UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA E INFORMÁTICA INDUSTRIAL

MARISÂNGELA PACHECO BRITTES

PROPOSTA DE MODELO DE GESTÃO DE CONFIANÇA PARA INTERNET DAS COISAS MÉDICAS

TESE

CURITIBA

2016

MARISÂNGELA PACHECO BRITTES

PROPOSTA DE MODELO DE GESTÃO DE CONFIANÇA PARA INTERNET DAS COISAS MÉDICAS

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do grau de "Doutor em Ciências" – Área de Concentração: Engenharia Biomédica

Orientador: Prof. Bertoldo Schneider Junior, Dr. Eng.

Co-Orientador: Prof. Emilio C. G. Wille, Dr. Eng.

CURITIBA

2016

Dados Internacionais de Catalogação na Publicação

B862p Brittes, Marisângela Pacheco

Proposta de modelo de gestão de confiança para internet das coisas médicas/ Marisângela Pacheco Brittes.-- 2016.

86 f. : il. ; 30 cm.

Texto em português, com resumo em inglês Disponível também via World Wide Web

Tese (Doutorado) – Universidade Tecnológica Federal do Paraná. Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Curitiba, 2016

Bibliografia: f. 75-86

1. Internet das coisas. 2. Internet das coisas – Medicina. 3. Tecnologia médica – Tendências. 4. Cuidados médicos – Inovações tecnológicas – Tendências. 5. Internet (Redes de computação) – Tendências. 6. Eletrônica médica – Tendências. 7. Engenharia elétrica – Teses. I. Schneider Junior, Bertoldo. II. Wille, Emílio Carlos Gomes. III. Universidade Tecnológica Federal do Paraná. Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial. IV. Título.

CDD: Ed. 22 – 621.3

Biblioteca Central da UTFPR, Câmpus Curitiba

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
Câmpus Curitiba

Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial

Título da Tese Nº. 144

Proposta de Protocolo de Gestão de Confiança para Internet das Coisas Médicas

por

Marisângela Pacheco Brittes

Orientador: Prof. Dr. Bertoldo Schneider Jr. (UTFPR)
Coorientador: Prof. Dr. Emilio Wille (UTFPR)

Esta tese foi apresentada como requisito parcial à obtenção do grau de DOUTOR EM CIÊNCIAS – Área de Concentração: Eng. Biomédica pelo Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial – CPGEI – da Universidade Tecnológica Federal do Paraná – UTFPR, às 14h do dia 07 de dezembro de 2016. O trabalho foi aprovado pela Banca Examinadora, composta pelos doutores:

Prof. Dr. Bertoldo Schneider Jr.
(Presidente – UTFPR)

Profª. Drª. Andreia Malucelli
(PUC-PR)

Prof. Dr. Raul Sidnei Wazlawick
(UFSC)

Prof. Dr. Rubens Alexandre de Faria
(UTFPR)

Prof. Dr. Roberto Candido
(UTFPR)

Visto da Coordenação:

Prof. Jean Carlos Cardozo da Silva, Dr.
(Coordenador do CPGEI)

DEDICATÓRIA

Dedico este trabalho ao meu primeiro aluno e minha primeira professora, meus pais, que me deram a vida e me ajudaram a me transformar em quem sou, todos os dias.

Por todos aqueles que acreditam que não há limites, quando existe uma razão sempre se encontra um caminho.

AGRADECIMENTOS

Primeiramente agradeço a Deus, meu criador e de todo o conhecimento, ao qual buscamos ter acesso através de nossos humanos esforços. Obrigada por me dar coragem para acreditar e recomeçar tudo após ter perdido.

Aos meus pais, Walfrido e Maria Hortência, pelo imenso amor, por nunca terem deixado de acreditar em mim, até quando eu mesma não acreditava ser possível.

À minha família, em especial à Sandriane, Rodrigo, Luciane, Luceli, Setembrino, Erondina, por sempre me mostrarem o valor de permanecermos juntos, não importa as circunstâncias.

Aos amigos e ao valor da amizade. Agradeço à todos indistintamente por provarem todos os dias o quanto podemos estar perto ou longe, não importando as distâncias geográficas.

Aos que permaneceram sempre ao meu lado, agradeço o apoio, o carinho e a compreensão pelas ausências. De modo especial Isabel, Leo Tostes, Leo Aguiar, Cilis, Deborah, Roberto, Luis Bueno, Vinícius, Luis Anton.

Aos que entraram nesse período em minha vida, sou grata aos novos estímulos e confiança em mim depositadas. Serão sempre lembrados com carinho Laís, Zeli, Diomar, Natalia, Eduardo, Felipe, Vania, Leandra, Claudinei.

Aos amigos que se foram, por terem me ensinado o valor das renúncias em prol de algo que se acredita. Quando optamos por uma coisa, precisamos abrir mão de outras. E aos que retornaram, por terem caminhado comigo no período mais difícil da minha vida acadêmica. Estão todos no meu coração e me recordam constantemente sobre o valor das pessoas em nossa vida.

Aos colegas e amigos da UTFPR, os quais me ajudaram nas dificuldades técnicas do caminho, agradeço imensamente, em especial Paulo. Por me ajudar a vencer mais uma batalha.

Ao meu orientador Bertoldo, agradeço pela coragem e paciência em me orientar, pela confiança no meu trabalho e por me ajudar durante todo esse período.

Ao meu orientador Emilio, por não terem desistido de mim. Por dedicar seu tempo me orientando, por ter acreditado junto comigo e ter me ajudado encontrar um caminho.

Agradeço também aos professores que contribuíram com para que o trabalho fosse aperfeiçoado e concluído. Andreia Malucelli, por todas as sugestões relacionadas à pesquisa e à tese. Ao professor José Roberto Amazonas, por ter me ajudado a melhorar meu artigo até sua publicação. Agradeço imensamente.

Agradeço de um modo geral à todos que de alguma forma contribuíram para que essa jornada chegasse ao fim, gratidão imensa e eterna.

EPÍGRAFE

A imaginação é mais importante que o conhecimento. O conhecimento é limitado, a imaginação circunda o mundo. Albert Einstein

RESUMO

BRITTES, Marisângela P. Proposta de Modelo de Gestão de Confiança para Internet das Coisas Médicas. 102 f. Tese de Doutorado – Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2016.

Nos últimos anos, o paradigma da Internet das Coisas (IoT) foi introduzido, ganhando relevância como uma tecnologia emergente, composta por redes amplamente conectadas e heterogêneas. No contexto médico essas redes suportam diferentes tipos de processos, sendo compostas por diversos tipos de dispositivos denominados objetos, os quais são capazes de interagir uns com os outros, colaborando para atingir um objetivo comum (diagnóstico, tratamento, monitoramento e reabilitação de pacientes). Este cenário caracteriza-se como Internet de Coisas Médicas (IoMT) e um dos maiores desafios a serem superados é o desenvolvimento de mecanismos de gestão de confiança para assegurar trocas de dados com um certo nível de credibilidade. Este trabalho propõe um modelo para gestão de confiança em redes IoMT a partir de conceitos de redes sociais e critérios de relevância biomédica. O modelo proposto baseia-se em um índice de recomendação calculado por um protocolo determinístico de gestão de confiança. Para avaliar sua eficácia, foram criadas simulações com diferentes cenários de redes IoMT. O modelo demonstrou ser útil para detectar objetos com comportamento suspeito na rede, evitando o estabelecimento de relações com estes objetos e minimizando os danos causados à IoMT durante as trocas de dados.

Palavras-chave: Redes Biomédicas, Confiança, Redes Sociais, Internet das Coisas Médicas, IoT.

ABSTRACT

BRITTES, Marisângela P. A Model Proposal for Trustworthiness Management for Internet of Medical Things. 102 f. Tese de Doutorado – Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2016.

In recent years, the Internet of Things (IoT) paradigm has been introduced, getting attention as an emerging technology, built upon pervasive connectivity of objects in heterogeneous networks. Medical environments are composed by many devices named objects that are able to interact with each other and collaborate in order to achieve a common objective (diagnosis, treatment, monitoring and patient rehabilitation). This scenario is characterized as Internet of Medical Things (IoMT) and one of its greatest challenges is to develop trustworthiness mechanisms to assure data exchanges in a certain level of credibility. This work proposes a model to manage trustworthiness for IoMT networks based on social network concepts and biomedical relevance criteria. The proposed model is based on a trust recommendation index, computed by a deterministic trustworthiness management protocol. To evaluate the model effectiveness, simulations were created with different IoMT scenarios. The model demonstrated to be useful to detect objects with suspicious behavior in the network, avoiding their relationships establishment and minimizing the IoMT damage during the data exchanges.

