAN
Alcance (m)	Diversos Km	10 - 50Km	2 - 45km	10 – 100m	10 – 100m	10 – 100m	15 – 30m	200m	0,1 – 1m	30	100m
Taxa de Transferência	2Kbps - 1Gbps	100 - 600bps	290bps - 50 Kbps	20/40/250 Kbps	20/40/250 Kbps	20/40/250 Kbps	1 Mbps	4 Mbps	424 Kbps	100 Kbps	1 Gbps
Tamanho da Mensagem (B)	-	12	230	127	127	127	47	12	255	64	2312

2.6 CONFIANÇA EM *IOT*

Confiança é um conceito das ciências sociais e na literatura, é possível encontrar um grande número de definições a seu respeito. Uma das definições mais citadas na literatura a define como "A expectativa de uma pessoa sobre as ações dos outros que afetam a escolha da primeira pessoa". Deste modo, a confiança é um nível particular de avaliação subjetiva com o qual uma entidade acessa outra ou um grupo de atividades para executar uma determinada ação, antes mesmo de poder monitorar tal ação, em um contexto que afete sua própria ação (Mendoza e Kleinschmidt, 2015; Gambetta et al., 2000).

Em *IoT* a confiança pode ser definida como um termo que envolve a análise do comportamento dos dispositivos conectados à mesma rede. A confiança fornece ao dispositivo uma maneira de avaliar outro dispositivo semelhante para tomar decisões adequadas a fim de estabelecer uma comunicação eficiente e confiável entre eles. Portanto, a relação de confiança entre dois dispositivos ajuda a influenciar os futuros comportamentos de suas interações. Assim, quando os dispositivos confiam uns nos outros, eles podem compartilhar serviços e recursos até certo ponto. Desta forma um mecanismo de confiança viável para um ambiente *IoT*, deve lidar com a escalabilidade e a heterogeneidade deste ambiente, visto que potencialmente um ambiente *IoT* terá um número elevado de dispositivos, os quais podem possuir limitação de recursos computacionais ou não (Mahalle et al., 2013; Billure et al., 2015; Al-Fuqaha et al., 2015; Kumar et al., 2016; Guo et al., 2017; Fremantle e Scott, 2017).

2.6.1 Sistema de gerenciamento de confiança

De acordo com (Bao et al., 2011), um sistema gerenciamento de confiança é um mecanismo que permite que os objetos estabeleçam conexões com um nível pré-definido de confiança entre si, contribuindo assim, para a segurança do ambiente. Em ambientes *IoT*, onde os objetos atuam de forma colaborativa, compartilhando serviços e trocando dados, há a necessidade de garantir que as conexões sejam efetuadas entre indivíduos confiáveis, de modo a evitar possíveis quebras de serviço e instabilidades na rede. Dentro deste contexto, um sistema de gerenciamento de confiança deve ser capaz de coletar informações dos dispositivos da rede e com base nessas informações calcular o valor de confiança dos mesmos. Essas informações devem ser armazenadas e posteriormente distribuídas pela rede (Brittes et al., 2016).

De acordo com (Guo et al., 2017), cinco propriedades devem ser consideradas para o projeto de um sistema de gerenciamento de confiança para *IoT*. A primeira propriedade a ser considerada diz respeito a composição de confiança, ou seja, quais componentes devem ser considerados no cálculo de confiança. Os componentes para a composição da confiança incluem confiança de qualidade de serviço (*QoS*) e confiança social, sendo que, a confiança de *QoS* refere-se à crença de que um dispositivo *IoT* é capaz de fornecer um serviço de qualidade em resposta a uma solicitação de serviço, por outro lado, a confiança social deriva da relação social entre proprietários de dispositivos de *IoT* e é medida pela intimidade, honestidade, privacidade, centralidade e conectividade. A segunda propriedade considerada, refere-se à agregação das evidências de confiança coletadas por auto-observações ou *feedbacks* dos dispositivos vizinhos. As principais técnicas de agregação de confiança investigadas na literatura de acordo com (Guo et al., 2017), incluem soma ponderada, teoria da crença, inferência bayesiana, lógica fuzzy e análise de regressão.

A terceira propriedade diz respeito a propagação das evidências de confiança para os dispositivos, em geral, três esquemas de propagação de confiança são considerados. O primeiro esquema considera a propagação de forma centralizada, assim, o valor de confiança é coletado e calculado por uma entidade central. Desta forma, o valor de confiança dos dispositivos

ficam disponíveis para toda a rede, onde cada dispositivo pode solicitar informações sobre os dispositivos como os quais pode realizar transações com certo nível de confiança. O segundo esquema, considera propagação das evidências de forma descentralizada, neste esquema, cada dispositivo é responsável por obter, calcular e armazenar os valores de confiança. As informações podem ser obtidas pelos dispositivos periodicamente ou por eventos de interação. No terceiro e último esquema, as informações podem ser armazenadas e distribuídas de forma hibrida, ou seja, é considerado a utilização em conjunto das formas centralizada e distribuída.

A quarta propriedade a ser considerada diz respeito a atualização da confiança e refere-se ao momento em que as informações de confiança serão atualizadas, em geral, exitem dois esquemas, o baseado em eventos e o orientado pelo tempo. No esquema baseado em eventos, todos os dados de confiança em um nó são atualizados após uma transação ou evento ser realizado. No esquema orientado pelo tempo, as evidências (auto-observações ou recomendações) são coletadas periodicamente e a confiança é atualizada com uma das técnicas de agregação de confiança. No caso de nenhuma evidência ser coletada, a decadência da confiança ao longo do tempo é frequentemente aplicada, visto que é preciso confiar nas informações recentes mais do que nas informações anteriores.

Por fim, a propriedade de formação de confiança, refere-se como formar a confiança geral de várias propriedades de confiança. Na literatura, a formação de confiança é considerada a partir do aspecto de confiança única ou confiança múltipla. A confiança única refere-se ao fato de que apenas uma propriedade de confiança é considerada, por exemplo, a qualidade de serviço, assim, um dispositivo *IoT* será avaliado com relação a sua capacidade de produzir um serviço de qualidade quando solicitado. A confiança múltipla implementa a crença comum de que a confiança é multidimensional, portanto, várias propriedades de confiança devem ser consideradas para a formação de confiança.

Além das propriedades descritas, um sistema de gerenciamento de segurança deve ainda, apresentar resiliência diante de nós maliciosos, visto que, em um ambiente *IoT* um nó malicioso visa quebrar a funcionalidade básica da rede que é o compartilhamento de serviços. Desta forma, um nó malicioso pode executar ataques de autopromoção, para promover a sua importância (fornecer boas recomendações de si mesmo) e ser selecionado como um prestador de serviço, mas depois parar de prestar os serviços ou prestar um serviço de má qualidade. Além disso, um nó malicioso pode arruinar a reputação de nós não maliciosos (fornecendo recomendações ruins contra nós não maliciosos - Ataque de (*bad-mouthing attack*)) diminuindo a hipótese de nós não maliciosos serem selecionados como provedores de serviços. Um nó malicioso, pode aumentar a reputação de nós maliciosos (fornecendo boas recomendações para ele - Ataques de *good-mouthing*) aumentando a hipótese desses nós serem selecionados como prestadores de serviços. Por fim, um nó malicioso, pode se comportar como um nó não malicioso ou um nó malicioso alternativamente, fazendo com que o sistema de gerenciamento considere o comportamento de um nó malicioso como um erro temporário (Ataques de *On-Off*) (Mendoza e Kleinschmidt, 2015; Guo et al., 2017; Jøsang et al., 2007).

2.7 CONSIDERAÇÕES SOBRE O CAPÍTULO

Neste capítulo foram apresentados os conceitos e fundamentos necessários para o entendimento desta dissertação. Nas seções 2.1, 2.2, 2.3, 2.4 e 2.5 foram descritos as características, elementos, arquitetura, modelo e tecnologias de comunicação utilizados em *IoT*, possibilitando assim o entendimento de seu funcionamento e aplicabilidade.

Por fim, a seção 2.6 abordou especificamente a confiança para *IoT*. Nesta seção é possível compreender sua conceituação, a estrutura de um sistema de gerenciamento de confiança e como nós maliciosos podem comprometer a confiabilidade em um ambiente *IoT*.

A fundamentação teórica obtida neste capítulo é a base para o desenvolvimento da proposta deste trabalho. O próximo capítulo apresenta o estado da arte dos sistemas de gerenciamento de confiança, considerando os conceitos apresentados na seção 2.6.1 deste capítulo.

3 GERENCIAMENTO DE CONFIANÇA

Esta seção apresenta o estado da arte para o gerenciamento de confiança para um ambiente de *IoT*. Os trabalhos foram selecionados de acordo com os requisitos para a composição de um sistema de gerenciamento de confiança abordados em (Guo et al., 2017).

O objetivo do trabalho (Chen et al., 2011) é desenvolver um modelo de gerenciamento de confiança e reputação baseado na teoria *fuzzy* para ambientes *IoT*. Nesta abordagem, as relações de confiança são baseadas em evidências ou reputações criadas pelas interações anteriores dos nós, considerando apenas a porção de pacotes encaminhados corretamente. Desta forma, os autores criaram um modelo matemático de confiança *fuzzy*, onde cada nó emprega um processo de monitoramento em modo promíscuo para coletar informações sobre o comportamento do encaminhamento de pacotes dos nós vizinhos. Assim, a avaliação da confiança local, é baseada na observação direta de um nó de origem a um nó de destino e utiliza uma função *fuzzy* para o cálculo da confiança direta. Neste trabalho, a avaliação global de confiança refere-se, ao fato do nó de origem não possuir uma observação direta com o nó de destino, assim, faz uso da observação indireta, solicitando experiências de reputação a seus vizinhos e as utiliza em uma função *fuzzy* para calcular o valor da confiança indireta. Considerar como métrica a porção de pacotes encaminhados corretamente é uma vantagem nesta abordagem, com relação à avaliação da confiança. No entanto, a necessidade da placa de rede estar modo promíscuo, faz com que o dispositivo aceite todos os pacotes de entrada, independente de seus destinos, fato este, que pode aumentar a utilização dos recursos computacionais do dispositivo, assim, avaliar apenas os pacotes encaminhados diretamente seria uma alternativa mais vantajosa quanto a utilização dos recursos.

Nos trabalhos (Bao e Chen, 2012) e (Chen et al., 2016a) os autores propõem um protocolo de gerenciamento de confiança dinâmico, com o objetivo de melhorar a segurança e aumentar o desempenho das aplicações em um ambiente social de *IoT*. Estas abordagens são centradas no usuário, assim, cada dispositivo (nó) tem um proprietário e um proprietário pode ter muitos dispositivos e, cada proprietário possui uma lista de amigos que representa suas interações sociais. Para garantir a escalabilidade do sistema, um nó pode manter apenas sua avaliação de confiança para um conjunto limitado de nós nos quais está mais interessado. Os autores usam a relação de amizade social entre os proprietários de dispositivos para caracterizar a cooperatividade, formando assim a hipótese de que os amigos provavelmente cooperam uns com os outros. A confiança de cooperação do nó i em relação ao nó j é calculado como a proporção do número de amigos comuns em relação ao número total de nós amigos i e j. Quando o nó i e o nó j se encontram e interagem diretamente uns com os outros, eles podem trocar suas listas de amigos assim, o nó i pode validar um amigo na lista de j se ele for seu amigo em comum. Para as recomendações, ou seja, se o nó j não for o nó k o nó i não terá observação direta sobre o nó j e usará sua experiência passada e recomendações do nó k para obter o valor de confiança de j. Ao considerar apenas as relações sociais dos proprietários dos dispositivos para composição da confiança, os autores tornam a abordagem proposta restrita a um ambiente muito específico, dificultando assim sua implementação em ambientes onde os dispositivos não possuem interação humana direta.

Em (Bao et al., 2013) é projetado e analisado um protocolo de gerenciamento de confiança escalável e adaptável para um sistema de *IoT* social, onde os nós podem entrar e sair dinamicamente e formar comunidades de interesse, conforme pode ser observado na Figura 3.1. Nesta abordagem, cada nó possui um endereço exclusivo na comunidade de interesse e não existe

uma autoridade de confiança centralizada. Desta forma, cada nó mantém sua própria avaliação de confiança em relação a outros nós. Para o cálculo da avaliação de confiança de um nó em relação a outro nó, os autores utilizam o sistema de reputação *Bayesian* onde cada nó calcula a confiança de acordo com suas observações diretas. Os nós também trocam seus resultados de avaliação de confiança em relação a outros nós de forma indireta, através de recomendações. A atualização de confiança direta é atualizada a cada encontro ou atividade de interação, enquanto a confiança indireta é atualizada periodicamente. Para garantir a escalabilidade do sistema, um nó mantém apenas os resultados de avaliação de confiança para um subconjunto limitado de nós na mesma comunidade de interesse, assim, o nó deve decidir quais valores de confiança devem ser mantidos. Para resolver este problema os autores utilizam a estratégia que os nós devem manter apenas os valores de confiança mais altos e as interações mais recentes com outros nós. O sistema proposto possibilita a atualização dos valores de confiança com o mínimo de gasto computacional, ou seja, uma única interação. Assim, quando dois nós se encontram ou estão envolvidos em uma atividade de interação direta, eles podem observar um ao outro diretamente e atualizar suas avaliações de confiança. Entretanto, ao não incluir no mesmo processo as recomendações, o sistema pode estar armazenando informações desatualizadas sobre os nós recomendados, visto que, eles mudam de comportamento constantemente e aumentar o gasto computacional para atualizar individualmente os valores de confiança dos nós indiretos.

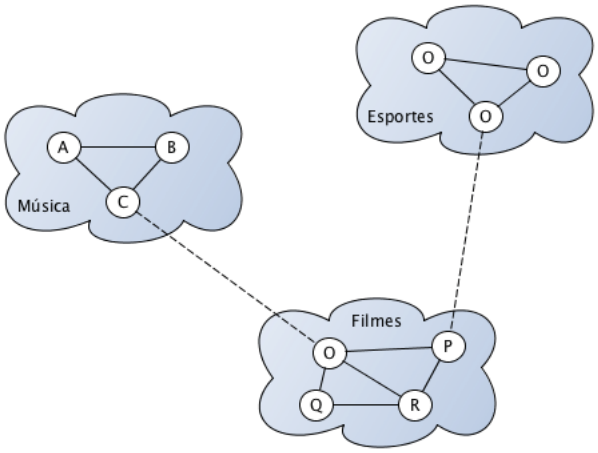


Figura 3.1: Comunidades de Interesse em *IoT*.
Adaptado de (Bao et al., 2013).

O trabalho (Saied et al., 2013) propõem um novo sistema de gerenciamento de confiança para *IoT*. Esta abordagem, considera um gerenciador de confiança centralizado, que armazena todos os relatórios de reputação enviados por servidores individuais. Este modelo, conforme pode ser observado na Figura 3.2, envolve uma sucessão cíclica das fases de, (i) inicialização e coleta de informações, (ii) seleção de entidades, (iii) transação e avaliação, (iv) avaliação do serviço recebido e (v) a aprendizagem. Este trabalho diferencia os conceitos de confiança e reputação. Desta forma, a confiança é usada para determinar a capacidade de um nó em cumprir uma tarefa específica e a reputação é usada para se referir à opinião global sobre a confiabilidade de um nó na rede após ter fornecido assistência para vários serviços. Nesta abordagem, os servidores são responsáveis por coletar as informações dos nós e repassar ao gerenciador de confiança um relatório com todas as informações coletadas. Assim, após receber um relatório de um servidor avaliando um nó, o gerenciador de confiança aprende sobre seu comportamento e pode, então atualizar a pontuação de confiança de todos os nós que já enviaram um relatório sobre

o mesmo servidor em condições semelhantes e, atualizar o nível de reputação dos nós. Apesar de os autores considerarem a presença de servidores confiáveis para coletar e disseminar dados de confiança, esta abordagem continua possuindo um único ponto de falha que é o gerenciador de confiança centralizado. Outro fator a ser considerado é que esta abordagem não é viável para a maioria dos ambientes de *IoT*, devido a sua complexidade para implementação.