Keywords: Biomedical Network, Trust, Social Networks, Internet of Medical Things, IoT

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE SIGLAS

C-LOR	Co-Location Object Relationship
C-WOR	Co-Work Object Relationship
EM	Embodied Microblogging
EPC	Eletronic Product Code
HIMSS	Healthcare Information and Management Systems Society
IERC	European Research Cluster on the Internet of Things
IOE	Internet das Empresas
IOM	Internet de Media
IOMT	Internet das Coisas Médicas
IOS	Internet de Serviços
IOT	Internet of Things/ Internet das coisas
ITU	União Internacional de Telecomunicações
LMNS	Like Mankind Neural System
M&DC	Management and Data Center
OOR	Ownership Object Relationship
P2P	Peer-to-Peer
PHD	Personal Health Devices
POR	Parental Object Relationship
QOS	Confiança social e confiança na qualidade de serviço
RFID	Radio Frequency Identification
RSSF	Redes de Sensores Sem Fio
SIOT	Social Internet of Things
SOF	Social Organization Framework
SOR	Social Object Relationship
TMP	Trustworthiness Management Protocol
WWW	World Wide Web

SUMÁRIO

1. INTRODUÇÃO

Na última década houve um grande avanço tecnológico nas áreas de sensores, circuitos integrados e comunicação sem fio, levando ao desenvolvimento de Redes de Sensores Sem Fio (RSSF). Este tipo de rede é aplicado no monitoramento, rastreamento, coordenação e processamento em diferentes contextos. Pode-se interconectar sensores para fazer o monitoramento e controle das condições ambientais numa floresta, cidade, ambientes industriais e corpo humano. A interconexão de sensores através de redes sem fio, com a finalidade de executar uma tarefa de sensoriamento maior, pode revolucionar a coleta e processamento de informações (AKYILDIZ et al., 2002). A tecnologia utilizada para desenvolver as RSSF compreende os componentes básicos para a nova geração de internet, com maior abrangência a qual evoluiu para o conceito de Internet das Coisas – Internet of Things (IoT).

A Internet das coisas representa uma tendência tecnológica emergente envolvendo o aumento de objetos e dispositivos com capacidade de sensoriamento, processamento e comunicação de variados tipos de dados, os quais são conectados em rede e fazem uso das capacidades coletivas de objetos em rede. É uma revolução tecnológica que representa o futuro da computação e comunicação (ITU, 2005).

IoT tem um grande potencial tecnológico e econômico, podendo transformar o cotidiano das pessoas e atividades em várias áreas, mas apresenta ainda muitos desafios, representando ainda um paradigma a ser estudado e aperfeiçoado. Questões como falta de padronizações, tanto do aspecto de hardware como protocolos de comunicação, confiabilidade em funcionalidades referentes a autonomia e aumento significativo de diferentes objetos conectados são algumas das questões encontradas neste vasto campo de atuação, as quais representam também novas oportunidades de pesquisa (ITU, 2005).

1.1. RELEVÂNCIA DO TEMA DE PESQUISA

Em IoT os objetos da rede participam ativamente dos processos em tempo real, sendo capazes de interagir e comunicar-se entre si atuando em diferentes processos de negócio e redes

muito semelhantes a redes sociais. Por meio de troca de informações coletadas no mundo físico podem reagir com autonomia e influenciar no contexto onde estão inseridos.

Esse novo cenário implica na possibilidade de que a comunicação e troca de serviços pode ser feita não somente entre objetos e pessoas, mas diretamente entre os objetos, sem intervenção humana. Assim, um dos grandes desafios a serem superados é a questão da confiança para realizar troca de informações.

Nesse sentido, é preciso que sejam constituídos mecanismos de gerenciamento de reputação e confiança, que permitam que os objetos possam estabelecer conexões com um nível predefinido de confiança e deste modo, contribuam para aumentar a credibilidade da IoT. Deve-se ainda considerar as limitações da IoT, como capacidade de processamento e de memória dos componentes, limitações de energia, heterogeneidade e requisitos específicos de cada área de aplicação. Essas características impedem a implementação de mecanismos de confiança tradicionais, tornando-se necessário desenvolver pesquisas que apresentem soluções efetivas para gerenciamento de confiança no contexto da Internet das Coisas.

Alguns trabalhos vêm sendo desenvolvidos propondo o estabelecimento de relacionamentos sociais para gerenciar serviços em rede (ATZORI et al., 2010b; ATZORI et al., 2012) assim como tratar questões de gestão de confiança entre os objetos de redes IoT (LIU et al., 2010; CHEN et al., 2011; BAO et al., 2011, CHEN et al., 2015). Diversos conceitos estão sendo apresentados, com destaque para os trabalhos que estão voltados ao estudo do comportamento dos objetos de redes IoT a partir da perspectiva de redes sociais, abrangendo seus relacionamentos e suas interconexões (BAO; CHEN, 2012). Esses trabalhos propõem soluções para minimizar o impacto de ocorrências de objetos suspeitos ou maliciosos em redes IoT, os quais provocam quebra de serviços e instabilidade entre as conexões dos objetos.

IoT tem ganhado espaço em quase todas as áreas de aplicação, porém na área de saúde seu uso vem se desenvolvendo de modo acelerado em função do crescente aumento de dispositivos pessoais e portáteis para medição e monitoramento de parâmetros biomédicos, denominados *Personal Health Devices* (PHD). Nesse cenário, a dinâmica das redes IoT modificou-se, tornando ambientes médicos e hospitalares mais heterogêneos, compostos de uma grande diversidade de dispositivos conectados, os quais entram e saem da rede.

Para esse contexto específico observou-se uma lacuna nas abordagens para gestão de confiança em IoT, pois não apresentam propostas com foco específico para ambientes médicos,

apresentando modelos para uso em redes compostas por dispositivos genéricos, com conceitos como espalhamento dos dados e comunicação ponto a ponto, os quais nem sempre se aplicam em redes IoT para a área de saúde devido ao tipo de dispositivos utilizados.

Essa associação de conceitos pode mudar a forma como pessoas e objetos se relacionam em uma mesma rede IoT para coleta e troca de dados, de modo cada vez mais autônomo com objetos inteligentes, com menos intervenção humana. É um passo adiante em direção a objetos com maior capacidade cognitiva.

1.2. CARACTERIZAÇÃO DO PROBLEMA

O crescente número de PHDs alavancam a adoção de IoT na área de saúde, sendo necessário propor novos modelos de gerenciamento de confiança de modo que se possam estabelecer a comunicação e troca de serviços entre objetos desconhecidos com limiares desejáveis de confiança.

O gerenciamento de confiança abrange os mecanismos para avaliar, estabelecer, manter e revogar a confiança entre dispositivos que formam parte de uma rede. O parâmetro de confiança pode ser usado para o controle de acesso entre dispositivos, roteamento e detecção de intrusos, entre outros. Geralmente, a noção de confiança está relacionada à reputação, sendo que a primeira é uma derivação da segunda. Reputação é a opinião de um objeto da IoT sobre outro, e é formada com base no histórico de comportamento do objeto avaliado (CHO et al., 2011). Por se tratar de ambientes compostos de objetos heterogêneos, desenvolver esses mecanismos para IoT é um desafio bastante complexo

Nesse contexto existe a necessidade de desenvolver soluções específicas para a Internet das Coisas Médicas (IoMT), por tratar-se de ambientes compostos por equipamentos tradicionais de instrumentação biomédica e novos dispositivos portáteis, vestíveis e/ou pessoais de monitoramento e troca de dados, de modo a preencher esta lacuna ao se estabelecer níveis de confiança predefinidos.

1.3. OBJETIVO

Esta pesquisa tem como objetivo criar um modelo para gerenciamento de confiança para redes IoMT a partir de recomendações entre os objetos levando em conta parâmetros objetivos decorrentes de eventos durante trocas de dados e/ou serviços na rede. O modelo é composto pelo protocolo de gerenciamento de confiança TMP (*Trustworthiness Management Protocol),* expresso por um algoritmo que atua nos objetos calculando as recomendações entre eles, visando identificar objetos danosos ou suspeitos os quais podem prejudicar o desempenho das trocas de dados e/ou serviços. O protocolo utiliza parâmetros que abrangem conceitos de redes sociais para obter o índice de confiança, um fator de relevância biomédica de cada objeto na rede IoMT e um limiar de conexões para cada objeto.

Para atingir o objetivo esperado nesta pesquisa, as seguintes atividades são executadas:

1. Definição de um modelo matemático para descrever o comportamento da rede IoMT
2. Cálculo da recomendação entre os objetos
3. Estabelecimento de um índice de confiança
4. Avaliação dos índices que compõe o a formação da recomendação
5. Avaliação comparativa do desempenho do novo protocolo e índice de confiança

1.4. RELEVÂNCIA DA PROPOSTA

A relevância do trabalho desenvolvido reside no fato de propor um modelo de gestão de confiança específico para redes IoMT, considerando parâmetros determinísticos. Esse protocolo pode ser estendido ou adaptado para redes IoT de outras áreas, adaptando-se novos parâmetros conforme necessidades específicas de outras aplicações.

1.5. CONTRIBUIÇÕES ESPERADAS

As contribuições presentes neste trabalho são:

1. Criação de parâmetros determinísticos para o cálculo de recomendações entre objetos.

2. Definição de um modelo matemático com parâmetros a serem utilizados pelo protocolo de gestão de confiança para redes IoMT.
3. Criação de um fator de relevância biomédica como parâmetro para o protocolo de gestão de confiança.
4. Protocolo para gestão de confiança entre objetos IoMT a partir de relacionamentos sociais, recomendações e fator de relevância biomédica do objeto na rede.
5. Avaliação da proposta com avaliação de desempenho do protocolo proposto e análise de resultados, comparando com outros trabalhos relevantes.
6. Estabelecimento de conexões com níveis predefinidos de confiança em redes IoMT, permitindo trocas de serviços mais confiáveis entre dispositivos.

1.6. PUBLICAÇÕES

BRITTES, M.P., SCHNEIDER, B., WILLE, E. C. G., **A Social Approach to Manage Trustworthiness for Internet of Medical Things,** in Proceedings of XXV Brazilian Congress on Biomedical Engineering – CBEB, 2016.

BRITTES, M.P., SCHNEIDER, B., WILLE, E. C. G., **Trustworthiness Management through social relationships in Internet of Medical Things,** Journal of Communication and Information Systems, Vol. 31, No. 1, pg. 313, 2016, DOI 10.14209/jcis.2016.27

1.7. ESTRUTURA DO TRABALHO

O Capítulo 1 apresenta uma breve introdução do tema e a estrutura geral do trabalho.

O Capítulo 2 trata dos temas fundamentais referentes a IoT, origem, modelos de arquiteturas, componentes básicos, assim como o estado da arte de aplicações na área médica.

O Capítulo 3 introduz conceitos fundamentais de gestão de confiança, alguns modelos existentes e a sua importância para redes IoT.

O Capítulo 4 apresenta a proposta deste trabalho com detalhes técnicos empregados na pesquisa e os resultados preliminares obtidos.

No Capítulo 5 são demonstradas as análises dos resultados das validações realizados em simulação, abrangendo detalhes do ambiente experimental Matlab, discutindo o algoritmo proposto.

No último Capítulo, são apresentadas as conclusões gerais e contribuições deste trabalho assim como propostas de trabalhos futuros.

2. INTERNET DAS COISAS

Depois da criação da internet – World Wide Web – nos anos 90 e da revolução do acesso móvel a internet, a partir de 2000, a internet atualmente encontra-se numa fase que pode ser considerada a mais disruptiva[1] de todas: a internet das coisas.

O conceito de IoT foi proposto inicialmente associado a uma primeira representação para o desenvolvimento de tecnologias para identificação individual de objetos. Esse sistema, denominado EPC (Eletronic Product Code), prevê que todos os objetos físicos sejam conectados via RFID (Radio Frequency Identification) através de um código único EPC, fazendo uso de *TAGS* RFID (EPCGLOBAL, 2009)

Desde então diversas pesquisas vêm propondo soluções para o conceito de IoT (CONTI, 2006; ITU, 2005; EPOSS, 2008; CASAGRAS, 2009), o qual tem ganhado bastante atenção e diversas extensões, devido às novas possibilidades de aplicação e desenvolvimento contínuo de tecnologia para esta área.

Uma outra definição para IoT vem de um grupo oficial formado pela Comunidade Europeia com apoio da União Internacional de Telecomunicações (ITU) denominado *European Research Cluster on the Internet of Things* (IERC), o qual define IoT como uma rede dinâmica com infraestrutura global, capacidades de autoconfiguração e autogerenciamento, baseada em padrões de interoperabilidade de protocolos de comunicação onde objetos físicos e virtuais possuem identidade, atributos físicos e personalidades virtuais, utilizam interfaces inteligentes e são integrados de forma similar no sistema de informações da rede (VERMESAN et al., 2014).

Atualmente as definições de IoT são propostas tomando-se como base diferentes tecnologias e pontos de vista. Alguns pesquisadores propõem soluções IoT baseadas nos conceitos de RFID e EPC (THIESSE et al., 2009), ou como objetos conectados através de

[1] O termo tecnologia disruptiva foi utilizado pela primeira vez por Clayton M. Christensen sendo introduzido em 1995 no artigo “Disruptive Technologies: Catching the Wave”, com Joseph L. Bower como co-autor. Harvard Business Review, Jan 1995. Significa algo que pode causar disrupção, que acaba por interromper o seguimento normal de um processo. Que tem capacidade de romper ou alterar.

serviços de interação pervasiva (BROLL, 2009), assim como também propostas para integração entre objetos e serviços móveis (VAZQUEZ, 2010).

No entanto, a maioria dos pesquisadores se concentram em aplicações específicas ou referentes a funções distintas (YAN et al., 2008) como aplicações envolvendo segurança (RENAULT, 2009; SHOU et al., 2011), gestão de redes (NING et al., 2007) e área médica (TSELENTIS et al., 2010). Com a popularização da internet e das redes de comunicação que permitem mobilidade, IoT tem sido considerada a terceira onda da tecnologia da informação (WANG et al., 2011). De acordo com vários estudos, objetos em uma rede IoT deverão ter identidade única e personalidade virtual, atuando em ambientes inteligentes através de interfaces inteligentes para se conectar ou comunicar em contextos sociais (HUANG et al., 2009). Assim, as tecnologias para IoT podem promover efetivamente a gestão de serviços para desenvolver a integração do mundo físico com o digital, através de ambientes onde todos os objetos podem ser unicamente identificados, reconhecidos, localizados e endereçados, cada vez mais autônomos e inteligentes.

A arquitetura IoT pode ser dividida em três camadas, elas compreendem a camada de sensoriamento, camada de transmissão e camada de aplicação. Na camada de sensoriamento os objetos IoT coletam dados do mundo físico por meio de dispositivos ou sensores, os dados são enviados para a próxima camada usando protocolos diversos como Bluetooth, RFID (MA et al., 2009). Na camada de transmissão é construída a base para comunicação com a rede, a qual recebe dados da camada de sensoriamento, preparando para envio para internet ou redes privadas de sensores, provendo a integração com o mundo físico IoT. Na camada de aplicação são construídas as plataformas de gestão de serviços e dados, provendo acesso a todos os usuários do mundo físico (ZHU et al., 2010). Essas camadas podem ser observadas na Figura 1.

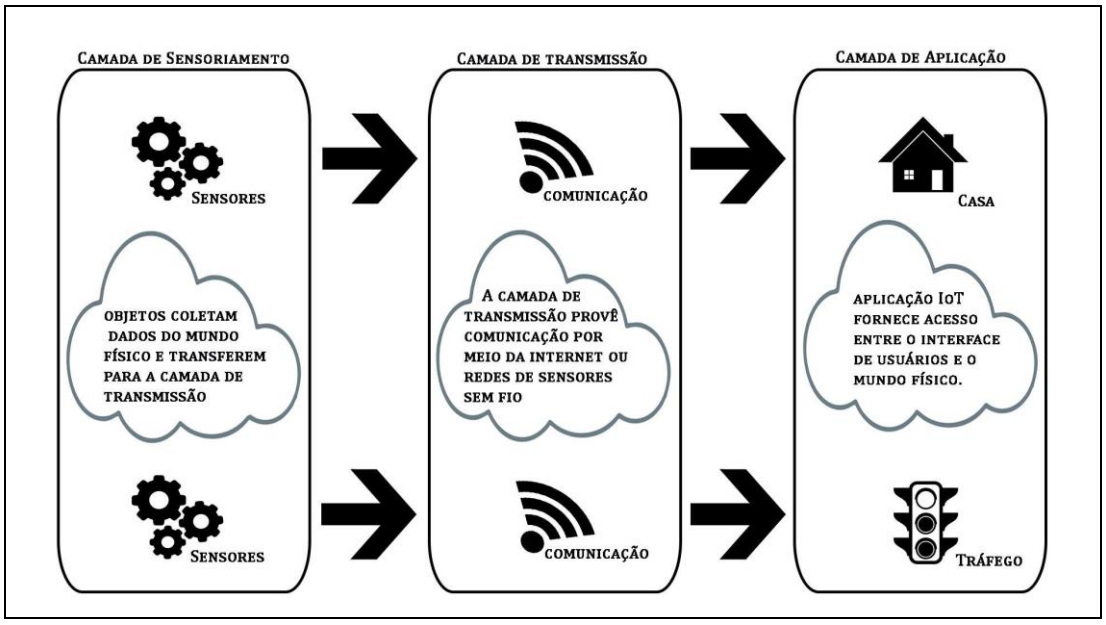

Figura 1: Arquitetura básica de aplicação IoT.

Fonte: Adaptado de (ZHU et al., 2010).

IoT combina diversas tecnologias e abrange muitos campos de pesquisa como arquitetura de redes, identificação remota de sensores e objetos, códigos de identificação única, técnicas de transmissão e agregação de dados, processamento de grandes volumes de dados, segurança e qualidade de serviço da rede.

Existem quatro componentes chaves que são importantes em IoT (COMISSION, 2009):

- Sensores inteligentes: um nó sensor em uma rede tradicional de sensores sem fio é projetada para coletar dados e enviar os resultados para um nó concentrador ou repetidor. Na futura internet IoT os sensores terão mais inteligência embarcada, através de algoritmos com capacidades cognitivas. Assim cada nó sensor poderá atuar como um objeto inteligente ao invés de um simples nó sensor coletor de dados.
- Agregadores de dados: trata-se de processamento moderado de mensagens o qual deve ser projetado para gerenciar a comunicação através de mensagens pelos objetos da rede.
- Rede ubíqua ou pervasiva: objetos geram e trocam informações sobre condições físicas ou status quando solicitações são disparadas. A rede está sempre ativa para alcançar informações para comunicar e realizar troca de dados.

- Serviços de inteligência de contexto: esta característica deve possibilitar aos objetos a capacidade de tomar decisões entre os mesmos, sem a necessidade de intervenção humana, sendo as operações realizadas automaticamente.

Além dos quatro componentes mencionados, existem três características fundamentais que envolvem IoT (VERMESAN; FRIESS, 2014):

- Capacidade cognitiva adequada: distribuição assertiva de sensores para envio e recebimento de dados.
- Robustez do canal de transmissão: capacidade de transmitir dados de forma estável e robusta.
- Processo inteligente: controles de automação programável adaptáveis para diversos ambientes de sensoriamento.