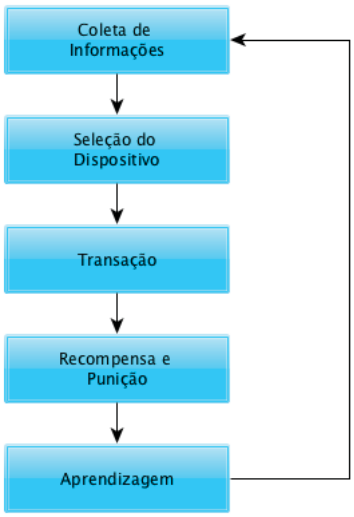


Figura 3.2: Fases do modelo proposto.
Adaptado de (Saied et al., 2013)

.

O trabalho (Mahalle et al., 2013) propõe a estrutrua *FTBAC (Fuzzy approach to the Trust Based Access Control)* para o controle de acesso dinâmico baseado em confiança para um ambiente *IoT* distribuído. A Figura 3.3 demonstra a estrutrua proposta. Esta abordagem propõe um *score* de confiança com base nos valores dos parâmetros de experiência *(EX)*, conhecimento *(KN)* e recomendação *(RC)*. Desta forma, o cálculo dos parâmetros *EX, KN e RC*, para a confiança do dispostivo *A* para o dispositivo *B* em um contexto particular *C* é baseado no histórico de interações anteriores *K*. Com o registro das interações bem-sucedidas e mal-sucedidas o valor *EX* para as interações *K* pode ser gravado. Para calcular o parâmetro *EX* é realizada uma soma normalizada de todas as experiências de confiança desse nó. Para um alto grau de confiança, o dispositivo *A* requer conhecimento *KN* completo sobre o dispositivo *B*, sendo este o segundo recurso característico para a avaliação da confiança. Segundo os autores, conhecimento insuficiente ou menor pode influenciar o valor da confiança. O cálculo de *KN* no contexto *C* é realizado pela soma ponderada dos valores do conhecimento direto e indireto. O terceiro recurso característico para a avaliação de confiança é o *RC*, que pode ser obtido pela soma ponderada dos valores de *RC* de *n* números de dispositivos sobre o dispositivo *B* no contexto *C*. Após o cálculo de cada um desses parâmetros a confiança é calculada através de uma base de regras difusas. Considerar apenas o valor de interações bem-sucedidas e mal-sucedidas entre o par de nós envolvidos é uma vantagem desta abordagem, no entanto, a utilização de várias métricas para a composição da confiança resulta em um tempo maior para se calcular a confiança e também maior consumo de recursos.

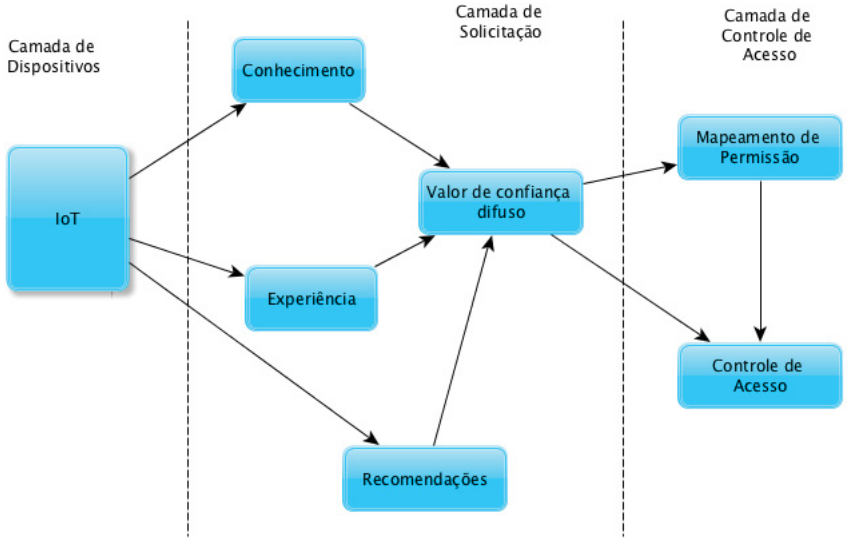


Figura 3.3: Estrutura do *FTBAC*.
Adaptado de (Mahalle et al., 2013).

O objetivo do trabalho (Wang et al., 2013) é fornecer uma estrutura geral para o desenvolvimento do gerenciamento de confiança para *IoT*. A Figura 3.4 oferece uma visão geral da estrutura proposta. Os autores consideram ser difícil o estabelecimento de um mecanismo de confiança para a *IoT* na sua totalidade, deste modo, estabeleceram mecanismos de confiança para a *IoT* em forma de camadas. Assim, a camada de sensor, inclui os dispositivos físicos, rede de sensores sem fio e estação base. A camada principal, inclui principalmente a rede de acesso e a *Internet*. A camada de aplicação, inclui várias redes distribuídas (por exemplo, *P2P*, *grid*, computação em nuvem), aplicações e interfaces de aplicações também são consideradas. O modelo proposto também considera as etapas de avaliação de confiança, transmissão de confiança e tomada de decisão de confiança como parte do gerenciamento de confiança. Segundo os autores, o mecanismo de gerenciamento de confiança deve lidar com o fluxo de informações e impedir que as informações de privacidade sejam acessadas por outro dispositivo não confiável, sendo necessário avaliar as informações de confiança para cada uma das camadas. Neste trabalho, os autores assumem que a transmissão de informação é segura, assim, a informação de confiança será transmitida para a camada superior sequencialmente. Para a tomada de decisão, os autores propõem duas categorias de tomada de decisão com base na confiança. Sendo a primeira, uma política de controle de acesso baseada em confiança, a qual pode decidir se fornecerá um serviço e em que grau fornecerá serviços de acordo com os valores de confiança dos usuários quando os usuários exigirem determinados serviços. A segunda categoria é a decisão auto-organizada, este tipo de tomada de decisão seleciona o prestador de serviço que oferecer melhor *QoS*. Este trabalho aborda uma estrutura geral para o desenvolvimento de um sistema de gerenciamento de confiança, os autores tratam do assunto de forma teórica. Desta forma não é possível realizar uma análise mais aprofunda do trabalho proposto.

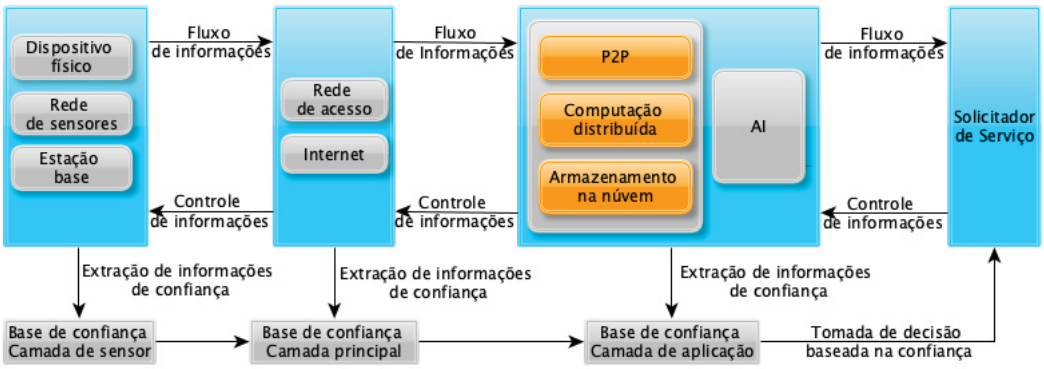


Figura 3.4: Visão geral do modelo proposto.
Adaptado de (Wang et al., 2013)

.

O objetivo principal do trabalho (Nitti et al., 2014) é o projeto de um modelo de confiança dinâmica para a avaliar o nível de confiabilidade dos nós em um ambiente *IoT* social. De acordo com os autores, um nó é capaz de fornecer um ou mais serviços, desta forma, um nó pode solicitar um serviço, consultando seus vizinhos, a fim de receber o conjunto de nós que podem fornecer o serviço solicitado, conforme pode ser verificado na Fig. 3.5. Diante deste cenário, é proposto pelos autores, um sistema de gerenciamento de confiança composto por dois modelos, onde o modelo de confiabilidade subjetiva destina-se a evitar um único ponto de falha no sistema, e o modelo de confiabilidade objetiva destina-se a otimizar o desempenho do sistema. Assim, no primeiro modelo o nó armazena e gerência o *feedback* necessário para calcular o valor da confiança localmente. Neste modelo, o nó obtém as informações necessárias para o cálculo da confiança através de sua experiência direta com os nós vizinhos e pela opinião dos vizinhos em comum com um potencial nó provedor do serviço solicitado. No segundo modelo, o valor de confiança é obtido a partir de cenários *P2P* e, os valores necessários para calcular o valor de confiança de um nó são armazenados em um sistema centralizado que utiliza uma estrutura *DHT (Dristributed Hash Table)*, para que qualquer nó possa fazer uso dessas informações. A abordagem proposta, demonstra dois modelos possíveis para o cálculo da confiança, no entanto, os autores não consideram como esses dois modelos irão trabalhar em conjunto, o que poderia ser útil visto que, um pode complementar o outro de acordo com o ambiente que estiver inserido.

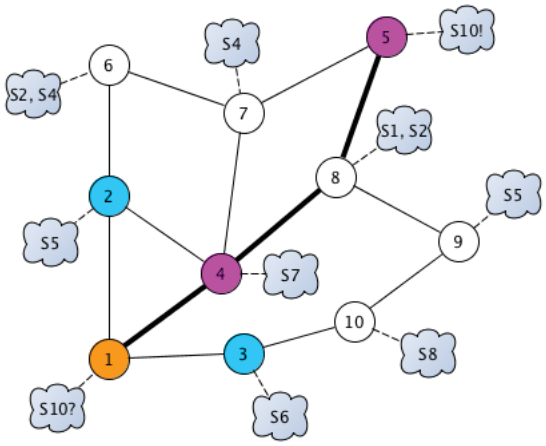


Figura 3.5: Representação da Rede.
Adaptado de (Nitti et al., 2014)

.

O objetivo do trabalho (Mendoza e Kleinschmidt, 2015), é identificar o comportamento de nós mal-intencionados e impedir possíveis ataques do tipo *On-Off* em um ambiente *IoT* multiserviço. Neste trabalho, é proposto um modelo de gerenciamento distribuído, onde o valor da confiança é computada diretamente por qualquer nó, sem a necessidade de uma entidade central. Nesta abordagem é considerado que cada nó na rede é capaz de fornecer um número diferente de serviços e é atribuído um valor de recompensa ou punição sempre que um serviço é, ou não fornecido ao nó que o solicitou. Desta forma, o valor de confiança de um nó é calculado pela soma das notas de todos os serviços fornecidos com sucesso. Os nós que não fornecem os serviços na rede são punidos com a diminuição do seu valor de confinaça pelo nó que esta solicitando o serviço. Segundo os autores, quanto mais próximo do valor negativo -1 estiver o valor de confiança do nó, significa grande desconfiança para o nó fornecer qualquer tipo de serviço e, quanto mais próximo do valor positivo 1, mais confiável será esse nó para fornecer qualquer tipo de serviço na rede. Uma vantagem desta abordagem é considerar o valor de confiança inicial de um nó vizinho como 0, assim todos os nós são inicialmente considerados desconhecidos e, somente por meio da comunicação entre eles, será possível descobrir se os nós vizinhos são confiáveis ou não para manter a comunicação. No entanto, a abordagem proposta, não considera qual o procedimento que um nó deve tomar quando não encontrar o serviço solicitado em seus vizinhos, outro aspecto negativo é não considerar a avaliação de confiança de forma indireta em sua abordagem.

No trabalho (Namal et al., 2015) é proposta uma estrutura autônoma de gerenciamento de confiança denominada *MAPE-K - Monitor, Analyse, Plan, Execute, Knowledge* para aplicações e serviços baseados em nuvem e altamente dinâmicos para *IoT*. A arquitetura do sistema de gerenciamento de confiança proposto, conforme pode ser verificado na Figura 3.6, obtém informações de contexto e ambientais dos dispositivos de sensores *IoT* e os entrega aos agentes de confiança que filtram as informações e as enviam para o *loop* de controle *MAPE-K* implementadado na nuvem. Segundo os autores, essa abordagem oferece vantagens como, disponibilidade, escalabilidade, acessibilidade e flexibilidade. Este modelo é dividido em duas camadas. A primeira é a camada de consumidor de serviços, que consiste em *APIs* onde, os clientes acessam os serviços e agentes confiáveis que filtram localmente informações relacionadas a confiança para o *pool* de dados de confiança. A segunda é a camada de rede de nuvem e aplicações, e é o local onde é implementada a confiança como um serviço e utiliza a inteligência da computação em nuvem para obter os parâmetros de confiança sobre os quais a confiança será

avaliada. Neste trabalho os autores consideram os parâmetros, disponibilidade, confiabilidade, tempo de resposta e capacidade para a avaliação da confiança. Após todos os parâmetros serem avaliados, os mesmos são integrados para avaliar o nível de confiança efetivo do sistema. O cálculo da confiança total efetiva é realizado usando a soma ponderada dos valores de confiança dos parâmetros avaliados. Ao final do processo, todos os parâmetros são armazenados no *pool* de parâmetros adaptáveis na nuvem e acessíveis pelos provedores de serviços por meio da camada de aplicação e serviço. Segundo os autores essa estrutura fornece flexibilidade para clientes e prestadores de serviços e ajusta o nível de confiança de acordo com o contexto, contudo, a complexidade para a implementação pode inviabilizar sua utilização para muitos cenários *IoT*.

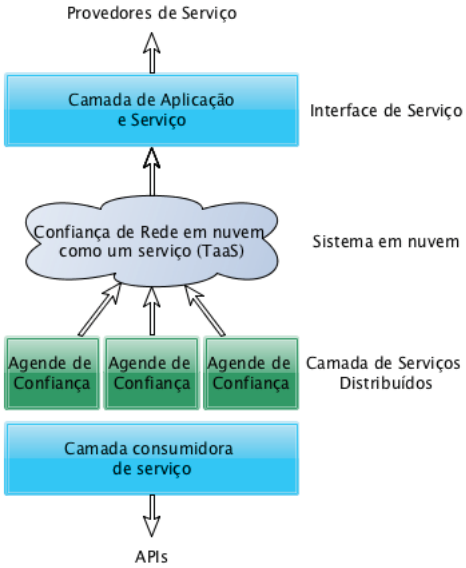


Figura 3.6: Visão geral da arquitetura proposta.
Adaptado de (Namal et al., 2015)

.

No trabalho (Chen et al., 2016b), os autores propõem um protocolo de gerenciamento de confiança adaptável e escalável para suportar aplicações *IoT* baseadas em serviços. Neste trabalho é considerado um ambiente social de *IoT* centrado no usuário, onde os nós são conectados fisicamente através de redes de comunicação e conectados socialmente através das redes sociais dos usuários. Do mesmo modo que em (Bao et al., 2013) cada nó possui um endereço exclusivo e não existe uma autoridade de confiança centralizada. Esta abordagem, considera dois tipos de nós, (i) dispositivos e (ii) usuários(ou proprietários), sendo que o relacionamento entre usuários e dispositivos é um relacionamento de um para muitos. Cada usuário mantém sua própria avaliação de confiança em relação aos dispositivos de outros usuários, sendo adotado o sistema de reputação *Baysian* como modelo para avaliação da confiança direta e a soma ponderada para agregar as recomendações de confiança indireta. De acordo com os autores, os dispositivos *IoT* em sua maioria são transportados por seres humanos ou operados por eles, sendo assim, o gerenciamento de confiança proposto considera as relações sociais entre os proprietários dos dispositivos. Desta forma, são considerados três tipos de relações sociais, (i) amizade, (ii) contato social e (iii) comunidade de interesse. Essas relações sociais são representadas por três listas, (i) lista de amigos com os amigos atuais; (ii) lista de locais com os locais visitados frequentemente para contato social e; (iii) lista de comunidades de interesses com os dispositivos (ou serviços) interagidos diretamente. De acordo com os autores, cada usuário deve ter pelo menos um

dispositivo sem restrições de recursos computacionais, o qual é designado a armazenar as listas no perfil do usuário, os outros dispositivos do mesmo usuário tem privilégio para acessar este perfil. Segundo os autores, ao delegar o armazenamento e o cálculo de confiança a um dispositivo sem restrições computacionais para cada usuário, os dispositivos com restrições computacionais podem compartilhar e usar as mesmas informações e maximizarem seu desempenho. No entanto, a necessidade de um dispositivo sem restrições, limita a abordagem a um cenário muito específico, dificultando assim sua implementação em cenários que possuam apenas dispositivos com restrições de recurso computacional.