No mundo IoT composto de vários objetos, que compreendem diferentes dispositivos com variados níveis de autonomia, a transmissão segura de dados e confidencialidade, integridade e disponibilidade de dados entre diferentes dispositivos é muito importante. Deste modo, é importante fazer uso de mecanismos para gerenciar a confiabilidade de forma efetiva. A internet das coisas possibilita ligar objetos do mundo real aos do mundo virtual, promovendo a conexão em qualquer lugar, a qualquer momento para qualquer indivíduo. Isso significa um mundo onde objetos virtuais e seres físicos, assim como dados e ambientes virtuais podem todos interagir entre si no mesmo espaço e ao mesmo tempo (ITU, 2005).

A Internet das coisas é parte integrante do conceito de Internet do Futuro, a qual pode ser definida como uma rede global com infraestrutura dinâmica, capacidade de autoconfiguração baseada em padrões e interoperabilidade de protocolos de comunicação onde objetos físicos e virtuais possuem identidades, atributos físicos, personalidades virtuais e uso inteligente de interfaces, sendo integrados facilmente na rede de informações (TSELENTIS et al., 2010).

De acordo com o conceito da internet do futuro, pessoas e objetos estarão conectados a qualquer momento, em qualquer lugar, com qualquer coisa ou qualquer pessoa, utilizando de forma apropriada algum tipo de rede e algum serviço. Na Tabela 1 são apresentados os modelos básicos de internet que compõem o conceito de internet do futuro, os quais compreendem IoT (Internet das Coisas), IoM (Internet de Media), IoS (Internet de Serviços) e IoE (Internet das Empresas).

Tabela 1: Modelos básicos de internet no conceito de Internet do Futuro.

Tipo	Conceito básico
IoT	Conecta redes de sensores sem fio a rede de comunicação móvel e internet. Os nós sensores são considerados como objetos/coisas em IoT.
IoM	Conecta recursos multimídia e aplicações na internet como as que envolvem vídeo e áudio.
IoS	Serviços disponibilizados para os usuários para serem acessados diretamente pela internet. Acesso a conteúdo como livros e serviços online.
IoE	Empresas utilizam a internet para realizar seu processo de negócio e modelo operacional, como modelos business to business (B2B)

Fonte: Adaptado de (TSELENTIS et al., 2010).

Pode se observar que IoT é a parte mais complexa e importante da Internet do Futuro, a qual provê uma plataforma global de tecnologia da informação, que deve combinar redes diferentes com sistemas de grande escala e sistemas físicos-virtuais. (JAMSHIDI, 2011).

As principais áreas de aplicação de IoT atualmente são (COMISSION, 2009):

- Aviação e aeroespacial
- Automotiva
- Telecomunicações
- Edifícios inteligentes
- Engenharia biomédica e atenção à saúde
- Vida assistida
- Indústria farmacêutica
- Cadeia de logística e distribuição
- Gestão de manufatura e ciclo de vida de produtos
- Indústria de petróleo e combustível
- Segurança e privacidade
- Monitoramento ambiental
- Transporte de pessoas e produtos
- Rastreabilidade na cadeia de alimentos

- Agricultura e alimentação
- Mídia, entretenimento e bilhetagem
- Seguros
- Reciclagem

Para que as aplicações em todas essas áreas sejam desenvolvidas, é necessário que tecnologias em diversas áreas sejam melhoradas. As capacidades de comunicação e processamento vêm se tornando mais acessíveis e versáteis, assim como a oportunidade de interconectividade entre diversas tecnologias.

Algumas das principais tecnologias que suportam a expansão de IoT em todos os contextos são listadas a seguir (COMISSION, 2009):

- Tecnologias de identificação
- Arquiteturas de software para IoT
- Tecnologias de comunicação
- Tecnologias de gestão de rede
- Hardware e eletrônica embarcada
- Tecnologias de processamento de dados e sinais
- Tecnologias de economia e armazenamento de energia
- Tecnologias de segurança e privacidade

De todos os itens listados um dos mais importantes e sensíveis em todas as áreas de aplicação se refere às tecnologias relacionadas à confiança, pois ela deve garantir a credibilidade dos processos suportados por tecnologias IoT (BAO; CHEN, 2012)

Mecanismos de encriptação de dados vêm sendo desenvolvidos, assim como algoritmos para garantir a confiança entre objetos na rede durante suas trocas de dados. Neste sentido, questões de confiança entre objetos em redes IoT serão abordados de forma mais detalhada neste trabalho ao longo das próximas sessões.

Dentre todas as áreas de aplicação possíveis para IoT, uma das mais promissoras é a área médica, com uma diversidade crescente de dispositivos criados para uso pessoal e portátil, o que torna esse tipo de rede IoT bastante heterogênea (composta por objetos de diversos tipos e tecnologias) e complexa, com grande potencial mas também limitações e desafios.

2.1. IOT NA ÁREA MÉDICA

Em nenhuma outra área de aplicação os objetos em redes IoT podem se correlacionar tanto como na área médica. Dispositivos de biotelemetria possuem naturalmente informações complementares de modo que a tendência é que compartilhem dados entre si e enviem informações integradas sobre o foco de seu monitoramento (TRANSPARENCY, 2013).

Uma rede IoT é composta de um conjunto de objetos físicos como sensores, atuadores, dispositivos computacionais e capacidades de comunicação de dados, através de uma rede que provê o transporte dos dados.

Nos últimos anos, essas tecnologias vêm sendo desenvolvidas na área de saúde a partir de sua capacidade de monitorar diversos parâmetros, como temperatura, batimento cardíaco, pressão, entre outros (LORINCZ et. al., 2004)

A partir de então, diversos conceitos permeiam a área de saúde, sendo *e-Health* o conceito mais abrangente, utilizado para descrever sistemas que utilizam tecnologia da informação e comunicação para desenvolver modelos centrados na atenção ao paciente. É uma combinação de ciências da vida e tecnologias da informação e comunicação, as quais podem ser usadas para solucionar questões importantes da sociedade, proporcionando benefícios e melhorias significativas para a qualidade de vida das pessoas (COLESCA et al., 2009).

De acordo com a Sociedade de Sistemas de Informação e Gestão em Saúde – HIMSS[2] (*Healthcare Information and Management Systems Society*), *e-Health* diz respeito a qualquer aplicação que utiliza a plataforma internet através de um conjunto de tecnologias da informação com foco em melhorar o acesso, eficiência, efetividade e qualidade de processos clínicos que suportam toda a cadeia de processos a área de saúde. O principal objetivo é prover melhores condições de tratamento em saúde com melhores custos dentro do sistema de saúde.

Nos últimos anos pesquisas extensivas vêm sendo desenvolvidas na área de *e-Health*, muitas delas com foco na utilização da internet para melhorar serviços de saúde, especialmente em formas de reduzir custos e aumentar a qualidade de vida dos pacientes. Uma das discussões

[2] http://www.himss.org

mais importantes encontra-se no papel da internet na melhoria da qualidade dos serviços médicos por meio de plataformas que promovam compartilhamento de informações entre pacientes, especialistas, provedores de serviços de saúde e instituições (BRITTES; SCHNEIDER, 2014).

Com as diversas tecnologias disponíveis em *e-Health* é possível otimizar os processos de gestão e uso de informação de saúde em função do grande e variado número de processos clínicos, operacionais, financeiros e de decisão estratégica, assim como a entrega de serviços em saúde. Desta forma, podem-se aumentar os recursos para acesso à informação, proporcionar aos pacientes um maior controle sobre suas condições de saúde e tomada de decisões, melhoria de processos organizacionais em clínicas e hospitais e aumento de segurança e vida dos pacientes (BRITTES; SCHNEIDER, 2014).

Em *e-Health*, existem diversas áreas de pesquisa e aplicação envolvendo tecnologias para gestão de informações médicas e desenvolvimento de ambientes de vida assistida, telemedicina e monitoramento remoto de parâmetros biomédicos.

A telemedicina e o monitoramento remoto de pacientes, também conhecido como ambiente de vida assistida, são áreas associadas à IoT que têm ganhado interesse especial por sua relação com pacientes crônicos que têm um impacto direto nos sistemas de saúde, sendo compostos em sua maioria por pacientes idosos, com crescimento populacional constante no cenário mundial (STEG, 2006).

Através de recursos tecnológicos integrados, como inteligência artificial e IoT, é possível identificar condições de saúde dos pacientes, aprender sobre seus padrões de comportamento, ganhar inteligência de contexto e definir regras para cenários de estudo envolvendo condições de saúde dos pacientes e seu comportamento (JARA et al., 2009).

Plataformas de monitoramento remoto são capazes de melhorar a vida de pacientes e seus familiares, assim como o trabalho de profissionais envolvidos nos processos de cuidados com a saúde. Também possibilitam a geração de uma quantidade considerável de informações que permitem estudos epidemiológicos relacionados com idade, localização e hábitos da população (JARA et al., 2010).

Outros trabalhos propõem o desenvolvimento de plataformas para *homecare* (cuidados domésticos), visando ampliar as soluções de monitoramento de parâmetros biomédicos de pacientes em ambiente doméstico (MILLAN et al., 2002)

Modelos inteligentes de monitoramento em saúde e formas inovadoras de educação do paciente, assim como frameworks para intervenção preventiva em eventuais ocorrências são cada vez mais necessários. Muitos grupos de pesquisa estão estudando problemas nas mais diversas áreas de saúde, visando explorar todas as possibilidades tecnológicas para prover alertas inteligentes, sistemas de suporte a decisão e monitoramento remoto, para melhorar as condições de vida dos pacientes, em especial os crônicos, através da tecnologia (OLLA et al., 2007)

O interesse nas áreas de pesquisa que envolvem *e-Health* está ganhando cada vez mais importância no mundo todo, estudos vêm sendo desenvolvidos para entender os impactos sócio econômicos e planejar soluções para os problemas mais críticos em saúde, utilizando tecnologia. Um importante estudo mundial foi desenvolvido abrangendo os 21 países mais ricos, visando entender o papel de tecnologias *e-Health* na gestão de doenças e melhoria de condições de saúde da população, concluindo-se que a adoção dessas tecnologias reduz custos operacionais das instituições de saúde, melhorando a gestão de informações e a atenção à saúde dos pacientes (MOEHR, 2006).

Nos últimos anos o paradigma IoT tem sido associado a *e-Health*, e seus conceitos vêm sendo analisados, especialmente as possibilidades de integração de novas plataformas que vêm sendo criadas às soluções já existentes, visto que a área da saúde apresenta um ambiente de soluções tecnológicas heterogêneas, a nível mundial.

O estudo deste campo pode resultar em diversas aplicações para beneficiar a área de saúde, como rastreamento de objetos, permitindo a autenticação de pessoas e dispositivos, para automação da coleta de dados, aplicações de suporte a decisão na área médica e prevenção e detecção de situações de emergência.

No caso dessas aplicações, são utilizados sistemas de difusão de dados, utilizando informações provenientes de sistemas heterogêneos com dados de posicionamento geográfico, áudio e vídeo, acelerômetros e medições de dados biomédicos como pressão sanguínea e batimento cardíaco. Com essas técnicas, é possível antecipar situações de risco e tomar decisões de forma mais apropriada (ISTEPANIAN et al., 2011).

As tecnologias IoT têm sido introduzidas na área da saúde em várias aplicações, como telemedicina e ambientes de vida assistida para melhorar a autonomia e confiança de pacientes, trazendo qualidade de vida e prevenindo acidentes domésticos, monitorando parâmetros biomédicos de pacientes crônicos e otimizando sistemas de saúde tradicionais, sejam públicos ou privados, para que utilizem melhor seus recursos (COMISSION, 2009).

A emergência de soluções de mobilidade, com hardware cada vez mais compacto, de simples operação e alcance de cobertura de rede cada vez maior, permite a evolução de aplicações voltadas a cuidados e atenção à saúde como nunca antes utilizada.

A miniaturização dos componentes eletrônicos e sua integração cada vez mais constante no cotidiano das pessoas tem permitido o desenvolvimento de áreas que aproximam a tecnologia dos hábitos humanos, de forma transparente. Nesse sentido, conceitos como dispositivos vestíveis (*wearables*) e computação ubíqua ou pervasiva, vêm ganhando cada vez mais atenção, tanto na academia como na indústria de tecnologia voltadas a área médica.

No contexto biomédico, pesquisas estão aplicando técnicas de IoT para melhorar funções simples de medição e transferência de dados através da troca autônoma de informações entre dispositivos vizinhos (objetos em uma rede IoT) para apoiar diagnósticos (LEE; OUYANG, 2013).

Medições de dados podem ser adquiridas através de dispositivos sensores e também podem ser recebidas por outros dispositivos médicos por meio de eventos. Os eventos podem aumentar sua frequência de acordo com os dados recebidos e com o nível de interação entre os objetos (SARIT; MANIK, 2011; JIAN et al., 2013).

Na área de saúde, uma grande quantidade de dispositivos são utilizados para monitorar parâmetros, como sensores ambientais, equipamentos biomédicos, dispositivos de biotelemetria, *Tags* RFID para identificação de medicamentos e objetos, leitos hospitalares inteligentes, *tablets* e *smartphones*, sensores veiculares, drones para funções médicas e paramédicas, dispositivos para manutenção preditiva e preventiva de equipamentos, assim como muitos tipos de biosensores vestíveis para monitoramento pessoal da saúde do paciente, implantes internos e robôs para medicação, melhorando o desempenho das ciências da vida por meio das tecnologias. Elas estão se tornando cada vez mais fáceis de utilizar, custarão cada vez menos e proveem informações em tempo real para médicos e pacientes. Em tais ambientes para

cuidados de saúde, incontáveis quantidades de dados são solicitadas e enviadas todo o tempo por muitos tipos de objetos, os quais referenciamos como Internet das Coisas Médicas (IoMT).

A maioria dos hospitais têm utilizado IoMT para os mais diversos propósitos, desde gestão de ativos até controle de temperatura e umidade em salas de cirurgia, assim como biossensores para monitoramento de parâmetros de pacientes, substituindo medições manuais.

Nos próximos anos, o mercado de biossensores deve testemunhar um considerável crescimento por meio de novas tecnologias e aplicações para monitoramento de diabetes, batimento cardíaco, novas drogas tecnológicas, ambientes para cuidados de saúde integrados e medicina preditiva. O aumento da população com diabetes associado a demanda por diagnósticos em ambiente doméstico e pontos de assistência médica tem estimulado o crescimento deste mercado. Além disso, o uso de biossensores em aplicações não médicas também é esperado, para alavancar ainda mais o crescimento da indústria em aplicações para prevenir doenças e evitar intercorrências médicas (TRANSPARENCY, 2013).

Assim há um grande potencial para a criação de aplicações médicas, de modo particular envolvendo o paradigma IoMT, ao conectar uma grande quantidade de dispositivos diversos e promover comunicação de dados através de uma mesma rede padronizada. É claramente necessário o uso de um ambiente de rede resistente e confiável para comunicar e prover serviços, assegurando a qualidade dos dados adquiridos. Em (PASCHE et al., 2008), os pesquisadores desenvolveram um sistema de sensoriamento ótico para monitorar a cicatrização de feridas. Outro grupo desenvolveu um biossensor (WHITWORTH, 2013), o qual é aplicado na pele como uma tatuagem temporária para medir níveis de lactação no suor. Ele incorpora três eletrodos impressos, um dos quais possui um sensor de lactose com seletividade química; os dados são detectados, monitorados e enviados através de um dispositivo de comunicação de dados acoplado.

Outra aplicação interessante é um sensor bucal para monitorar metabólitos na saliva, com potencial para fornecer informações em tempo real sobre saúde, bem estar e até mesmo condições de stress do utilizador (KIM et al., 2014). Com a miniaturização dos circuitos e a integração da eletrônica para aquisição de dados, pode-se realizar o processamento de dados e transmissão wireless, informando potenciais níveis de toxidade e biocompatibilidade.

Todas essas pesquisas podem futuramente permitir que dispositivos possam ser utilizados como sistemas de alerta de longo prazo, avisando os médicos quando uma doença pode ter início ou retornar e apoiando em tratamentos de terapia com medicações invasivas.

Dado o aumento de dispositivos nas redes IoT são necessárias abordagens para proporcionar o melhor gerenciamento de serviços entre os objetos assim como sua organização e atuação. Diversas estratégias vêm sendo propostas envolvendo conceitos de redes sociais, as quais se assemelham a redes heterogêneas e complexas, podendo serem exploradas como base conceitual para novas propostas em IoT.

2.2. REDES SOCIAIS E IOT

A próxima fronteira para IoT no contexto da internet do futuro é promover a interação harmoniosa entre humanos, sociedades e objetos inteligentes conectados em rede (ZHONG, 2010). A pesquisa em IoT desenvolve trabalhos cada vez mais relevantes, principalmente da perspectiva do objeto (*thing-oriented*). Diversas pesquisas são desenvolvidas incluindo identificação e rastreamento de objetos em rede, endereçamento e conectividade, sensoriamento e acesso a dados, controle de objetos, dentre outras (ATZORI et al., 2010a)

Conceitos de redes sociais vêm sendo aplicados em diversas áreas envolvendo redes de comunicação, desde gerenciamento de tolerância a falhas até arquitetura de redes *Peer-to-Peer* (P2P). Recentemente tem surgido propostas de pesquisas visando trazer as capacidades sociais de interação dessas redes para os objetos em IoT. Tais propostas visam a criação de plataformas conceituais, as quais podem ser expandidas para desenvolver e implementar aplicações complexas que necessitem de interação direta entre objetos. O objetivo desses estudos é o desenvolvimento de técnicas que permitam a rede gerenciar a confiabilidade entre objetos através de níveis de relacionamento entre si, como nas redes sociais humanas (ATZORI et al., 2010b)

Os autores em (NING et al., 2011) propuseram dois modelos de arquitetura para IoT, o primeiro baseado nas redes neurais humanas e o segundo como um framework a partir de organização social. Atualmente, a especificação IoT ainda não possui um padrão definido, sendo que muitos pesquisadores discutem possíveis arquiteturas para IoT.