O principal objetivo do trabalho (Chen et al., 2016c) é projetar um esquema de recomendação de serviços para ambientes dinâmicos de *IoT*. Neste trabalho os autores, consideram um ambiente social de *IoT* heterogêneo, descentralizado e sem uma autoridade confiável, no qual cada nó pertence a um proprietário específico e um proprietário pode ter vários nós, conforme representado na Fig. 3.7. Neste ambiente, cada nó atua tanto como um provedor de informações/serviços, como também solicitante ou recomendador de informações/serviços. Quando um nó solicita um determinado serviço, ele transmite a requisição na rede e seleciona o nó com maior valor de confiança. O valor da confiança é obtido pelo agrupamento de três partes distintas. Sendo a primeira parte, uma avaliação da reputação com base em uma média ponderada da quantidade de *feedbacks* (positivo/negativo) e classificações para transações passadas. A recomendação indireta é calculada com base nas opiniões recebidas de amigos comuns. O relacionamento social entre dois nós é a segunda parte da avaliação da confiança e os nós que possuem interesses em comum têm um relacionamento mais próximo, ou seja, maior confiabilidade. Os autores consideram também a capacidade computacional como uma característica para as relações sociais, visto que os nós com maior capacidade computacional são capazes de fornecer serviços melhores e menos propensos a serem comprometidos. A terceira e última parte, considera o *status* atual da energia. Desta forma, o *status* de energia de um nó é baseado na energia restante e na taxa de consumo de energia. Portanto, um nó com menos energia restante e uma taxa alta de consumo tem como valor atribuído um nível de energia baixo, diminuindo assim sua confiabilidade para prestar um serviço. Após a avaliação de cada nó, o esquema proposto gera uma lista de recomendações com base nos valores de confiança integrados. Em seguida, o nó do solicitante seleciona um ou vários nós com alta confiabilidade de acordo com os requisitos de serviço e interage com eles. No final de cada transação, o nó do solicitante atribui um valor de *feedback* (positivo/negativo) a cada nó provedor de serviço de acordo com a qualidade do serviço recebido. Além disso, como um mecanismo de incentivo/penalidade, o nó também atribui o valor de *feedback* aos amigos para suas recomendações. Como a confiabilidade de um nó é baseada na *QoS* e na precisão das recomendações fornecidas, os nós não maliciosos acumulam o valor de confiança mais rápido do que os nós maliciosos, assim de acordo com os autores, é possível distinguir nós não maliciosos e maliciosos com mais facilidade e otimizar recomendação. Devido ao fato desta abordagem considerar o usuário como entidade principal e um ambiente específico de *IoT* esta abordagem não pode ser utilizada em outros cenários de *IoT*. Outro problema encontrado neste trabalho diz respeito as requisições de serviços que são enviadas a rede por *broadcast* o que pode causar uma sobre carga na rede.

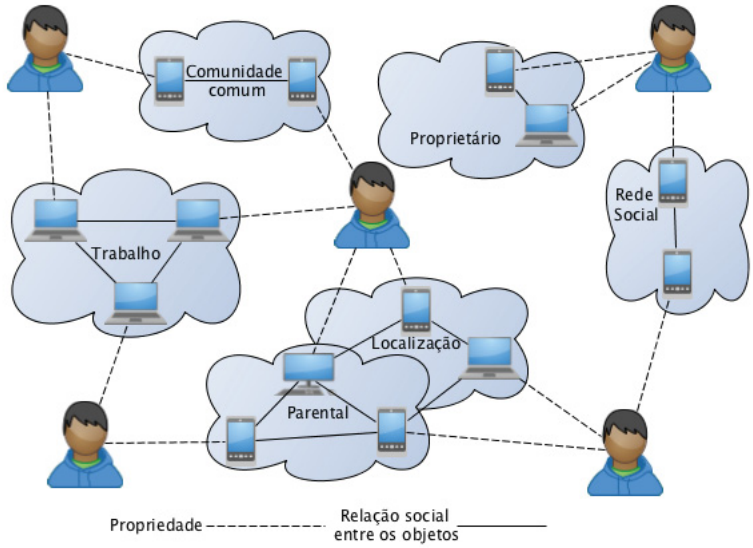


Figura 3.7: Arquitetura do sistema social de *IoT*.
Adaptado de (Chen et al., 2016c)

.

3.1 CONSIDERAÇÕES SOBRE O CAPÍTULO

Este capítulo foi dedicado ao estudo do estado da arte do gerenciamento de confiança para *IoT*. Este processo de investigação levou à identificação de um número significativo de propostas que abordam o tema.

Entre estas propostas verificou-se que os trabalhos (Bao et al., 2013) e (Chen et al., 2016b) utilizam métricas de *QoS* e social para a composição da confiança, a propagação da confiança é distribuída, utilizam a inferência *baysiana* e a soma ponderada para a agregação da confiança, a atualização da confiança é realizada por eventos para a observação direta e por tempo para a observação indireta. O trabalho (Nitti et al., 2014) utiliza métricas de *QoS* e social para a composição da confiança, considera a propagação de confiança distribuída e centralizada, contudo, não considera a utilização mútua desses meios de propagação, a agregação da confiança é realizada através da soma ponderada estática, a atualização da confiança é baseada em eventos. A proposta (Saied et al., 2013) utiliza apenas a métrica de *QoS* para a composição da confiança, a propagação da confiança é realizada de forma centralizada, deixando assim o sistema vulnerável a um único ponto de falha, a agregação da confiança é realizada através da soma ponderada dinâmica, a atualização da confiança é baseada em eventos. Os trabalhos (Chen et al., 2011) e (Mahalle et al., 2013) utilizam apenas a métrica de *QoS* para a composição de confiança, a propagação da confiança é realizada de forma distribuída, utiliza a soma ponderada dinâmica para a agregação da confiança e a atualização da confiança é basada em tempo. Os trabalhos (Bao e Chen, 2012), (Chen et al., 2016a) e (Chen et al., 2016c) utilizam métricas de *QoS* e social para composição da segurança, a propagação das informações são realizadas de forma distribuída, a agregação da confiança é baseada na soma ponderada, atualização da confiança é baseada em eventos para a observação direta e tempo para observação indireta, consideram múltiplas propriedades de confiança (honestidade, cooperatividade e comunidade de interesse) para a formação da confiança, no entanto, os autores não abordaram como formar uma confiança efetiva com essas propriedades.

Conforme pode ser observado na tabela 3.1, todas as abordagens estudadas possuem os requisitos necessários para o gerenciamento de confiança conforme especificado no capítulo 2 na seção 2.6.1.

Tabela 3.1: Comparação dos trabalhos relacionados

	Propagação			Atualização		Composição		Formação	
Trabalhos	Distribuida	Centralizada	Agregação da Confiança	Eventos	Tempo	QoS	Social	Única	Múltipla
(Chen et al., 2011)	X		X		X	X		X	
(Bao e Chen, 2012)	X		X	X	X	X	X		X
(Saied et al., 2013)		X	X	X		X		X	
(Wang et al., 2013)	X		X	X		X		X	
(Mahalle et al., 2013)	X		X		X	X		X	
(Bao et al., 2013)	X		X	X	X	X	X	X	
(Nitti et al., 2014)	X	X	X	X		X	X		X
(Mendoza e Kleinschmidt, 2015)	X		X	X		X		X	
(Namal et al., 2015)		X	X		X	X		X	
(Chen et al., 2016a)	X		X	X	X	X	X		X
(Chen et al., 2016b)	X		X	X	X	X	X	X	
(Chen et al., 2016c)	X		X	X	X	X	X		X

No entanto, apesar dos trabalhos relacionados apresentarem soluções interessantes para o gerenciamento de confiança para *IoT*, durante o estudo das propostas foram encontrados alguns problemas aparentes e fatores que deixam as abordagens restritas a ambientes muito específicos. Os trabalhos (Bao e Chen, 2012; Chen et al., 2016a,c,b) são centrados no usuário, o que dificulta a utilização dessa abordagem em ambientes com pouca ou nenhuma interação do usuário, como é o caso de objetos que se encontram em ambientes remotos. O trabalho (Chen et al., 2011) necessita que a placa de rede esteja em modo promíscuo, fazendo com que o dispositivo receba todas as mensagens dos seus vizinhos, mesmo que não estejam direcionadas diretamente a ele, esta abordagem pode ser inviável para dispositivos com poucos recursos computacionais devido ao alto consumo dos recursos utilizados para a verificação dos pacotes. O trabalho (Bao et al., 2013) não considera a atualização da confiança direta e indireta no mesmo momento, o que pode causar uma sobrecarga na rede, visto que os valores de confiança direta e indireta são atualizados em momentos distintos. O trabalho (Saied et al., 2013) considera um gerenciador de confiança centralizado, dificultando assim a sua implementação em um ambiente distribuído como a *IoT*. O trabalho (Mahalle et al., 2013) utiliza várias métricas para a composição da confiança, resultando em um tempo maior para se calcular a confiança, bem como, um maior consumo de recursos computacionais. O trabalho (Wang et al., 2013) aborda o gerenciamento de confiança de forma teórica não sendo possível uma análise mais detalhada desta abordagem. O trabalho (Nitti et al., 2014) considera a propagação da confiança distribuída e centralizada, no entanto, a proposta não detalha como os dois meios de propagação da confiança podem ser utilizados em conjunto. O trabalho (Mendoza e Kleinschmidt, 2015) não considera a avaliação de confiança de forma indireta em sua abordagem. Por fim, o trabalho (Namal et al., 2015) considera a confiança como um serviço que opera na nuvem, no entanto, essa abordagem pode não ser viável para ambientes *IoT* remotos.

Com base nas informações obtidas nesse estudo, é possível verificar a relevância do tema proposto nesta dissertação. Assim, foi desenvolvida uma nova proposta para o gerenciamento de confiança, totalmente descentralizado e distribuído, considerando os requisitos listados no capítulo 2 seção 2.6.1, capaz de avaliar o nível de confiabilidade dos nós em um ambiente *IoT*. O próximo capítulo, detalha a proposta.

4 TRUMIT - TRUST MANAGER FOR IOT

O objetivo principal deste trabalho é o projeto de um modelo de confiança dinâmico para avaliar o nível de confiabilidade dos nós em um ambiente de *IoT*. Para atingir tal objetivo, é proposto o *TRUMIT - Trust Manager for IoT*, um sistema de gerenciamento de confiança totalmente descentralizado e distribuído para ambientes *IoT*. O *TRUMIT* não necessita de uma entidade de confiança centralizada, assim, os nós são capazes de interagir de forma autônoma e independente com outros nós para avaliar, recomendar e armazenar as informações de confiança. Nesta abordagem, cada nó cria, de forma auto-organizada sua rede de confiança, para obter e recomendar informações sobre a confiabilidade dos nós. Essas informações são obtidas através de experiências diretas e indiretas. Assim, o cálculo do valor da confiança é realizado localmente, diminuindo o número de interações necessárias entre os nós para obter as evidências de confiança. As próximas seções descrevem a notação, o modelo e as funcionalidades do sistema de gerenciamento de confiança proposto nesta dissertação.

4.1 NOTAÇÃO E DEFINIÇÃO DO PROBLEMA

O conjunto de nós *IoT* é definido como $N = \{n_1, n_2, ..., n_m\}$ com cardinalidade *M*, onde n_i representa um nó genérico. A rede é representada por um grafo não direcionado $G = \{V, E\}$, onde $E \subseteq \{VxV\}$ é o conjunto de arestas, que representa o relacionamento entre um par de nós. O conjunto $P_i = \{n_j \in V{:}n_i, n_j \in E\}$ representa os nós que compartilham uma relação com o nó n_i, ou seja, seus vizinhos. O conjunto $K_{i,j} = \{n_k \in V{:}n_k \in P_i \cap P_j\}$ representa os nós comuns entre n_i e n_j. Esta representação, conforme pode ser verificada na figura 4.1, visa a busca e troca de evidências de confiança e, é representado por um determinado nó n_m avaliando ou recomendando um nó específico em um ambiente *IoT*.

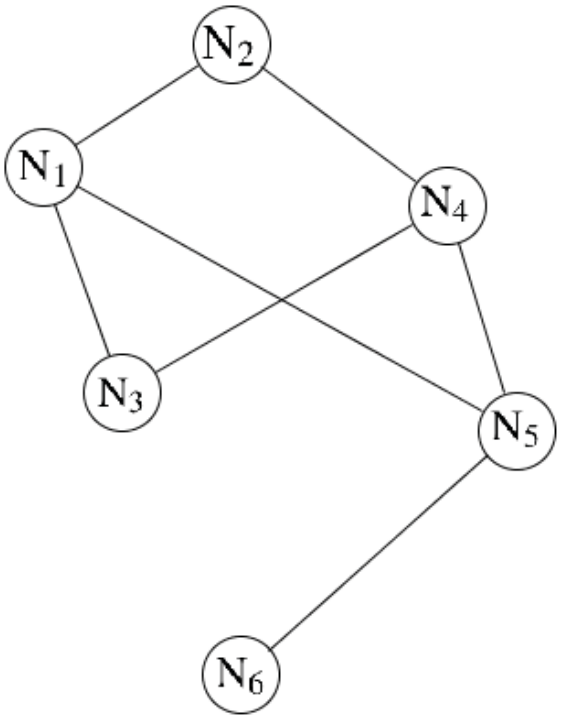


Figura 4.1: Representação do grafo de confiança.
Fonte: Do autor.

Para o melhor entendimento do trabalho proposto, a tabela 4.1 apresenta as notações utilizadas nesta dissertação.

Tabela 4.1: Notação utilizada.

Notação	Descrição
N_i	Identidade do nó *i*
G^i	Grafo da rede confiança do nó N_i
D_{ij}	Confiança direta do nó *i* em relação ao nó *j*
D*jk*	Valor de confiança direta do nó *j* em relação ao nó *k*
ΔT_p	Intervalo entre as trocas de informação
IS	Interações realizadas com sucesso
IU	Interações realizadas sem sucesso
R*ijk*	Recomendação do nó *j* em relação ao nó *k*
T_{ij}	Valor de confiança final direta do nó *i* em relação ao nó *j*
RT_{ijk}	Valor de confiança final indireta do nó *i* em relação ao nó *k*
α	Parâmetro de confiança direta e indireta entre [0,1]

4.1.1 Modelo do Sistema

Neste trabalho, assume-se um cenário no qual os nós podem se comunicar mutuamente, estabelecendo múltiplas conexões (relacionamentos) para a troca de dados e serviços, as quais devem ser executadas de um objeto para outro em ligações ponto a ponto. Assim, a rede *IoT* deve ser composta por objetos que realizam interações diretas e indiretas, como proposto em ((Bao et al., 2013; da Silva, 2014; Nitti et al., 2014; Chen et al., 2016b)).

São consideradas também as seguintes características:

- Assume-se uma topologia *peer-to-peer*;
- Cada nó tem um endereço exclusivo para identificação;
- Não há uma autoridade confiável centralizada;
- Cada nó pode entrar e sair do sistema voluntariamente;
- Cada nó calcula sua própria avaliação de confiança em relação a outros nós no mesmo raio de transmissão;
- Um nó mantém os resultados da avaliação de confiança dos nós no mesmo raio de transmissão e dos nós recomendados por seus vizinhos;
- Dois nós envolvidos em uma atividade de interação direta, observam um ao outro e atualizam seus valores de confiança;
- Os nós trocam seus resultados de avaliação de confiança em relação a outros nós através de recomendações;
- Um nó será recomendado quando seu valor na tabela de confiança do nó recomendador for maior ou igual ao parâmetro de confiança direta e indireta α.
- Um nó pode ser comprometido e se tornar malicioso;
- Um nó malicioso visa quebrar a funcionalidade básica (ex. composição de serviços) da rede.
- Os nós maliciosos podem executar ataques relacionados a confiança conforme, descrito em 2.6.1.