A arquitetura como redes neurais humanas (*Like Mankind Neural System* – LMNS) é composta por três componentes:

- Cérebro: responsável pela gestão dos objetos e centralização dos dados, os quais são chamados M&DC (*Management and Data Center*)
- Medula espinhal: composto de pontos distribuídos para controle de sensores de mais baixo nível
- Rede de nervos: implementa a rede IoT no lado final dos sensores

Essa arquitetura IoT permite a transmissão de mensagens desde os sensores de mais baixo nível para os pontos de controle da camada intermediário, até o nível mais elevado M&DC. Este recebe, traduz e envia mensagens de retorno para os sensores para controlar os objetos/coisas. O M&DC é uma central de dados, com as funções de processamento de informações, armazenamento de dados e gestão da rede IoT.

A segunda arquitetura proposta compreende um framework para organização social (*Social Organization Framework – SOF*), o qual representa três papeis na rede IoT. Para IoT nacional, a arquitetura SOF atua como gerenciador nacional e central de dados, denominada M&DC. Com esses frameworks, o objeto IoT pode ter maior poder computacional e capacidade de alcançar alto nível de cálculos. Assim, esse framework pode oferecer uma maior contribuição para o gerenciamento de confiabilidade para redes IoT.

Para IoT industrial, SOF atua como um gestor industrial e central de dados, o qual é chamado iM&DC. E para IoT regional, SOF corresponde ao gerenciamento local e central de dados, denominado IM&DC. Com diferentes tipos de SOF IoT, cada IoT possui diferentes níveis de políticas de privacidade, monitoramento, segurança e *backup* de dados importantes. A arquitetura LMNS pode ser considerada como uma rede IoT única, assim a SOF consiste de muitas LMNSs como se fossem multi redes IoT.

A maior diferença entre LMNS e SOF é que cada rede única IoT pode trocar informações com outra rede IoT. É como o funcionamento de uma rede social, uma LMNS pode compartilhar seus sensores com diferentes LMNSs. O comportamento e status são parecidos com o que acontece em uma conversa entre humanos na sociedade.

Outras arquiteturas também vêm sendo estudadas, a partir do surgimento da inteligência coletiva nas redes sociais (SUROWIECKI, 2004), tendo sido apontado por diversos pesquisadores como um fator decisivo para uma nova era na ciência.

Sites como *Facebook* e *Twitter* têm sido capazes de armazenar e disponibilizar uma quantidade imensa de dados, a partir de estruturas de redes sociais, tornando-se objeto de estudo para pesquisadores em diversas áreas (KLEINBERG, 2008).

No contexto de redes e comunicação, vem sendo propostos diversos modelos para explorar a similaridade nos interesses entre amigos para serem utilizados em mecanismos de busca na internet (MISLOVE et al., 2006) ou para otimizar redes *Peer-to-Peer* (P2P) (FAST et al., 2005).

Também vem sendo propostos mecanismos que usam relacionamentos sociais para estabelecer níveis mais altos de confiança e desse modo, melhorar a eficiência de soluções de segurança (MARTI et al., 2004; YU et al., 2006).

O primeiro conceito de socialização entre objetos foi introduzido por (HOLMQUIST et al., 2001), no início da expansão das redes sociais e do surgimento dos conceitos de IoT, com foco em soluções para dispositivos sem fio, em sua maioria sensores, ao estabelecer relacionamentos temporários. Os autores também analisam a forma como os donos dos dispositivos controlavam os processos.

Os estudos mais recentes têm se voltado para a pesquisa de aplicações experimentais baseadas em uma nova geração de objetos *smart*, os quais atuam ativamente no cotidiano das pessoas com potencial para atuarem de forma autônoma. Trabalhos sugerem a possibilidade de objetos *smart* interagirem em redes sociais, dando surgimento a um neologismo Blogject, ou seja, objetos que blogam (BLEECKER, 2006).

O conceito teórico de *Embodied Microblogging (EM)* (NAZZ; SOKOLER, 2011), apresenta desafios para a visão atual de IoT. Ao invés de se focar nas interações coisa-coisa ou humano-coisa, ele propõe dois novos papeis que os objetos podem representar: (i) mediar a comunicação humano-humano e (ii) dar suporte a mecanismos de notificação de atividades do cotidiano.

Também existem trabalhos relacionados ao empoderamento dos objetos, através de habilidades de compartilhar figuras, comentários e dados de sensoriamento através de redes

sociais (KRANZ et al., 2010). Discute-se as implicações das chamadas redes sócio técnicas, no contexto de IoT.

Recentemente a ideia de que IoT e redes sociais são mundos muito próximos tem aparecido cada vez mais na literatura. Os autores em (NING; WANG, 2011) propõem o futuro da IoT como uma arquitetura ubíqua, a partir de um modelo para organização social (SOF). Este trabalho apresenta um modelo bastante interessante sobre a estrutura de redes IoT, contudo, não busca inserir características de redes sociais em uma arquitetura IoT. No entanto em (DING et al., 2010), os autores consideram que, estando os objetos inseridos em uma rede conjuntamente com pessoas, as redes sociais podem ser criadas baseadas em IoT, visando estudar a evolução e as relações dos objetos nas redes IoT.

Finalmente, a convergência entre IoT e redes sociais é considerada em (GUINARD et al., 2010), onde um indivíduo humano pode compartilhar serviços oferecidos por seu objeto *smart* com seus amigos e seus objetos. Trata-se de uma rede social para humanos que pode ser utilizada por objetos como uma infraestrutura para serviços de avisos, descoberta e acesso.

Com relação ao conceito de social IoT, de modo mais específico, em (KRANZ et al., 2010) são investigadas as implicações da integração entre IoT e redes sociais, sendo apresentadas algumas aplicações como exemplo. Entretanto, não descreve como as relações sociais deveriam ser estabelecidas entre objetos e não propõe nenhuma solução considerando protocolos e arquitetura necessários.

Em um recente estudo sobre atributos sociais (JIAN et al., 2011), o qual estuda as relações sociais entre os nós em uma rede, foram quantificadas diversas relações sociais entre nós móveis, as quais foram estabelecidas através de parâmetros como fator de interação e fator de distância. Além disso, os autores estudaram o comportamento dos nós moveis através da aplicação da teoria clássica de redes sociais. Entretanto, assume-se que existe uma correspondência de um para um entre humanos e objetos. Por outro lado, em um ambiente típico IoT, muitos objetos podem estar conectados a uma mesma pessoa, enquanto uma grande parte dos objetos permanecerão estáticos ou inseridos no ambiente.

Como resultado dos estudos citados anteriormente, recentemente o termo *Social Internet of Things* – SIoT – começou a aparecer em documentos oficiais e publicação de trabalhos científicos. Muitos destes, seguem as atividades e objetivos a serem alcançados por agendas estratégicas de pesquisa (FINISH, 2011) que visam explorar as potencialidades das redes IoT

em diversos segmentos. O termo SIoT é formalmente cunhado como uma rede composta por objetos que se relacionam entre si a partir dos relacionamentos sociais de seus proprietários (ATZORI et al., 2011).

Por se tratar de uma área de pesquisa bastante recente, é necessário realizar estudos sobre como realmente viabilizar uma rede social de objetos inteligentes. Na verdade, de forma análoga as redes sociais de humanos, uma rede IoT com conceitos sociais deve apresentar: (i) definição de noções de relacionamentos sociais entre objetos, (ii) modelo de referência arquitetural baseado na estrutura de uma rede social com relacionamentos entre objetos, (iii) análise da estrutura da rede social com interações entre objetos baseando-se em relacionamentos sociais. Estudos iniciais relacionados a esses paradigmas foram propostos em (FINISH, 2011), com a proposta de uma arquitetura sugerida a partir de modelos existentes de redes sociais.

Pode-se partir da premissa de que, no futuro, os objetos serão associados a serviços que eles podem entregar. Assim sendo, em uma rede social de objetos, um objetivo chave poderá ser publicar informações e serviços, encontrá-los e descobrir novos recursos para melhor implementar os serviços através de uma consciência do ambiente. Isso pode ser alcançado utilizando uma rede social de objetos com vínculos semelhantes a amizades, ao invés de utilizar ferramentas típicas de descoberta na rede, as quais não conseguirão abranger os trilhões de objetos previstos para as redes do futuro.

A escolha do melhor conjunto de relacionamentos sociais pode ser feita ao se observar amostras de tipologias de aplicações e interações entre objetos. Na sequência associam-se comportamentos sociais dos objetos aos modelos relacionais elementares da teoria de redes sociais (FISKE, 1992; HASLAM, 1994) conforme representados na Tabela 2:

Tabela 2: Relacionamentos básicos.

Modelo Relacional	Descrição breve
Comunhão compartilhada	Equivalência e coletividade entre os membros está acima de qualquer forma de distinção individual
Igualdade de encontro	Relações igualitárias caracterizadas por reprocidade e troca balanceada
Classificação de autoridade	Assimétrica, baseada em precedência, hierarquia, status, comando e deferência.

Preço de mercado	Baseado em proporcionalidade, com interações organizadas com referência a escala comum do raio de valores.

Fonte: Adaptado de (FISKE, 1992; HASLAM, 1994).

Esses padrões de interações entre humanos podem ser aplicados a comportamentos sociais típicos em objetos implementados em aplicações pervasivas. É possível que no futuro muitas aplicações e serviços podem ser associados a grupos de objetos os quais terão sua individualidade suprimida em função do interesse em prover serviços para usuários. Do mesmo modo, muitas aplicações podem necessitar de interações onde cada objeto oferecerá seu serviço específico para a comunidade. Além disso, diversos serviços podem estar disponíveis, os quais envolvem o uso de múltiplos objetos para estabelecer relações assimétricas, como serviços de rede baseados em Zigbee, RFID, NFC, sensores e atuadores. Em outros serviços, os objetos condicionam sua relação de amizade entre eles para alcançar múltiplos benefícios, como serviços cooperativos para redução de consumo de energia em dispositivos sem fio.