4.2 FUNCIONALIDADES DO TRUMIT

O modelo de gerenciamento de confiança proposto é composto de etapas, que se complementam entre si. As próximas seções descrevem o modelo do sistema proposto e as funcionalidades das etapas de criação da rede de confiança, avaliação de confiança direta e avaliação de confiança indireta.

4.2.1 Modelo

A figura 4.2 mostra a arquitetura do modelo de confiança proposto. A confiança direta é calculada a partir de interações diretas. A confiança indireta é calculada com base nas recomendações. O *TRUMIT* computa a confiança final com base nos valores da confiança direta e indireta e, armazena os valores em sua tabela de confiança.

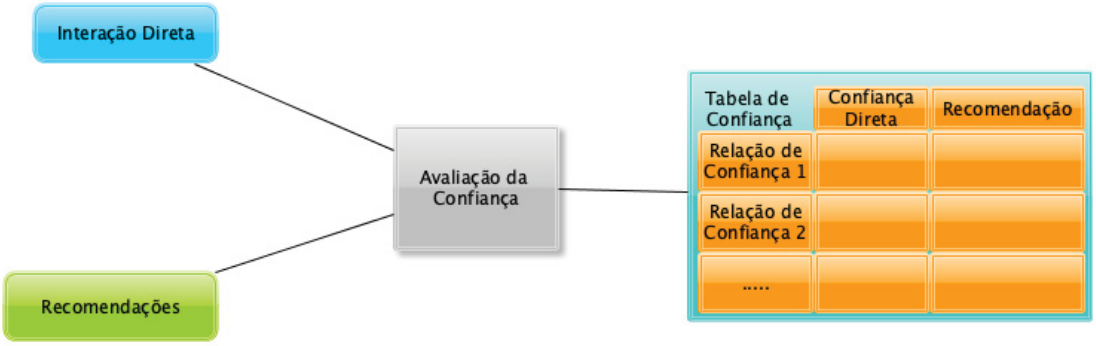


Figura 4.2: Arquitetura do *TRUMIT*.
Fonte: Do autor.

4.2.2 Criação da rede de confiança

Ao entrar no sistema, cada nó cria sua própria rede de confiança na forma de um grafo de confiança estático, conectado e não direcionado $G^i = \{V^i, E^i\}$ de forma auto-organizada. Inicialmente, os nós possuem informações apenas sobre os nós com o quais tiveram relações de confiança direta, e somente esses dados são armazenados na rede de confiança.

Assim, em intervalos de tempo pré-determinado ΔT_p, os nós trocam, com seus vizinhos, as evidências de confiança armazenadas em suas redes de confiança. Essas evidências são usadas para preencher a tabela de confiança do *nó*. Desta forma, os valores de confiança armazenados podem ser propagados pela rede.

4.2.3 Confiança direta

A confiança direta é avaliada com base na experiência do próprio nó com seus vizinhos através de observações sobre se as interações entre os nós são bem-sucedidas ou não. Desta forma, quando um nó interage diretamente com um nó vizinho, ele avalia a confiança do nó vizinho conforme a notação 4.1, onde D_{ij} corresponde a avaliação de confiança do nó N_i em relação ao nó N_j, *IS* é o número de interações realizadas com sucesso pelo nó *i* com o nó *j* e *IU* é o número de interações realizadas sem sucesso.

$$D_{ij} = \frac{IS}{IS + IU} \tag{4.1}$$

4.2.4 Confiança indireta

A confiança indireta é avaliada com base nas informações que o nó recebe dos nós vizinhos, assim, quando ocorre uma interação entre os nós conectados diretamente, os nós envolvidos nessa interação, trocam os valores armazenados em suas tabelas de confiança (fig. 4.3).

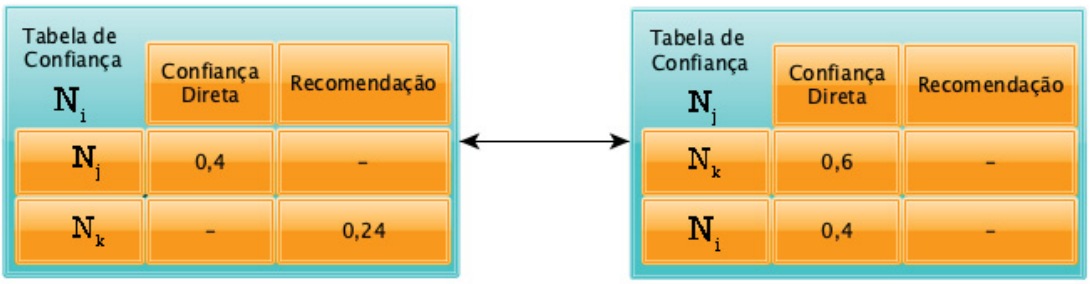


Figura 4.3: Avaliação de Confiança Indireta.
Fonte: Do autor.

Desta forma, um nó N_k que não esteja conectado diretamente a um nó N_i (Fig.4.4), pode ser avaliado de forma indireta. Esta avaliação é denominada de recomendação.

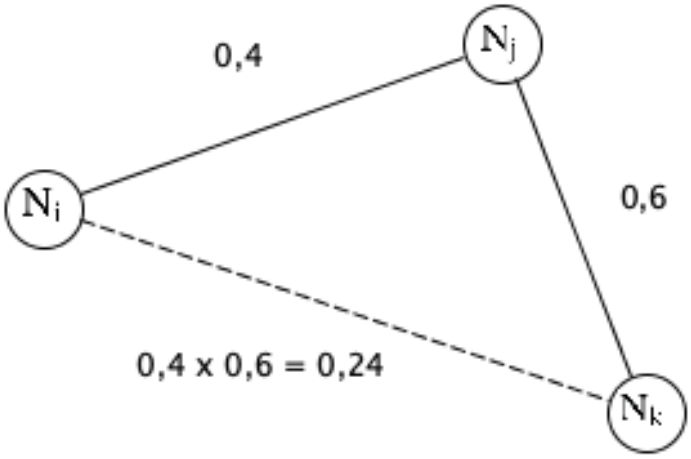


Figura 4.4: Avaliação de confiança indireta.
Fonte: Do autor.

Assim, a confiança indireta do nó N_k com base na recomendação do nó N_j é calculada pelo nó N_i da seguinte maneira:

$$R_{ijk} = (D_{ij} * D_{jk}) \tag{4.2}$$

Desta forma, R_{ijk} corresponde a avaliação de confiança indireta do nó N_i em relação ao nó N*k*, D_{ij} indica o valor de confiança direta do nó N_i no nó N_j e D_{jk} o valor de confiança direta do nó N_j em relação ao nó N_k, conforme demonstrado na Figura 4.4. Caso haja um conflito de recomendação, ou seja, mais de um nó recomendar o nó N_k, o nó N_i poderá considerar as seguintes abordagens:

1. Aceitar a recomendação do nó vizinho com o maior valor de confiança direta. Conforme pode ser verificado na Figura 4.5, os nós N_j e N_l estão recomendando o nó N_k ao nó N_i, desta forma, o nó N_i aceitará a recomendação do nó N_j com o qual possui maior valor de confiança direta, descartando assim a recomendação do nó N_l;

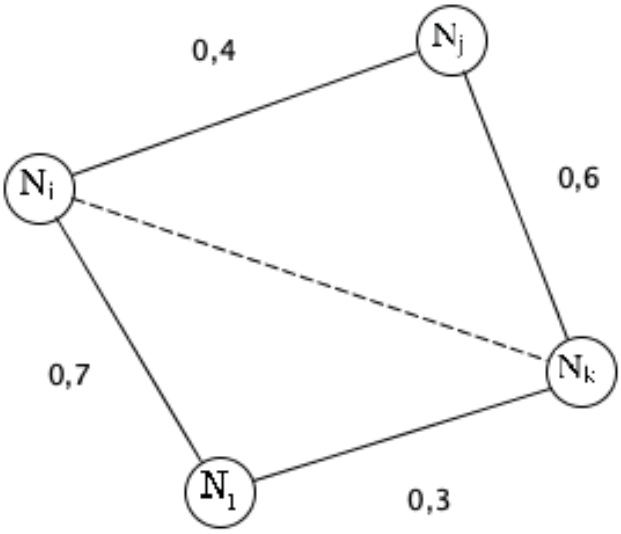


Figura 4.5: Maior valor de confiança direta.
Fonte: Do autor.

2. Calcular o valor da confiança indireta de todas as recomendações e, aceitar a qual possuir o maior valor para o cálculo da confiança indireta. Conforme pode ser verificado na figura 4.6, apesar do nó N_i possuir maior confiança no nó N_l, ele aceitará a recomendação do nó N_j, visto que, o valor da confiança indireta da recomendação R_{ijk} é maior em relação a recomendação de R_{ilk}.

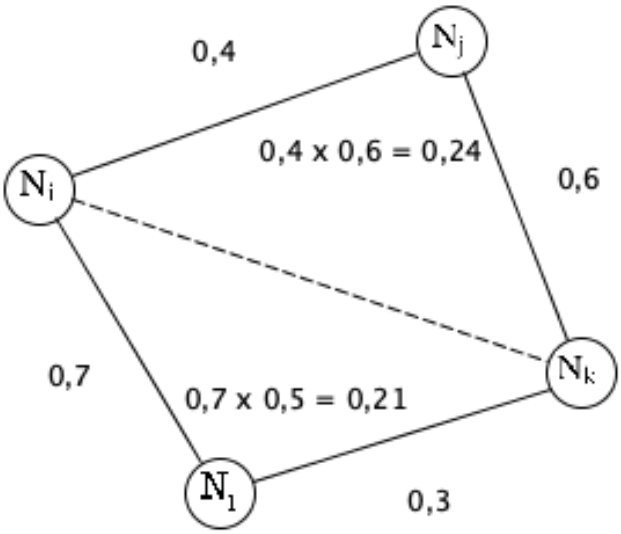


Figura 4.6: Maior valor de confiança indireta.
Fonte: Do autor.

3. Aceitar a recomendação do nó vizinho que possuir o maior valor do *timestamp*. Conforme pode ser verificado na figura 4.7, a recomendação R_{ijk} possui o maior valor do *timestamp* em relação a recomendação R_{ilk}, assim, o nó N_i aceita a recomendação R_{ijk} e calcula o valor da confiança indireta com base nesta recomendação, descartando a recomendação R_{ilk}.

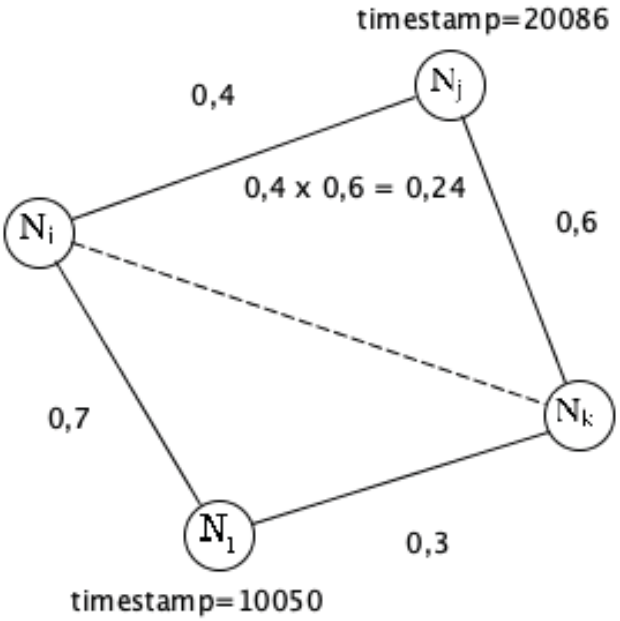


Figura 4.7: Maior valor *timestamp*
Fonte: Do autor.

Nesta dissertação assume-se que será aceita a recomendação com o maior valor do *timestamp*, visto que um nó esta sujeito a mudanças no decorrer do tempo, armazenando assim a informação mais recente sobre o nó recomendado em relação as abordagens 1 e 2, além disso, esta abordagem possui um custo computacional menor em relação a abordagem 2, visto que o cáclculo da confiança indireta é realizado uma única vez.

O *TRUMIT* permite que um nó seja recomendado mesmo estando a mais de um salto de distância do nó que receberá sua recomendação, assim, conforme pode ser verificado na Figura 4.8, o nó N_n poderá ser recomendado ao nó N_i.

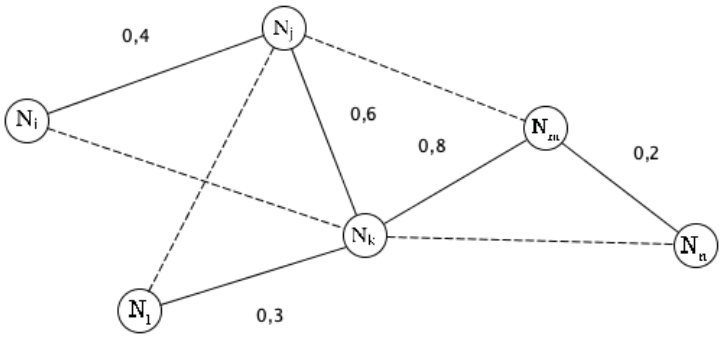


Figura 4.8: Recomendação mais de um salto de distância.
Fonte: Do autor.

Esta recomendação é possível visto que os nós trocam suas tabelas de confiança em períodos de tempo pré-determinados, disseminando as suas evidências de confiança pela rede. A Figura 4.9 demonstra as tabelas de confiança dos nós com seus respectivos valores de confiança direta e indireta já disseminados pela rede. Desta forma, para que o nó N_i obtenha a recomendação do nó N_n, os nós devem:

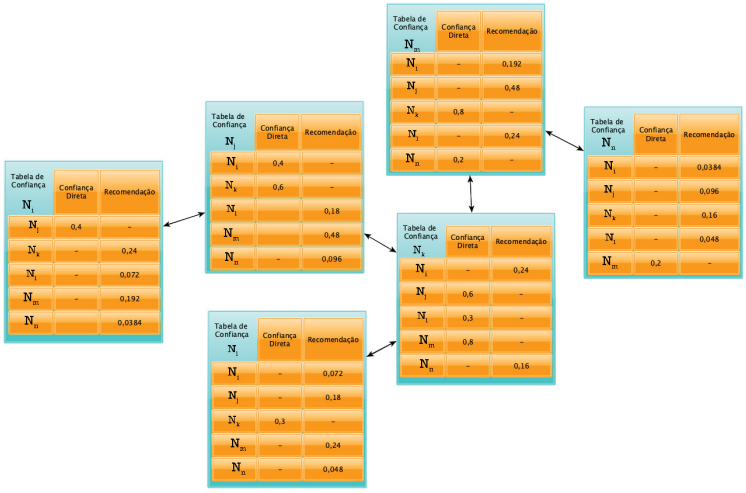


Figura 4.9: Disseminação tabelas de confiança.
Fonte: Do autor.

a) Preencher inicialmente suas tabelas de confiança com os valores de confiança direta. Exemplo: $N_i \rightarrow N_j \rightarrow N_k \rightarrow N_m \rightarrow N_n$, $N_l \rightarrow N_k$ e $N_n \rightarrow N_m$; e

b) Trocar as suas tabelas de confiança com os nós vizinhos, iniciando assim o preenchimento dos valores de confiança indireta de suas tabelas;

c) Assim, o N_i pode calcular a recomendação do nó N_n com base nas informações que recebeu do nó N_j. Exemplo: 0,4 x 0,096 = 0,384, sendo, 0,4 o seu valor de confiança em relação ao nó N_j e 0,096 o valor da recomendação no nó N_j em relação ao nó N_n.

É possível verificar também na Figura 4.9 que, quanto mais distante está o nó recomendado, menor será seu valor de confiança indireta.

4.2.5 Cálculo do valor de confiança final

O valor de confiança é um número real no intervalo de [0, 1], em que 1 indica confiança total e 0 desconfiança. Desta forma, quanto mais o nó *i* confiar em seu vizinho *j*, mais próximo de 1 será o seu valor confiança no nó vizinho. Assim, o cálculo do valor de confiança final do nó *i* em relação ao nó *j* é denotado da seguinte forma:

$$T_{ij} = \alpha D_{ij} + (1 - \alpha) \tag{4.3}$$

Sendo, α e 1 - α os pesos para ajustar o valor de confiança direta final entre 0 e 1. Assim, $0 < \alpha < 1$, $0 < T_{ij} < 1$. O cálculo do valor de confiança final para nós recomendadados, é denotado da seguinte forma:

$$RT_{ijk} = \alpha R_{ijk} + (1 - \alpha) \tag{4.4}$$

Sendo, α e 1 - α os pesos para ajustar o valor de confiança indireta final entre 0 e 1. Como os valores de confiança direta D_{ij} e D_{jk} estão no intervalo [0,1], a confiança indireta do no *i* para o nó *k* (com base nas recomendações do nó *j*) é sempre menor que os valores de D_{ij} ou D_{jk}.

4.2.6 Atualização da confiança

Devido à rede *IoT* ser um ambiente dinâmico, o comportamento de um nó pode mudar com o decorrer do tempo. Desta forma, para evitar que a informação de confiança sobre um nó fique desatualizada e tornar o *TRUMIT* resiliente a nós maliciosos, é necessário manter as informações dos nós constantemente atualizadas, de modo que informações antigas não afetem o desempenho do sistema.

Para fazer isso, cada nó armazena além do valor de confiança um valor de registro de data e hora, denominado *timestamp*. Assim, quando um nó N_i interage com o N_j, o nó N_i armazena juntamente com o valor de confiança o *timestamp* do nó N_j, registrando assim o momento em que a interação ocorreu. Desta forma, quando o nó N_i interagir com o nó N_j no futuro, o nó N_i pode saber quanto tempo se passou desde a última interação entre eles. Assim, a cada interação, o nó N_i compara o *timestamp* atual com o *timestamp* armazenado e atualiza a informação de confiança com o valor do *timestamp* atual, descartando assim, a informação mais antiga.

4.3 CUSTO DE ARMAZENAMENTO

O custo de armazenamento da tabela de confiança de um nó está proporcionalmente condicionado ao número de nós da rede e é denotado no *TURMIT* pela seguinte notação:

$$CA = \sum_{ID=1}^{n} ID * 32 + \sum_{CD=1}^{n} CD * 48 + \sum_{CD=0}^{n} CI * 48 + \sum_{TS=1}^{n} TS * 48 \tag{4.5}$$

Sendo, *CA* o custo do armazenamento, *ID* um campo de valor inteiro que representa o identificador do nó na tabela de confiança, *CD* um campo de valor real que representa a confiança direta, *CI* um campo de valor real que representa a confiança indireta e *TS* um campo de valor real que representa o valor de *timestamp* na tabela de confiança. Assim, um nó que possua uma tabela com informações de confiança de 5 nós, conforme pode ser verificado na Figura 4.10, terá seu *CA* de 640 bits, como pode ser verificado na equação 4.6.

Figura 4.10: Custo armazenamento.
Fonte: Do autor.

$$CA = 5 * 32 + 1 * 48 + 4 * 48 + 5 * 48 = 640 \tag{4.6}$$

4.4 CUSTO DE TRANSMISSÃO

O custo de transmissão da tabela de confiança no *TRUMIT* está condicionado à tecnologia de comunicação a ser utilizada pelo dispositivo e pode ser denotado da seguinte forma:

$$CT = \frac{CA}{TU} \tag{4.7}$$

Sendo, *CT* o custo da transmissão, *CA* o tamanho da mensagem e *TU* o tamanho total da mensensagem na tecnologia

4.5 COMPARATIVO *TRUMIT*

A tabela 4.2 faz uma comparação do *TRUMIT* com os trabalhos relacionados no capítulo 3, considerando as propriedades de Propagação de confiança, Agregação de confiança, Atualização de confiança e Formação de confiança.

Tabela 4.2: Comparação dos trabalhos relacionados

	Propagação			Atualização		Composição		Formação	
Trabalhos	Distribuida	Centralizada	Agregação da Confiança	Eventos	Tempo	QoS	Social	Única	Múltipla
TRUMIT	X		X		X	X			X
(Chen et al., 2011)	X		X		X	X		X	
(Bao e Chen, 2012)	X		X	X	X	X	X		X
(Saied et al., 2013)		X	X	X		X		X	
(Wang et al., 2013)	X		X	X		X		X	
(Mahalle et al., 2013)	X		X		X	X		X	
(Bao et al., 2013)	X		X	X	X	X	X	X	
(Nitti et al., 2014)	X	X	X	X		X	X		X
(Mendoza e Kleinschmidt, 2015)	X		X	X		X		X	
(Namal et al., 2015)		X	X		X	X		X	
(Chen et al., 2016a)	X		X	X	X	X	X		X
(Chen et al., 2016b)	X		X	X	X	X	X	X	
(Chen et al., 2016c)	X		X	X	X	X	X		X

Em sua abordagem o trabalho (Chen et al., 2011), considera apenas a porção de pacotes encaminhados corretamente de todos os seus vizinhos para a formação da confiança, enquanto o *TRUMIT* considera os pacotes enviandos com e sem sucesso para a formação da confiança. Os trabalhos (Bao e Chen, 2012) e (Chen et al., 2016a) consideram as relações sociais dos proprietários dos dispositivos para formação da confiança, o *TRUMIT* é um modelo de sistema totalmente auto-organizado, não dependendo de listas que representem as suas interações. O trabalho (Mahalle et al., 2013) considera as interações bem e mal-sucedidas para a foramção da confiança, no entanto, antes de ser calculado o valor de confiança, é necessário realizar o cálculo dos parâmtros de experiência (EX), conhecimento (KN) e recomendação (RC), o que demanda tempo e recursos computacionais. Os trabalhos (Saied et al., 2013) e (Namal et al., 2015) consideram a propagação da confiança de forma centralizada, deixando assim o sistema vulnerável a um único ponto de falha, o *TRUMIT* considera em sua abordagem a propagação da confiança de forma distribuída. O trabalho (Bao et al., 2013), considera a atualização de confiança baseada em eventos para a confiança direta e a atualização de confiança orientado por tempo para a confiança indireta, o *TRUMIT* considera apenas a atualização de confiança orientado por tempo para os valores de confiança direta e indireta, reduzindo assim o número de interações necessárias para a atualização de ambos os valores de confiança. O trabalho

(Nitti et al., 2014), considera dois modelos para a propagação dos valores de confiança, sendo o modelo de confiabilidade subjetiva destinado a propagação da confiança de forma distribuída e o modelo de confiabilidade objetiva destinado a propagação dos valores de confiança de forma centralizada, no entanto, o trabalho não possui informações se esses modelos podem ser utilizados em conjunto, diante deste fato, esta abordagem se limita a ambientes distintos e muito específicos. Apesar do trabalho (Chen et al., 2016b) considerar a propagação do valor de confiança de forma distribuída, ao contrário do *TRUMIT*, esta abordagem necessita de um dispositivo sem restrições computacionais para o armazenamento das informações. O trabalho (Mendoza e Kleinschmidt, 2015), não considera em sua abordagem a confiança indireta. O trabalho (Chen et al., 2016c), apresenta uma abordagem totalmente centrada no usuário, enquanto no *TRUMIT* o dispositivo é o responsável por gerenciar os relacionamentos de confiança. Por fim, o trabalho (Wang et al., 2013), apresenta de forma teórica uma estrutura geral para gerenciamento de confiança em *IoT*.

4.6 CONSIDERAÇÕES SOBRE O CAPÍTULO

Neste capítulo foram apresentadas as funcionalidades do *TRUMIT (Trust Manager for IoT)* para o gerenciamento de confiança para ambientes *IoT*. O trabalho proposto pode avaliar, atualizar e manter as evidências de confiança entre os nós por meio da observação direta e indireta. Também é realizado um comparativo entre o modelo proposto e os trabalhos relacionados. No próximo capítulo serão apresentados os resultados da avaliação das funcionalidades do *TRUMIT*, bem como, o seu comportamento, considerando cenários com e sem nós maliciosos.

5 AVALIAÇÃO DO *TRUMIT*

Nesta seção, são apresentados os resultados obtidos da avaliação do sistema de gerenciamento de confiança - *TRUMIT*, proposto nesta dissertação.

5.1 SIMULADOR

O *Cooja Simulator* é parte do sistema operacional *ContikiOS*, um sistema operacional de código aberto para a *Internet* das Coisas que conecta microcontroladores de baixo custo e baixo consumo de energia à *Internet* (Dunkels et al., 2004). O *Cooja*, é um simulador flexível baseado em Java e muito utilizado pela comunidade de pesquisa de *WSN* devido à sua capacidade de programar sensores para *IoT* (Tutunović e Wuttidittachotti, 2019).

As simulações no *Cooja* consistem em cenários onde cada nó possui um tipo, memória e um número de interfaces. Em comparação com outros simuladores, o *Cooja* não é estritamente um simulador de rede, mas sim um simulador capaz de simular protocolos diferentes em diferentes camadas da rede e permite a simulação simultânea no nível da rede, no nível do sistema operacional e no nível do conjunto de instruções. O *Cooja* também permite que os pesquisadores reproduzam cenários realistas que incluem a execução de protocolos populares da camada de aplicação para padrões criados para redes de sensores como 802.15.4 e *IPv6* para redes de área pessoal sem fio de baixa potência (*6LoWPAN*) (Chernyshev et al., 2017; Tutunović e Wuttidittachotti, 2019).

O *Cooja* possui uma interface para analisar e interagir com os nós, facilitando a visualização do ambiente *IoT* e seus atributos. Além disso, é possível a criação de cenários personalizados e a emulação de plataformas de *hardware* reais (Österlind et al., 2006; Santos et al., 2016). Desta forma, o *Cooja* foi o simulador escolhido para simular as interações entre os nós em um ambiente *IoT* para posterior avaliação do modelo de gerenciamento proposto nesta dissertação.

5.2 CONFIGURAÇÃO E PARAMETRIZAÇÃO DO AMBIENTE

Para realizar a simulação das interações, os nós utilizam um canal de comunicação sem fio, seguindo o modelo de propagação *Unit Disk Graph Medium (UDGM)*. O *UDGM* é o modelo de propagação padrão do *Cooja* (Long et al., 2012; Ruckebusch et al., 2015). Este modelo calcula o valor de *RSSI* com base na distância entre os nós, este modelo também degrada a qualidade do sinal com base na distância entre os nós. Todos os ambientes simulados possuem 50 nós do tipo *Tmote Sky* distribuídos aleatoriamente com um atraso de início de 1000ms em uma dimensão de $10000m^2$. O *Tmote Sky* é um módulo sem fio de baixo consumo, para uso em redes de sensores, aplicações de monitoramento e prototipagem rápida de aplicações para redes de sensores e *IoT* (Gajjar et al., 2014). Foram utilizados três raios de transmissão, 20, 30 e 50m. O tempo de simulação estabelecido para a avaliação é de 240s. As simulações foram realizadas considerando a presença de nós honestos e nós maliciosos. A tabela 5.1 apresenta os parâmetros utilizados para gerar as interações dos nós no simulador *Cooja* bem como, na avaliação do modelo proposto.

Tabela 5.1: Parâmetros da Avaliação.

Parâmetros	Cenário 1	Cenário 2	Cenário 3
N^o de nós	50	50	50
Tecnologia de comunicação	802.15.4	802.15.4	802.15.4
Raio de transmissão	20m	30m	50m
Àrea da Simulação	$10000m^2$	$10000m^2$	$10000m^2$
Duração da simulação(s)	240	240	240
Parâmetro de Confiança direta e indireta (α)	0,0 - 1,0	0,0 - 1,0	0,0 - 1,0
Intervalo de Interações (ΔT_p)	10s	10s	10s
N^o de execuções	4	4	4

Os parâmetros utilizados para a avaliação do *TRUMIT*, levam em consideração o comportamento que um nó terá em relação aos demais nós da rede *IoT*. Desta forma, para este trabalho, optou-se por cenários com a mesma área de simulação, quantidade de nós, tecnologia de comunicação e duração da simulação, alterando-se apenas o tamanho do raio de transmissão, a quantidade de nós maliciosos e valor do parâmetro de confiança direta e indireta. Ao considerar tais parâmetros, as funcionalidades do *TRUMIT* serão avaliadas sob um mesmo fato, no entanto, por diferentes perspectivas. Desta forma, os dados coletados das diferentes simulações, proporcionaram uma linha de base para avaliar as funcionalidades do *TRUMIT*.

5.3 METODOLOGIA

Para testar o modelo de confiança proposto, os valores obtidos das interações dos nós no simulador *Cooja* foram exportados para um arquivo no formato *txt*. De posse desses valores, os dados foram importados para uma planilha e organizados em colunas com os seguintes valores, *timestamp*, origem, destino e tabela de confiança.

Em seguida, foi selecionado um nó aleatoriamente para cada cenário avaliado. Com o nó a ser avaliado definido, foi criada uma nova planilha, esta planilha foi utilizada para simular o comportamento do nó selecionado. Desta forma, inicialmente a planilha foi preenchida com as informações dos nós que estão diretamente conectados ao nó selecionado, criando assim a sua tabela de confiança. O mesmo processo foi realizado para cada nó conectado de forma direta e indireta ao nó selecionado nesta avaliação.

Após a criação da tabela de confiança inicial do nó selecionado e dos demais nós envolvidos nesta avaliação, foi realizada para cada interação registrada no arquivo gerado pelo simulador *Cooja*, a avaliação da confiança direta e indireta de cada nó envolvido nesse processo de acordo com o que foi proposto no 4. Cada interação realizada e avaliada, foi devidamente registrada nas tabelas de confiança dos respectivos nós avaliados.

Para a avaliação do cenário com a presença de nós maliciosos, além do nó selecionado aleatoriamente para simular o comportamento do modelo proposto em cada cenário, foram também selecionados outros nós aleatórios para representarem o comportamento de nós maliciosos, os demais passos seguem a metologia já detalhada nesta seção. Por fim, foram elaborados os gráficos, utilizando a *suite LibreOffice*. Os resultados dessa avaliação, bem com os gráficos gerados são detalhados nas próximas seções.

5.4 RESULTADOS

Considerando um cenário sem nós maliciosos, o *TRUMIT* foi avaliado com relação ao número de interações e o tempo necessário para que um determinado nó possua o conhecimento

total da rede. Para a avaliação dos resultados, foi selecionado um nó aleatóriamente de cada cenário. O nó selecionado representa o comportamento de qualquer nó não malicioso na rede; se um nó diferente na rede for selecionado, serão obtidos resultados semelhantes ao do nó selecionado nesta avaliação. Neste experimento, o valor do parâmetro de confiança direta e indireta (α) variou de 0,0 a 1,0.

Desta forma, o *TRUMIT* foi avaliado em três cenários, sendo o primeiro cenário composto por 50 nós, com raio de transmissão dos nós de 20m e uma área total de $10000m^2$. O segundo cenário com 50 nós, com raio de transmissão dos nós de 30m e uma área total de $10000m^2$. O terceiro e último cenário, possui 50 nós, com raio de transmissão dos nós de 50m e uma área total de $10000m^2$.

As figuras 5.1, 5.2 e 5.3, demonstram as variações das interações realizadas pelo nó para obter as evidências de confiança bem como, o conhecimento total da rede nos diferentes cenários simulados. Assim, é possível verificar que, quando o valor do parâmetro de confiança direta e indireta (α) é igual a zero, o nó necessita de um número menor de interações para obter as evidências de confiança dos demais nós da rede. Isso ocorre porque, com α = 0,0 os nós aceitam as evidências todos os demais nós da rede. Assim, as evidências são trocadas rapidamente. No entanto, quando o valor de α aumenta, o nó necessita realizar um número maior de interações para obter e disseminar as evidências de confiança.