A partir destes relacionamentos básicos existentes entre humanos, da avaliação dos possíveis serviços e tipologias de aplicação, os autores em (ATZORI et al., 2011) propuseram alguns relacionamentos básicos nos quais perfis de relacionamentos são definidos conforme a arquitetura de um sistema, conforme descritos a seguir:

- *Parental Object Relationship* (POR): Relacionamento parental entre objetos, estabelecido entre objetos pertencentes a mesma origem de produção, geralmente objetos homogêneos procedentes do mesmo período de tempo e do mesmo produtor/indústria.
- *Co-Location Object Relationship (C-LOR):* Relacionamento entre objetos conforme localização, sejam eles homogêneos ou heterogêneos, que estão sempre no mesmo lugar, como sensores, atuares, objetos *smart* utilizados em alguns ambientes como *smart home* e *smart cities.* Em certos casos, pode-se estabelecer C-LORs entre objetos que usualmente não cooperam entre si para alcançar determinado objetivo. Além disso, são capazes de oferecer a rede uma malha de links curtos através dos relacionamentos.
- *Co-Work Object Relationship (C-WOR):* Relacionamento entre objetos conforme trabalho, estabelecido sempre que os objetos colaboram e oferecem a mesma aplicação IoT, como objetos que estão em contato para serem utilizados

em conjunto cooperando em aplicações de emergência medica, telemedicina, biotelemetria.

- *Ownership Object Relationship (OOR):* Relacionamento entre objetos conforme propriedade, estabelecido entre objetos heterogêneos os quais pertencem ao mesmo dono/usuário, como smartphones, medidores de pressão, console de *games*, *smartwatches*.
- *Social Object Relationship (SOR):* Relacionamento social entre objetos, estabelecido quando objetos entram em contato, esporadicamente ou continuamente, devido ao fato de seus donos entrarem em contato, como dispositivos pertencentes a amigos, colegas de trabalho, companheiros de viagem.

A ideia principal da proposta SIoT é permitir o estabelecimento e gestão de relacionamentos somente entre estes objetos, sem a intervenção humana.

Uma rede SIoT é baseada na ideia de que cada objeto pode buscar por um serviço desejado utilizando seus relacionamentos, listando seus amigos e amigos de amigos, de um modo distribuído que possa garantir que a descoberta de objetos e serviços seja feita de forma distribuída e escalável, a partir dos mesmos princípios que caracterizam as redes sociais entre humanos.

O princípio de navegabilidade da rede SIoT baseia-se no princípio proposto em (TRAVERS; MILGRAM, 1969) sobre o fenômeno do mundo pequeno. Esse paradigma se refere à existência de cadeias curtas de conhecidos entre indivíduos nas sociedades.

De acordo com esse paradigma, cada objeto armazena e gerencia informações relacionadas a suas amizades, implementa funções de busca e eventualmente aplica ferramentas adicionais como confiabilidade do relacionamento para avaliar a lealdade de cada amigo. Claramente o número de relacionamentos tem impacto direto na capacidade computacional e no consumo de bateria, e a eficácia das operações de busca dos serviços. Como resultado, a seleção dos relacionamentos é a chave para o desenvolvimento bem-sucedido de uma rede SIoT.

2.3. SERVIÇOS EM IOT

Uma das principais características de aplicações IoT é a possibilidade de objetos buscarem e fornecerem serviços entre si conforme o contexto em que estão inseridos. Para tanto, é necessário que se faça a descoberta dos indivíduos na rede a partir da busca por serviços e troca de mensagens. Existem trabalhos relacionados a descoberta de serviços e troca de mensagens como apresentado em (WANG et al., 2010), onde cada sensor carrega uma descrição textual no formato de palavras-chave ao requisitar por determinados serviços na rede. Os dados são organizados através de uma hierarquia de duas camadas, onde os que estão na camada mais baixa são responsáveis por grupos de sensores de áreas geográficas e o que está na camada mais alta mantém uma visão geral de toda a rede. Entretanto, essa abordagem não pode ser aplicada para uma busca global devido a limitação da proposta de centralização de informações sobre a rede em um único objeto, com a qual não é possível realizar trocas frequentes de dados.

Em (YAP et al., 2005) o modelo é similar, o qual utiliza três níveis de hierarquia ao invés de dois para trabalhar com dados de mobilidade, mas ainda assim mostra-se inapropriado para grandes redes por exigir grande capacidade computacional e consumo de energia.

Em (OSTERMAIER et al., 2010) os autores propuseram um sistema centralizado onde objetos são encontrados a partir de um modelo de predição que calcula a probabilidade de encontro. Nesse caso, a busca não precisa entrar em contato com todos os objetos, proporcionando escalabilidade na rede. Todavia, não é escalável com relação ao tráfego da rede, pois o número de resultados possíveis é significativamente maior do que o número atual de resultados. Sendo assim, um grande número de objetos é contatado sem nenhuma razão.

No caso das redes SIoT, os objetos possuem capacidades similares ao comportamento humano quando estão em busca de outros objetos e serviços (ATZORI et al., 2011). Deste modo, os relacionamentos que ocorrem em uma rede SIoT devem seguir os princípios estudados nos campos de sociologia e antropologia, como (FISKE, 1992) e (HOLMQUIST et al., 2001), a partir dos quais o dono ou criador define as regras para sua criação. O objeto então cria e gerencia diversos tipos de relacionamentos e os utiliza para navegar na rede, buscando por serviços. O objeto pergunta a seus amigos se eles podem prover um serviço em particular ou se eles possuem alguma conexão que pode prover esse serviço. A Figura 2 a seguir, apresenta um exemplo de uma rede SIoT, onde as linhas finas representam vínculos de relacionamento, e as fortes representam o melhor caminho para o objeto 2 alcançar o serviço desejado.

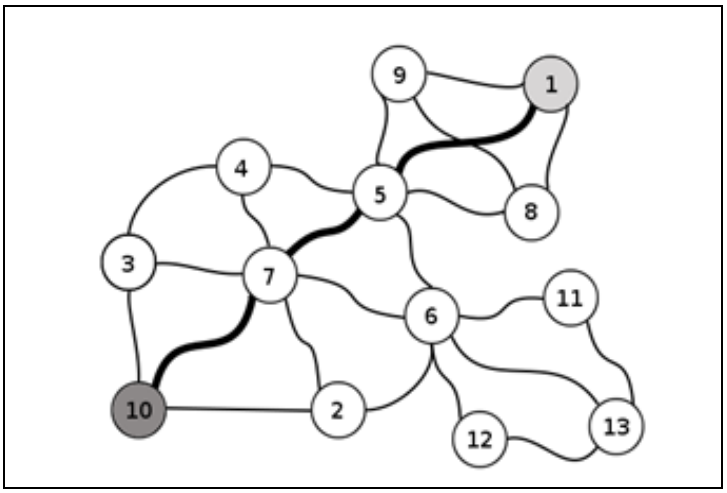

Figura 2: Busca descentralizada em uma SIoT.

Fonte: Adaptado de (ATZORI et al., 2011).

Nessa rede, quando o objeto 1 precisa de um serviço em particular, ele não precisa enviar uma solicitação a uma central de buscas, ele usa seus próprios relacionamentos para buscar, de uma forma descentralizada, um objeto com o serviço desejado, entrando em contato com seus amigos e amigos de seus amigos. Nesse cenário, se faz necessário avaliar o impacto de estratégias para seleção e estabelecimento de contatos, visando estabelecer um número ótimo de relacionamentos para otimizar o uso dos recursos computacionais necessários para as operações de busca.

Essas questões de busca por serviços na rede vêm sendo bastante estudadas nos últimos anos. Em (KLEINBERG, 2001) definiu-se que uma rede é navegável se ela contém caminhos curtos entre muitos ou todos os pares de objetos.

Alguns trabalhos (BOGU, 2009; AMARAL; OTTINO, 2004) descrevem formalmente as condições para navegabilidade da rede: todos ou a maior parte dos objetos devem estar conectados, sendo que a maior distância existente entre os pares de objetos não deve exceder $log_2(N)$, onde N é o número de objetos na rede.

Quando cada objeto possui total conhecimento da conectividade global da rede, encontrar caminhos curtos entre objetos é somente uma questão de distribuição computacional. Entretanto, essa solução não se torna pratica quando existe uma entidade centralizada, a qual deve gerenciar as solicitações de todos os objetos, ou quando os objetos trocam informações entre eles, gerando uma grande quantidade de tráfego na rede.

A partir das pesquisas de Milgram (TRAVERS; MILGRAM, 1969), Kleinberg concluiu que existem meios estruturais que podem ajudar as pessoas a encontrar um caminho eficiente

mesmo sem um conhecimento global da rede (KLEINBERG, 2001; KLEINBERG, 2000). Isso significa que existem propriedades de redes sociais que tornam essa busca descentralizada possível.