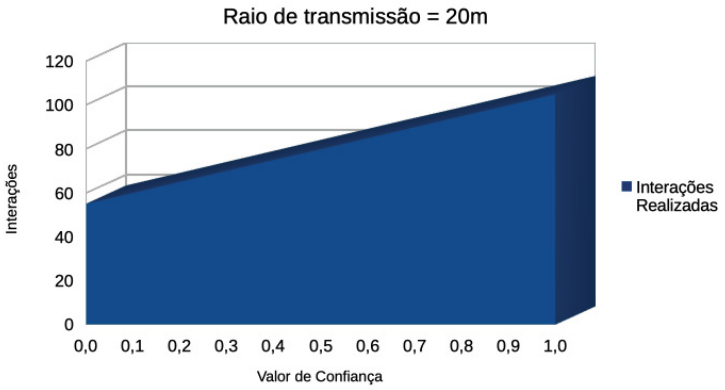


Figura 5.1: Raio de transmissão = 20m

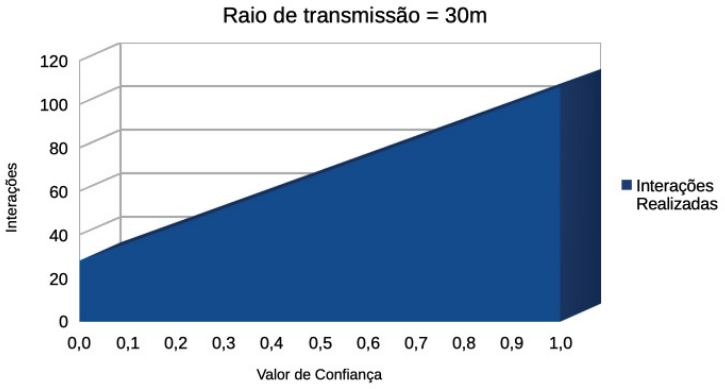


Figura 5.2: Raio de transmissão = 30m

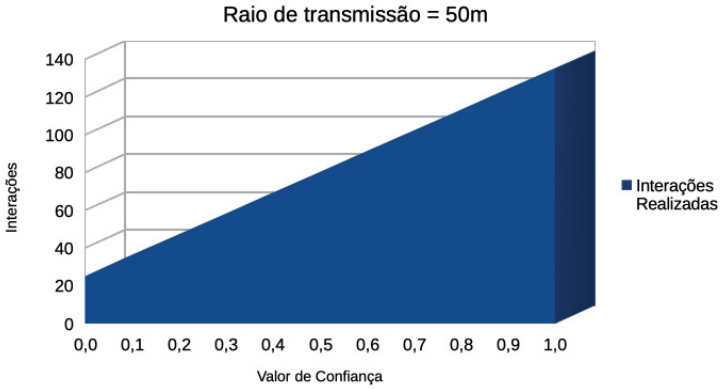


Figura 5.3: Raio de transmissão = 50m

Nesta avaliação, verificou-se que, o cenário com o raio de transmissão de 20m realizou um número elevado de interações para obter as evidências de confiança da rede, no entanto, neste cenário não houve convergência da rede. Sendo assim, o nó coletou apenas 88% das evidências de confiança da rede. Com relação aos demais cenários, houve a convergência da rede e verificou-se que, não há um aumento significativo entre o número de interações que o nó realizou nesses cenários. Por fim, a Tabela 5.2, mostra o tempo médio (em segundos) que o nó leva para obter as evidências de confiança da rede para cada um dos cenários avaliados. Os cenários com raio de transmissão de 30m e 50m possuem valores próximos, o que demonstra a eficácia do sistema em redes de maior densidade.

Tabela 5.2: Tempo - Sem presença de nós maliciosos.

α	Raio de transmissão = 20m		Raio de transmissão = 30m		Raio de transmissão = 50m	
	Tempo (s)	Nó (%)	Tempo (s)	Nós (%)	Tempo (s)	Nós (%)
0,0	90	88	40	100	30	100
0,1	100	88	50	100	40	100
0,2	110	88	60	100	50	100
0,3	120	88	70	100	60	100
0,4	130	88	80	100	70	100
0,5	140	88	90	100	80	100
0,6	150	88	100	100	90	100
0,7	160	88	110	100	100	100
0,8	170	88	120	100	110	100
0,9	180	88	130	100	120	100
1,0	190	88	140	100	130	100

O *TRUMIT* também foi avaliado considerando nós maliciosos em seus cenários. Em todos os cenários avaliados, os nós se comportam de forma maliciosa depois de formarem suas redes de confiança. Os nós maliciosos neste experimento alteram os valores dos nós de suas tabelas de confiança para 0,0, fazendo com que este nós não sejam recomendados aos seus vizinhos. Esta avaliação foi realizada em cenários considerando 10%, 20%, 30% e 50% de nós maliciosos na rede. Para esta análise, foi selecionado um nó não maliciosos de forma aleatória de cada cenário. O nó selecionado representa o comportamento de qualquer nó bem comportado na rede; se outro nó não malicioso na rede for selecionado, serão obtidos resultados semelhantes ao do nó selecionado para esta avaliação.

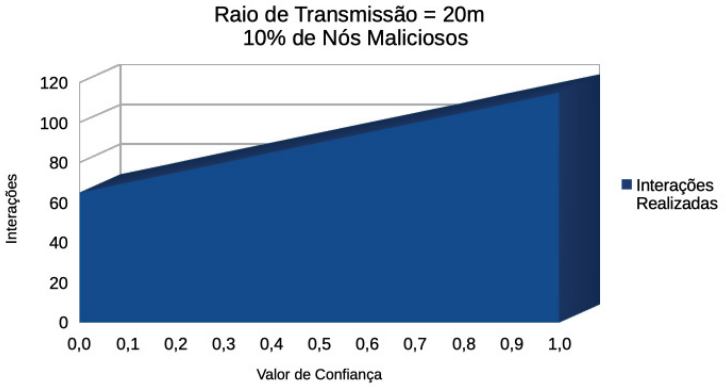


Figura 5.4: Raio de transmissão = 20m
10% nós maliciosos

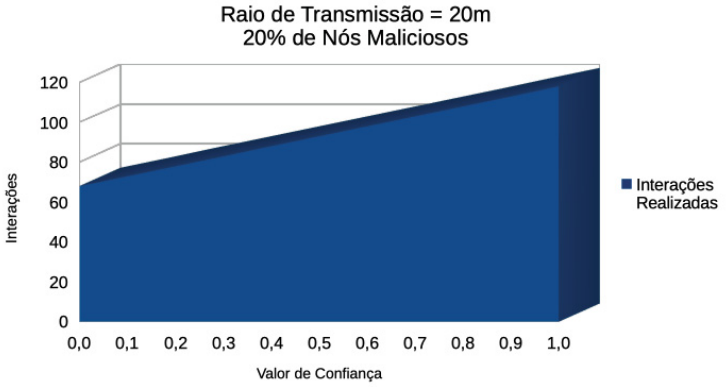


Figura 5.5: Raio de transmissão = 20m
20% nós maliciosos

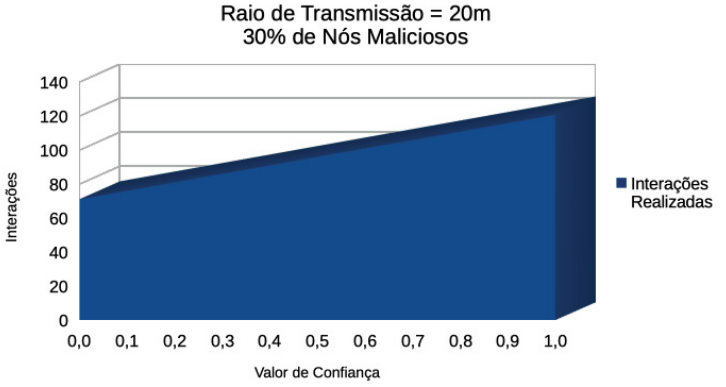


Figura 5.6: Raio de transmissão = 20m
30% nós maliciosos

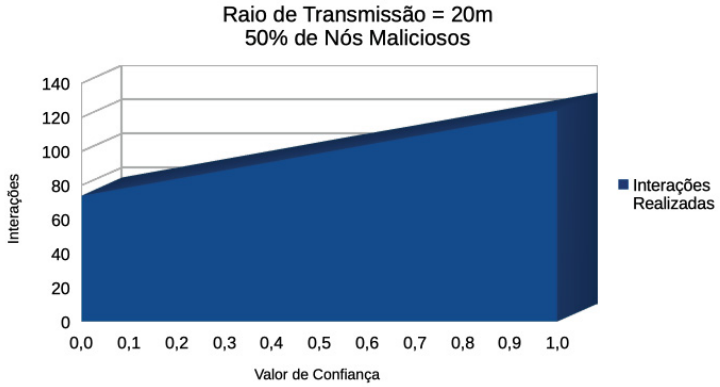


Figura 5.7: Raio de transmissão = 20m
50% nós maliciosos

As figuras 5.4, 5.5, 5.6 e 5.7, demonstram as variações das interações realizadas pelo nó para obter as evidências de confiança da rede para as diferentes quantidades de nós maliciosos com raio de transmissão de 20m. Nesta avaliação, assim como na avaliação sem a presença de nós maliciosos, não houve convergência da rede para o cenário raio com transmissão de 20m, no entanto, verificou-se que, com a presença de nós maliciosos, o nó selecionado, coletou um número menor de evidências de confiança, tendo coletado 79,2% das evidências de confiança em sua avaliação com 10% de nós maliciosos, 70% das evidências de confiança em sua avaliação com 20% de nós maliciosos, 61,6% das evidências de confiança em sua avaliação com 30% de nós maliciosos e 44% das evidências de confiança em sua avaliação com 50% de nós maliciosos. Neste experimento é possível verificar que em uma rede de menor densidade menor e com a presença de nós maliciosos o modelo proposto não conseguiu obter desempenho similar aos dos demais cenários avaliados, conforme pode ser verificado na figura 5.16. Por fim, a Tabela 5.3, demonstra o tempo médio (em segundos) que o nó leva para obter as evidências de confiança da rede para cada um dos cenários avaliados.

Tabela 5.3: Tempo - Raio de Transmissão = 20m.

α	10% Nós Maliciosos		20% Nós Maliciosos		30% Nós Maliciosos		50% Nós Maliciosos	
	Tempo (s)	Nó (%)	Tempo (s)	Nós (%)	Tempo (s)	Nós (%)	Tempo (s)	Nós (%)
0,0	100	79,2	110	70,4	120	61,6	130	44
0,1	110	79,2	120	70,4	130	61,6	140	44
0,2	120	79,2	130	70,4	140	61,6	150	44
0,3	130	79,2	140	70,4	150	61,6	160	44
0,4	140	79,2	150	70,4	160	61,6	170	44
0,5	150	79,2	160	70,4	170	61,6	180	44
0,6	160	79,2	170	70,4	180	61,6	190	44
0,7	170	79,2	180	70,4	190	61,6	200	44
0,8	180	79,2	190	70,4	200	61,6	210	44
0,9	190	79,2	100	70,4	210	61,6	220	44
1,0	200	79,2	210	70,4	220	61,6	230	44

Em sua avaliação considerando o raio de transmissão de 30m, o *TRUMIT* mostrou-se resiliente aos nós maliciosos, obtendo o conhecimento total da rede. As Figuras 5.8, 5.9, 5.10 e 5.11 demonstram as variações das interações realizadas pelo nó para obter as evidências de confiança da rede para as diferentes quantidades de nós maliciosos. Neste experimento, foi

observado que o nó realizou o mesmo número de interações para os cenários com 10%, 20% e 30% de nós maliciosos, havendo alteração com relação a número de interações no cenário com 50% de nós maliciosos, visto que, o nó necessitou realizar um número maior de interações para coletar as evidências de confiança da rede, no entanto, este fato, não inviabiliza o *TRUMIT* para este tipo de cenário, uma vez que, o nó obteve o conhecimento total da rede, não havendo um aumento significativo com relação ao tempo médio que o nó levou para obter as evidências de confiança com relação aos demais cenários avaliados, conforme pode ser verificado na Tabela 5.4.

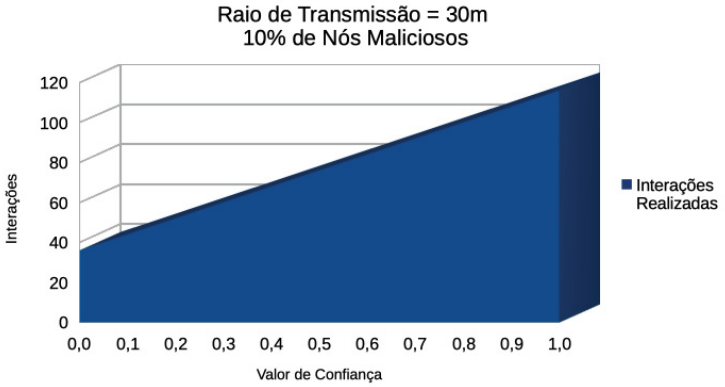


Figura 5.8: Raio de transmissão = 30m
10% nós maliciosos

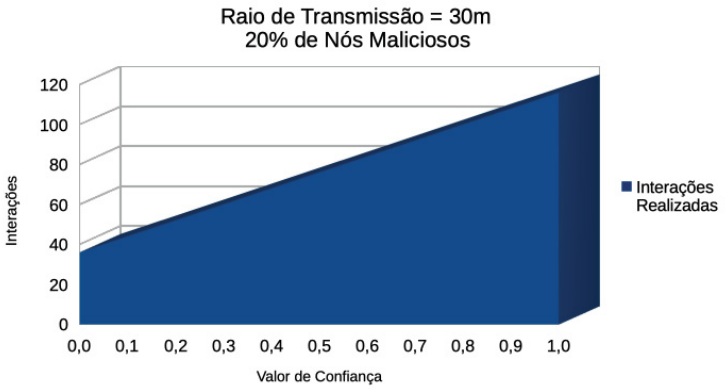


Figura 5.9: Raio de transmissão = 30m
20% nós maliciosos

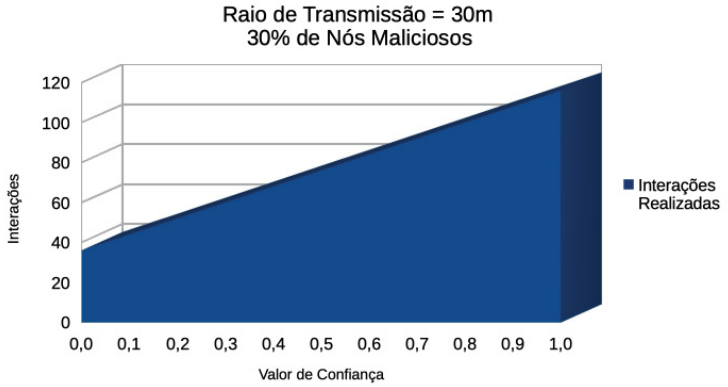


Figura 5.10: Raio de transmissão = 30m
30% nós maliciosos

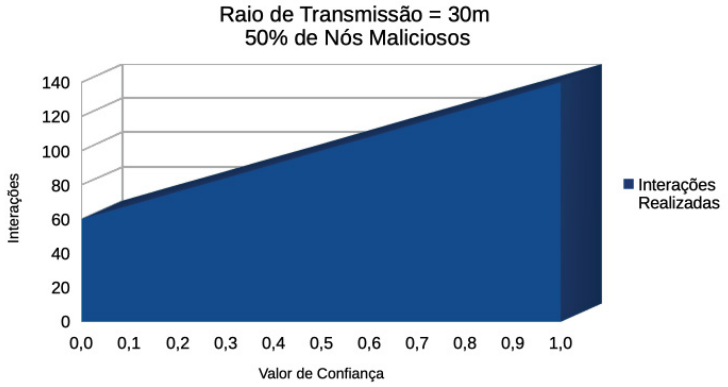


Figura 5.11: Raio de transmissão = 30m
50% nós maliciosos

A Tabela 5.4, demonstra o tempo médio (em segundos) que o nó leva para obter as evidências de confiança da rede para cada um dos cenários avaliados. O tempo necessário para o nó obter as evidências de confiança da rede é igual para os cenários com 10%, 20% e 30% de nós maliciosos, no entanto, o nó necessitou de um tempo maior para obeter as evidências de confiança ao ser considerado que 50% dos nós da rede agiam de forma maliciosa, este aumento está diretamente relacionado ao número de interações necessárias para que o nó possua o conhecimento total da rede.

Tabela 5.4: Tempo - Raio de Transmissão = 30m.

α	10% Nós Maliciosos		20% Nós Maliciosos		30% Nós Maliciosos		50% Nós Maliciosos	
	Tempo (s)	Nó (%)	Tempo (s)	Nós (%)	Tempo (s)	Nós (%)	Tempo (s)	Nós (%)
0,0	50	100	50	100	50	100	80	100
0,1	60	100	60	100	60	100	90	100
0,2	70	100	70	100	70	100	100	100
0,3	80	100	80	100	80	100	110	100
0,4	90	100	90	100	90	100	120	100
0,5	100	100	100	100	100	100	130	100
0,6	110	100	110	100	110	100	140	100
0,7	120	100	120	100	120	100	150	100
0,8	130	100	130	100	130	100	160	100
0,9	140	100	140	100	140	100	170	100
1,0	150	100	150	100	150	100	180	100

Assim como no experimento anterior, o *TRUMIT* mostrou-se resiliente a nós maliciosos e obteve o conhecimento total da rede considerando o cenário com raio de transmissão de 50m. As Figuras 5.12, 5.13, 5.14 e 5.15 demonstram as variações das interações realizadas pelo nó para obter as evidências de confiança da rede para as diferentes quantidades de nós maliciosos. Nesta avaliação, não houve alteração com relação ao número de interações necessárias para que o nó obtenha as evidências de confiança da rede para os diferentes cenários avaliados.

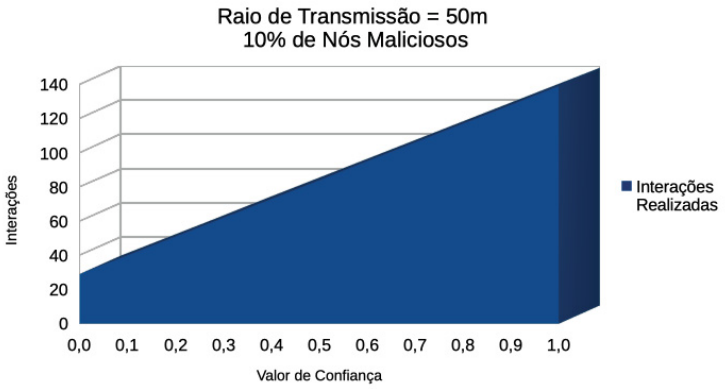


Figura 5.12: Raio de transmissão = 50m
10% nós maliciosos

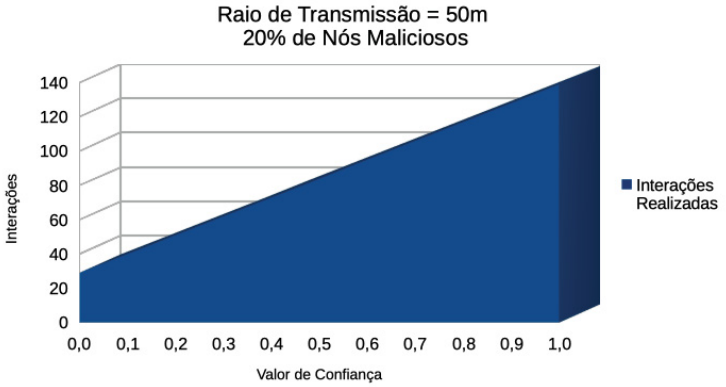


Figura 5.13: Raio de transmissão = 50m
20% nós maliciosos

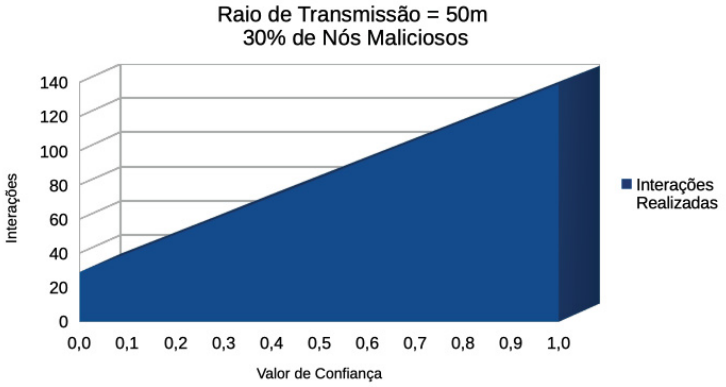


Figura 5.14: Raio de transmissão = 50m
30% nós maliciosos

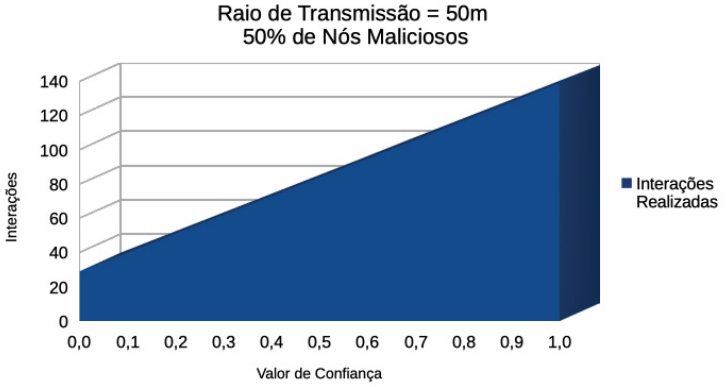


Figura 5.15: Raio de transmissão = 50m
50% nós maliciosos

A Tabela 5.5, mostra o tempo médio (em segundos) que o nó leva para obter as evidências de confiança da rede para cada um dos cenários avaliados.

Tabela 5.5: Tempo - Raio de Transmissão = 50m.

α	10% Nós Maliciosos		20% Nós Maliciosos		30% Nós Maliciosos		50% Nós Maliciosos	
	Tempo (s)	Nó (%)	Tempo (s)	Nós (%)	Tempo (s)	Nós (%)	Tempo (s)	Nós (%)
0,0	30	100	30	100	30	100	30	100
0,1	40	100	40	100	40	100	40	100
0,2	50	100	50	100	50	100	50	100
0,3	60	100	60	100	60	100	60	100
0,4	70	100	70	100	70	100	70	100
0,5	80	100	80	100	80	100	80	100
0,6	90	100	90	100	90	100	90	100
0,7	100	100	100	100	100	100	100	100
0,8	110	100	110	100	110	100	110	100
0,9	120	100	120	100	120	100	120	100
1,0	130	100	130	100	130	100	130	100

Na Figura 5.16, é possível verificar um comparativo entres as interações realizadas pelo nó selecionado para os diferentes cenários avaliados. Nota-se que para os cenários com raio de transmissão de 20m o nó precisou realizar um número elevado de interações para obter as evidências de confiança da rede. Os cenários com raios de transmissão de 30 e 50m, possuem valores próximos, comprovando assim que o *TRUMIT* o desempenho em redes de maior densidade.

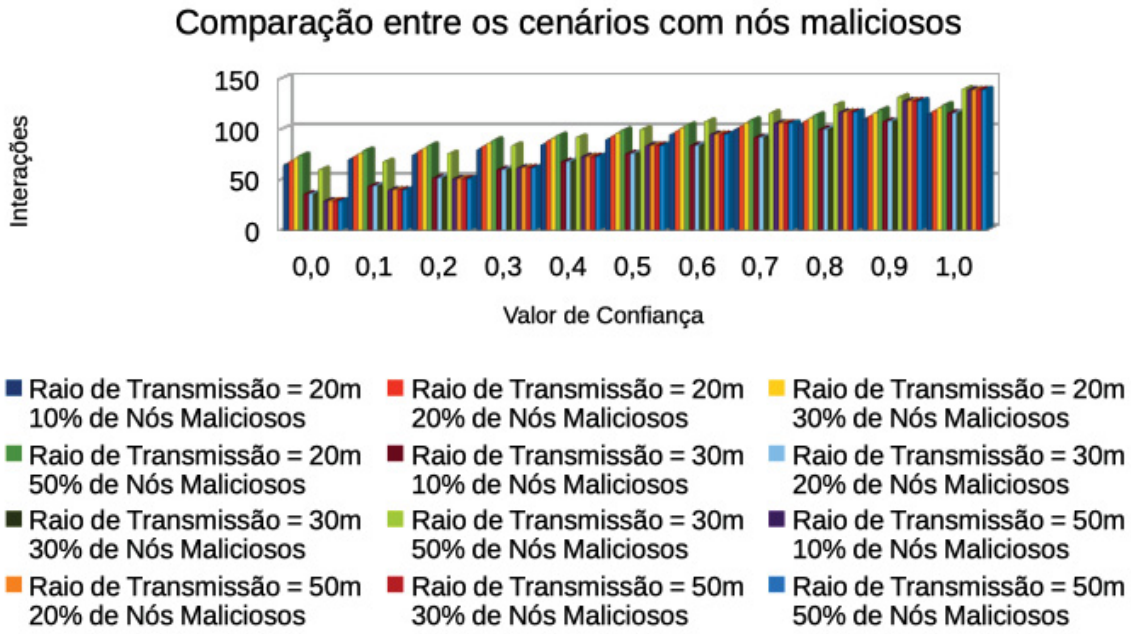


Figura 5.16: Comparação entre os cenários com nós maliciosos

A Figura 5.17, mostra um comparativo das interações realizadas pelo nó para os cenários sem nós maliciosos e com nós maliciosos. Nesta figura é possível verificar que, em cenários com maior densidade, não há um aumento expressivo entre os valores das interações realizadas pelo nó, o que comprova eficácia e a resiliência do *TRUMIT* em ambientes sem a presença de nós maliciosos bem como, com nós maliciosos.

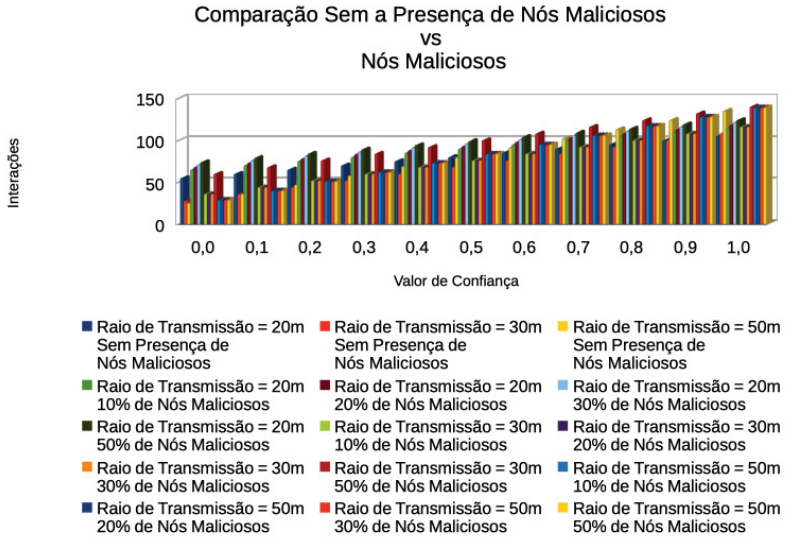


Figura 5.17: Comparação Sem Nós Maliciosos vs Nós Maliciosos

5.5 AVALIAÇÃO GERAL DO *TRUMIT*

De acordo com (Guo et al., 2017) cinco propriedades são desejadas para um sistema de gerenciamento de confiança para *IoT*. Esta seção, avalia a capacidade do *TRUMIT* de satisfazer a tais propriedades.

- Propagação de confiança: O *TRUMIT* realiza a propagação das evidências de confiança para os nós vizinhos de forma distribuída, sem a necessidade de uma entidade de confiança centralizada;
- Agregação de confiança: O *TRUMIT* coleta as informações de confiança através de observações diretas e indiretas, agregando essas informações para formar o valor de confiança utilizando a soma ponderada;
- Atualização da confiança: O *TRUMIT* é capaz de realizar a atualização da confiança de duas formas, sendo a primeira baseada em eventos, onde os dados de confiança são atualizados após uma interação direta entre dois nós, a segunda é baseada pelo tempo, onde em intervalos de tempo pré-determinados, os nós trocam, com seus vizinhos, as evidências de confiança armazenadas em suas redes de confiança;
- Composição da confiança: O *TRUMIT* considera o componente de confiança de qualidade de serviço *QoS* para a composição da confiança;
- Formação de confiança: O *TRUMIT* utiliza duas métricas para calcular o valor de confiança, estas métricas dizem respeito as mensagens enviadas com sucesso e sem sucesso para o nó vizinho.

Com relação à utilização de recursos computacionais, o *TRUMIT* apresentou um resultado satisfatório com relação ao custo da comunicação, conforme pode ser verificado nas Tabelas 5.6 e 5.7, a sobrecarga de comunicação pode ser considerada baixa, visto que não há um aumento significativo no número de mensagens adicionais utilizadas para a troca das evidências de confiança. Conforme descrito no capítulo 4 seção 4.4, o custo de comunicação

está diretamente relacionado à tecnologia de comunicação utilizada pelo dispositivo, assim, o custo de comunicação no *TRUMIT* é representa um valor variável, o qual deve ser levado em consideração, no momento da implementação do modelo proposto.

Tabela 5.6: Total de Mensagens - Raio de Transmissão de 30m.

α	Sem Nós Maliciosos		10% Nós Maliciosos		20% Nós Maliciosos		30% Nós Maliciosos		50% Nós Maliciosos	
	Interações	Msg. Adic.	Interações	Msg. Adic.	Interações	Msg. Adic.	Interações	Msg. Adic.	Interações	Msg. Adic.
0,0	28	19	36	29	36	29	36	19	60	43
0,1	36	19	44	29	44	29	44	19	68	43
0,2	44	19	52	29	52	29	52	19	76	43
0,3	52	19	60	29	60	29	60	19	84	43
0,4	60	19	68	29	68	29	68	19	92	43
0,5	68	19	76	29	76	29	76	19	100	43
0,6	76	19	84	29	84	29	84	19	108	43
0,7	84	19	92	29	92	29	92	19	116	43
0,8	92	19	100	29	100	29	100	19	124	43
0,9	100	19	108	29	108	29	108	19	132	43
1,0	108	19	116	29	116	29	116	19	140	43

Tabela 5.7: Total de Mensagens - Raio de Transmissão de 50m.

α	Sem Nós Maliciosos		10% Nós Maliciosos		20% Nós Maliciosos		30% Nós Maliciosos		50% Nós Maliciosos	
	Interações	Msg. Adic.	Interações	Msg. Adic.	Interações	Msg. Adic.	Interações	Msg. Adic.	Interações	Msg. Adic.
0,0	25	24	29	29	29	26	29	27	29	19
0,1	36	24	40	29	40	26	40	27	40	19
0,2	47	24	51	29	51	26	51	27	51	19
0,3	58	24	62	29	62	26	62	27	62	19
0,4	69	24	73	29	73	26	73	27	73	19
0,5	80	24	84	29	84	26	84	27	84	19
0,6	91	24	95	29	95	26	95	27	95	19
0,7	102	24	106	29	106	26	106	27	106	19
0,8	113	24	117	29	117	26	117	27	117	19
0,9	124	24	128	29	128	26	128	27	128	19
1,0	135	24	139	29	139	26	139	27	139	19

A sobrecarga de memória também é considerada pequena. Nos experimentos realizados, o valor do espaço utilizado para o armazenamento da tabela de confiança do nó, variou entre 50 e 500 *Bytes*, sendo o valor de 50 *Bytes* correspondente a criação da rede de confiança e o valor 500 *Bytes* correspondente ao valor da tabela de confiança contendo todas as evidências da rede.

No entanto, a sobrecarga computacional para manter a rede de confiança atualizada pode ser significativa. Visto que, os nós devem computar os valores de confiança de todos os nós com que mantém conexões de forma direta, bem como, os nós que irá recomendar. Assim, a cada nova interação o nó deverá recalcular o grafo de rede de confiança, considerando as novas informações. Consequentemente, a sobrecarga computacional depende diretamente do tempo de atualização dos valores de confiança e do número de vizinhos de cada nó.

5.6 CONSIDERAÇÕES SOBRE O CAPÍTULO

Após a avaliação do *TRUMIT* em diversos cenários, é possível concluir que o sistema apresenta as funcionalidades necessárias para o gerenciamento de confiança em um ambiente *IoT*. O sistema provou ser resiliente em cenários com nós maliciosos, mantendo valores próximos aos cenários sem nós maliciosos, o que o torna viável para uso no mundo real. No próximo capítulo serão apresentadas as considerações finais e sugestões de trabalhos futuros.

6 CONSIDERAÇÕES FINAIS

A *Internet* das Coisas, irá conectar uma grande quantidade de objetos inteligentes no mundo físico, que vão desde etiquetas de identificação por rádio frequência (*RFID*) até objetos no ciberespaço. A integração desses objetos proporcionará o compartilhamento de informações para a execução de tarefas de nosso dia a dia. No entanto, é necessário garantir que estes os objetos possam estabelecer conexões e compartilhar serviços e informações com um nível de confiança entre si.

A confiança pode ser definida como a crença de que algo não falhará, de que é bem-feito ou forte o suficiente para cumprir sua função. Partido deste princípio, um sistema que gerencie o nível de confiabilidade entre os objetos em um ambiente de *IoT*, irá proporcionar aos objetos uma tomada de decisão adequada a fim de estabelecer uma comunicação eficiente e confiável entre seus pares. Para atingir esse objetivo, diversas soluções de gerenciamento de confiança para *IoT* foram propostas e cada uma delas apresentam ganhos significativos para o gerenciamento de confiança para *IoT*. Mas, ainda é necessário realizar novos avanços nesta área.

Este trabalho propõe um novo modelo de confiança, denominado *TRUMIT* para gerenciar relações de confiança entre dispositivos em um ambiente *IoT*. O modelo proposto é totalmente descentralizado e distribuído, assim, os objetos podem identificar rapidamente quais outros objetos são confiáveis ou não. Nesta abordagem, cada objeto cria, de forma auto-organizada sua rede de confiança, para obter, avaliar e recomendar informações sobre a confiabilidade dos demais objetos da rede. Os objetos obtêm essas informações através de observações diretas e indiretas. Assim, um objeto calcula localmente o valor da confiança, diminuindo o número de interações entre eles. Com o passar do tempo os objetos vão obtendo informações de confiança de outros objetos que não estão conectados diretamente, através de recomendações e os adicionam a sua rede de confiança, assim quando houver uma interação direta entre eles no futuro, os objetos possuirão um certo nível de confiança entre eles, sem mesmo terem interagido diretamente em outro momento.

Em sua avaliação, o sistema proposto demonstrou resiliência em ambientes com objetos maliciosos, obtendo as evidências de confiança da rede, com valores aproximados aos da avaliação sem objetos maliciosos. Com relação ao uso dos recursos computacionais, a sobrecarga relacionada utilização de tais recursos é considera baixa. Desta forma, é possível concluir que o sistema apresenta as funcionalidades necessárias para o gerenciamento de confiança em um ambiente *IoT*. Como dito anteriormente, novos avanços devem ser realizados, assim, como trabalhos futuros do *TRUMIT* estão:

- Testar o *TRUMIT* em outros cenários, considerando um número maior de objetos e outras tecnologias de comunicação;
- Implementar no *TRUMIT*, um esquema de punição onde, os objetos que não apresentarem um comportamento adequado, serão penalizados a diminuição gradual do seu valor de confiança, facilitando assim, a identificação de objetos maliciosos;
- Adicionar novas métricas para o cálculo do valor de confiança, como consumo de energia, cooperatividade e comunidades de interesses;
- Por fim, testar o *TRUMIT* em um ambiente *IoT* real.

REFERÊNCIAS

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-Sarawi, S., Anbar, M., Alieyan, K. e Alzubaidi, M. (2017). Internet of things (iot) communication protocols. Em *Information Technology (ICIT), 2017 8th International Conference on*, páginas 685–690. IEEE.

Albuquerque, C., Cavalcanti, A., Ferraz, F. S. e Furtado, A. P. (2016). A study on middleware for iot: A comparison between relevant articles. Em *Proceedings on the International Conference on Internet Computing (ICOMP)*, página 32. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Ali, B. e Awad, A. (2018). Cyber and physical security vulnerability assessment for iot-based smart homes. *Sensors*, 18(3):817.

Ashton, K. (2011). That 'internet of things' thing. *RFiD Journal*, 22(7).

Azzedin, F. e Ghaleb, M. (2019). Internet-of-things and information fusion: Trust perspective survey. *Sensors*, 19(8):1929.

Bandyopadhyay, S., Sengupta, M., Maiti, S. e Dutta, S. (2011). Role of middleware for internet of things: A study. *International Journal of Computer Science and Engineering Survey*, 2(3):94–105.

Bao, F. e Chen, I.-R. (2012). Dynamic trust management for internet of things applications. Em *Proceedings of the 2012 international workshop on Self-aware internet of things*, páginas 1–6. ACM.

Bao, F., Chen, I.-R., Chang, M. e Cho, J.-H. (2011). Hierarchical trust management for wireless sensor networks and its application to trust-based routing. Em *Proceedings of the 2011 ACM Symposium on Applied Computing*, páginas 1732–1738. ACM.

Bao, F., Chen, R. e Guo, J. (2013). Scalable, adaptive and survivable trust management for community of interest based internet of things systems. Em *Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on*, páginas 1–7. IEEE.

Bauer, J., Staudemeyer, R. C., Pöhls, H. C. e Fragkiadakis, A. (2016). Ecdsa on things: Iot integrity protection in practise. Em *Information and Communications Security*, páginas 3–17. Springer.

Bhuvaneswari, A. (2017). A survey on internet of things [iot]. *International Journal of Advanced Research in Computer Science*, 8(1).

Billure, R., Tayur, V. M. e Mahesh, V. (2015). Internet of things-a study on the security challenges. Em *Advance Computing Conference (IACC), 2015 IEEE International*, páginas 247–252. IEEE.

Brittes, M. P. et al. (2016). *Proposta de modelo de gestão de confiança para internet das coisas médicas*. Tese de doutorado, Universidade Tecnológica Federal do Paraná, Curitiba - Brasil.

Chelloug, S. A. e El-Zawawy, M. A. (2017). Middleware for internet of things: Survey and challenges. *Intelligent Automation & Soft Computing*, páginas 1–9.

Chen, D., Chang, G., Sun, D., Li, J., Jia, J. e Wang, X. (2011). Trm-iot: A trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems*, 8(4):1207–1228.

Chen, R., Bao, F. e Guo, J. (2016a). Trust-based service management for social internet of things systems. *IEEE transactions on dependable and secure computing*, 13(6):684–696.

Chen, R., Guo, J. e Bao, F. (2016b). Trust management for soa-based iot and its application to service composition. *IEEE Transactions on Services Computing*, 9(3):482–495.

Chen, Z., Ling, R., Huang, C.-M. e Zhu, X. (2016c). A scheme of access service recommendation for the social internet of things. *International Journal of Communication Systems*, 29(4):694–706.

Chernyshev, M., Baig, Z., Bello, O. e Zeadally, S. (2017). Internet of things (iot): Research, simulators, and testbeds. *IEEE Internet of Things Journal*, 5(3):1637–1647.

Cui, J., Xu, W., Zhong, H., Zhang, J., Xu, Y. e Liu, L. (2018). Privacy-preserving authentication using a double pseudonym for internet of vehicles. *Sensors*, 18(5):1453.

da Silva, E. (2014). *SEMAN-uma proposta de Middleware seguro para as redes ad hoc móveis*. Tese de doutorado, UFPR - Universidade Federal do Paraná, Curitiba - Brasil.

de Jesus Júnior, A. A. e Moreno, E. D. (2016). SeguranÇa em infraestrutura para internet das coisas - infrastructure security for internet of things. *GESTÃO. Org-Revista Eletrônica de Gestão Organizacional*, 13.

Dragomir, D., Gheorghe, L., Costea, S. e Radovici, A. (2016). A survey on secure communication protocols for iot systems. Em *Secure Internet of Things (SIoT), 2016 International Workshop on*, páginas 47–62. IEEE.

Dunkels, A., Gronvall, B. e Voigt, T. (2004). Contiki-a lightweight and flexible operating system for tiny networked sensors. Em *29th annual IEEE international conference on local computer networks*, páginas 455–462. IEEE.

Fremantle, P. e Scott, P. (2017). A survey of secure middleware for the internet of things. *PeerJ Computer Science*, 3:e114.

Gajjar, S., Choksi, N., Sarkar, M. e Dasgupta, K. (2014). Comparative analysis of wireless sensor network motes. Em *2014 International Conference on Signal Processing and Integrated Networks (SPIN)*, páginas 426–431. IEEE.

Gambetta, D. et al. (2000). Can we trust trust. *Trust: Making and breaking cooperative relations*, 13:213–237.

Guo, J., Chen, R. e Tsai, J. J. (2017). A survey of trust computation models for service management in internet of things systems. *Computer Communications*, 97:1–14.

ITU, O. (2012). Y.4000: Overview of the internet of things. https://www.itu.int/rec/T-REC-Y.4000/en. Acessado em 07/06/2019.

ITU, O. (2019). Y.4460 : Architectural reference models of devices for internet of things applications. https://www.itu.int/rec/T-REC-Y.4460/en. Acessado em 07/06/2019.

Jøsang, A., Ismail, R. e Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision support systems*, 43(2):618–644.

Khan, R., Khan, S. U., Zaheer, R. e Khan, S. (2012). Future internet: the internet of things architecture, possible applications and key challenges. Em *Frontiers of Information Technology (FIT), 2012 10th International Conference on*, páginas 257–260. IEEE.

Kumar, S. A., Vealey, T. e Srivastava, H. (2016). Security in internet of things: Challenges, solutions and future directions. Em *System Sciences (HICSS), 2016 49th Hawaii International Conference on*, páginas 5772–5781. IEEE.

Long, N. T., De Caro, N., Colitti, W., Touhafi, A. e Steenhaut, K. (2012). Comparative performance study of rpl in wireless sensor networks. Em *2012 19th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*, páginas 1–6. IEEE.

Madakam, S., Ramaswamy, R. e Tripathi, S. (2015). Internet of things (iot): A literature review. *Journal of Computer and Communications*, 3(05):164.

Mahalle, P. N., Thakre, P. A., Prasad, N. R. e Prasad, R. (2013). A fuzzy approach to trust based access control in internet of things. Em *Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2013 3rd International Conference on*, páginas 1–5. IEEE.

Malhotra, J. et al. (2015). Zigbee technology: Current status and future scope. Em *2015 International Conference on Computer and Computational Sciences (ICCCS)*, páginas 163–169. IEEE.

Mendoza, C. V. e Kleinschmidt, J. H. (2015). Mitigating on-off attacks in the internet of things using a distributed trust management scheme. *International Journal of Distributed Sensor Networks*, 11(11):859731.

Mikhaylov, K., Petäjäjärvi, J. e Janhunen, J. (2017). On lorawan scalability: Empirical evaluation of susceptibility to inter-network interference. Em *2017 European Conference on Networks and Communications (EuCNC)*, páginas 1–6. IEEE.

Moinuddin, K., Srikantha, N. e Narayana, A. (2017). A survey on secure communication protocols for iot systems. *IJECS*, 6:21802–21807.

Namal, S., Gamaarachchi, H., MyoungLee, G. e Um, T.-W. (2015). Autonomic trust management in cloud-based and highly dynamic iot applications. Em *ITU Kaleidoscope: Trust in the Information Society (K-2015), 2015*, páginas 1–8. IEEE.

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.

Nitti, M., Girau, R. e Atzori, L. (2014). Trustworthiness management in the social internet of things. *IEEE Transactions on knowledge and data engineering*, 26(5):1253–1266.

Österlind, F., Dunkels, A., Eriksson, J., Finne, N. e Voigt, T. (2006). Cross-level sensor network simulation with cooja. Em *First IEEE International Workshop on Practical Issues in Building Sensor Network Applications (SenseApp 2006)*.

Palade, A., Cabrera, C., White, G., Razzaque, M. e Clarke, S. (2017). Middleware for internet of things: A quantitative evaluation in small scale. Em *A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2017 IEEE 18th International Symposium on*, páginas 1–6. IEEE.

Pandya, H. B. e Champaneria, T. A. (2015). Internet of things: Survey and case studies. Em *2015 international conference on electrical, electronics, signals, communication and optimization (EESCO)*.

Pandya, K. (2015). Comparative study on wireless mobile technology: 1g, 2g, 3g, 4g and 5g. *IJRTER*, 1(1):24–27.

Pawar, A. B. e Ghumbre, S. (2016). A survey on iot applications, security challenges and counter measures. Em *Computing, Analytics and Security Trends (CAST), International Conference on*, páginas 294–299. IEEE.

Rahman, A. e Jain, R. (2015). Comparison of internet of things (iot) data link protocols.

Raza, U., Kulkarni, P. e Sooriyabandara, M. (2017). Low power wide area networks: An overview. *IEEE Communications Surveys & Tutorials*, 19(2):855–873.

Razzaque, M. A., Milojevic-Jevric, M., Palade, A. e Clarke, S. (2016). Middleware for internet of things: a survey. *IEEE Internet of Things Journal*, 3(1):70–95.

Robertazzi, T. G. (2017). *Introduction to computer networking*. Springer.

Ruckebusch, P., Devloo, J., Carels, D., De Poorter, E. e Moerman, I. (2015). An evaluation of link estimation algorithms for rpl in dynamic wireless sensor networks. Em *International Internet of Things Summit*, páginas 349–361. Springer.

Saied, Y. B., Olivereau, A., Zeghlache, D. e Laurent, M. (2013). Trust management system design for the internet of things: A context-aware and multi-service approach. *Computers & Security*, 39:351–365.

Samie, F., Bauer, L. e Henkel, J. (2016). Iot technologies for embedded computing: A survey. Em *Hardware/Software Codesign and System Synthesis (CODES+ ISSS), 2016 International Conference on*, páginas 1–10. IEEE.

Samuel, S. S. I. (2016). A review of connectivity challenges in iot-smart home. Em *Big Data and Smart City (ICBDSC), 2016 3rd MEC International Conference on*, páginas 1–4. IEEE.

Santos, B. P., Silva, L., Celes, C., Borges, J. B., Neto, B. S. P., Vieira, M. A. M., Vieira, L. F. M., Goussevskaia, O. N. e Loureiro, A. (2016). Internet das coisas: da teoria à prática. *Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*.

Singh, N. e Gaur, M. S. (2017). Fundamental concept of internet of things. *International Research Journal of Engineering and Technology (IRJET)*, 4.

Suárez-Albela, M., Fraga-Lamas, P. e Fernández-Caramés, T. (2018). A practical evaluation on rsa and ecc-based cipher suites for iot high-security energy-efficient fog and mist computing devices. *Sensors*, 18(11):3868.

Tiburski, R. T., Amaral, L. A., de Matos, E., de Azevedo, D. F. e Hessel, F. (2016). The role of lightweight approaches towards the standardization of a security architecture for iot middleware systems. *IEEE Communications Magazine*, 54(12):56–62.

Timalsina, S. K., Bhusal, R. e Moh, S. (2012). Nfc and its application to mobile payment: Overview and comparison. Em *2012 8th International Conference on Information Science and Digital Content Technology (ICIDT2012)*, volume 1, páginas 203–206. IEEE.

Tschofenig, H. et al. (2015). Architectural considerations in smart object networking, tech. Relatório técnico, No. RFC 7452, Internet Architecture Board, 2015. https://www. rfc-editor. org/rfc/rfc7452. txt.

Tutunović, M. e Wuttidittachotti, P. (2019). Discovery of suitable node number for wireless sensor networks based on energy consumption using cooja. Em *2019 21st International Conference on Advanced Communication Technology (ICACT)*, páginas 168–172. IEEE.

Wang, J. P., Bin, S., Yu, Y. e Niu, X. X. (2013). Distributed trust management mechanism for the internet of things. Em *Applied Mechanics and Materials*, volume 347, páginas 2463–2467. Trans Tech Publ.

Weber, M. e Boban, M. (2016). Security challenges of the internet of things. Em *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2016 39th International Convention on*, páginas 638–643. IEEE.

Yen, L.-H. e Tsai, W.-T. (2010). The room shortage problem of tree-based zigbee/ieee 802.15. 4 wireless networks. *Computer Communications*, 33(4):454–462.