Supondo que em uma rede como representada anteriormente na Figura 2, onde o objeto 1 quer acessar informação do objeto 10 (o objeto 1 não sabe onde a informação está localizada); o caminho ótimo apresenta-se como sendo entre os objetos 5 e 7. Entretanto, o objeto 1 tem três possíveis caminhos para escolher e somente sabe poucas informações sobre seus vizinhos: a propriedade que faz com que o objeto 1 escolha o objeto 5 é sua centralidade, o qual possui muitas conexões. Como o objeto 5 apresenta-se como um hub, um ponto central, está conectado com muitos outros. A habilidade de um objeto de rapidamente alcançar um hub é assegurada pela existência de clusters (agrupamentos) onde os objetos são altamente interligados. Essa característica é garantida por meio de um valor alto no coeficiente de cluster local, apresentado em (WATTS; STROGATZ, 1998), calculado para cada objeto na rede.

Assim, o objeto 5 precisa de informações adicionais para escolher o objeto 7 ao invés do objeto 6, pois ambos os objetos estão no mesmo nível. Essa característica é chamada de similaridade, uma propriedade externa a rede, derivada de algumas informações adicionais sobre os objetos. Em uma rede SIoT, a similaridade do objeto dependerá do serviço particular solicitado e do tipo de relacionamento entre os objetos.

A questão envolvendo a navegabilidade da rede transforma-se em um problema local, onde os objetos vizinhos se engajam em negociações para criar, manter ou descartar seus relacionamentos em função de criar hubs e clusters na rede. Nos conceitos propostos em SIoT, os objetos podem criar, através do comportamento de seus donos, diversos tipos de relacionamentos, podendo futuramente serem adicionados outros tipos de relacionamentos.

Para tornar o processo de busca mais eficiente e escalável, foram propostas 5 heurísticas para ajudar os objetos nos processos de seleção do melhor conjunto de amigos. Primeiramente, o objeto aceita todas as solicitações de amizade até atingir o número máximo de conexões permitidas. Esse parâmetro é utilizado para limitar a capacidade computacional que um objeto precisa para resolver uma solicitação de busca de serviço. Então, um objeto aplica uma das seguintes estratégias para gerenciar as solicitações:

1. Um objeto recusa qualquer nova solicitação de amizade até que as conexões estejam estáticas

2. Um objeto aceita novas amizades e descarta amizades antigas em função de maximizar o número de objetos que ele pode alcançar através de seus amigos, i.e, para maximizar a média de conexões. O objeto distribui as conexões entre seus amigos e o objeto com conexão menos importante (menor valor) é descartado.
3. Um objeto aceita novas amizades e amizades antigas para minimizar o número de objetos que ele pode alcançar através de seus amigos, i.e, para minimizar a média de graus entre seus amigos. O objeto distribui conexões entre seus amigos conforme níveis de amizade, o nível com maior importância (maior valor) é descartado.
4. Um objeto aceita novas amizades e descarta amizades antigas em função de maximizar seu próprio coeficiente de cluster. O objeto calcula quantos de seus amigos são amigos em comum, e o objeto com o menor número de amigos em comum é descartado.
5. Um objeto aceita novas amizades e descarta amizades antigas em função de minimizar seu próprio coeficiente de cluster. O objeto calcula quantos de seus amigos são amigos em comum, e o objeto com mais amigos em comum é descartado.

Essas heurísticas podem ser analisadas na Figura 3, conforme apresentada a seguir:

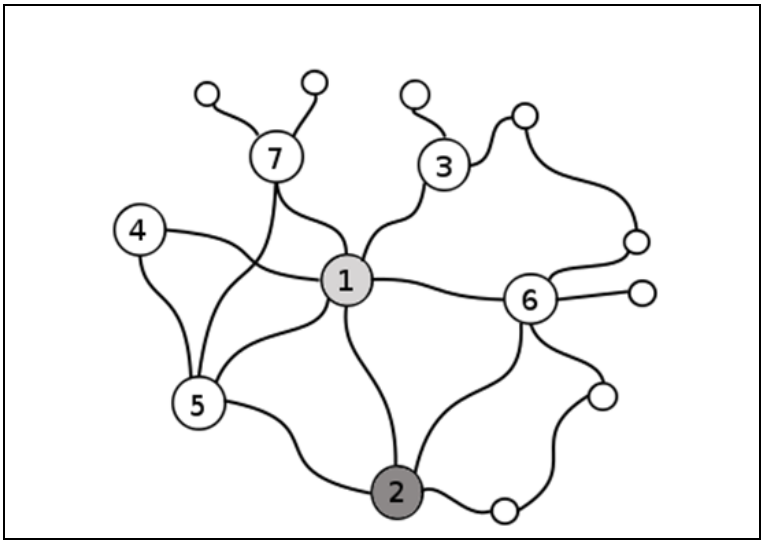

Figura 3: Estratégias de seleção de relacionamentos.

Fonte: Adaptado de (ATZORI et al., 2011).

Considerando-se uma rede como exemplo, conforme figura acima, onde o número máximo de conexões é 5, pode-se supor que o objeto 2 envia uma solicitação de amizade para o objeto 1. O objeto 1 já atingiu número máximo de conexões, então a decisão sobre a solicitação de amizade depende de qual estratégia será implementada. Se o objeto 1

implementar a estratégia 1, ele simplesmente recusará a solicitação. Com a estratégia 2, deverá observar os graus de todos os seus amigos e do objeto 2 e então finaliza seu relacionamento com o objeto 4, o qual possui somente um amigo, em função de aceitar a solicitação do objeto 2, que possui 3 amigos. Do mesmo modo, ao implementar a estratégia 3, o objeto 1 finaliza sua amizade com o objeto 6, o qual possui número máximo conexões, e aceita a solicitação. Com a estratégia 4, o objeto 1 compara amigos comuns entre seus amigos e o objeto que está solicitando amizade, descartando o objeto 3 com o qual não possui nenhum amigo em comum. De modo similar com a estratégia 5 o objeto 1 descarta a amizade com o objeto 5 com o qual possui o número mais alto de amigos em comum.

2.4. CONCLUSÃO DO CAPÍTULO

Este capitulo apresentou os conceitos gerais de IoT, elementos básicos, áreas de aplicação e arquiteturas utilizadas assim como as tecnologias que suportam seu desenvolvimento. Essa fundamentação é base para o desenvolvimento da proposta deste trabalho, com foco na área medica.

A necessidade de novas soluções para essa área demanda novas pesquisas, onde a adoção crescente de IoMT apresenta-se como uma alternativa viável para suportar os processos envolvendo atenção à saúde nos mais diversos ambientes.

3. GESTÃO DE CONFIANÇA

3.1. CONFIANÇA E REPUTAÇÂO

Confiança e reputação são mecanismos de segurança utilizados em ambientes onde diversas entidades podem se comunicar e interagir, a partir de dois atributos encontrados nos relacionamentos humanos: confiança e reputação.

Confiança é um conceito composto proveniente das ciências sociais que envolve não somente segurança, mas também força, bondade e confiabilidade em uma entidade. Deste modo, confiança pode ser definida como 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 (GAMBETTA, 2000).

Reputação é frequentemente utilizada em sistemas de gestão de confiança e é alcançada pelo acúmulo de confiança a partir da avaliação direta ou indireta realizada entre as entidades em decorrência de transações passadas (EDER et al., 2013).

É difícil formalizar tal fenômeno subjetivo pois ao se formalizar esse conceito somente são cobertos alguns aspectos de confiança sendo deixados de lado outros como moralidade e justiça (MARSH, 1994).

Existem diversas abordagens para representar confiança e reputação nas quais entidades ou agentes tomam como base suas decisões. A maioria delas utiliza modelos numéricos para representar estados de confiança através da avaliação da reputação. Algumas propostas representam confiança como uma variável continua em um intervalo definido onde certos subintervalos implicam no quanto a entidade é ou não confiável (MARSH, 1994). Outras usam uma abordagem similar fazendo uso de métricas entre entidades com escalas de intervalos entre 0 e 1 para computar a confiança, onde 0 significa não confiável e 1 significa totalmente confiável (ANURAG, et al., 2007).

Reputação de um modo geral diz respeito à estimativa de como uma entidade se comportara no futuro baseando-se em observações de seu comportamento passado. Pode também ser o acúmulo de diversas observações realizadas por diferentes entidades que se

comunicam ou pode ser somente baseada na experiência de somente uma entidade. Sistemas de reputação têm sido utilizados como uma fonte adicional de informações para que entidades possam confiar e melhorar seu processo de tomada de decisões. Essa fonte é necessária porque é muito difícil que uma entidade sozinha possa considerar cada aspecto possível em uma decisão envolvendo confiança. Além disso, pelo fato da reputação ser constituída por várias experiências de diversas entidades pode ser considerada um ponto de vantagem, pois esse conjunto de experiências oferece informações que uma entidade sozinha poderia não conseguir fornecer (EDER et al., 2013).

De um modo geral os sistemas de confiança e reputação seguem 5 passos (EDER et al., 2013):

- Coleta de informações: o primeiro passo consiste em coletar informações de diversos pontos do sistema. Essas informações dizem respeito ao comportamento das entidades no passado e são um indicador de como é a confiança relacionada a ela. As fontes dessas informações devem ser entidades com experiências em primeiro nível o que significa interação direta e relevante com a entidade no passado.
- Pontuação e classificação: após coletar as informações e dar pesos classificatórios às informações da entidade deve ser criado uma pontuação para calcular a reputação a partir de algum algoritmo de reputação. Depois que a classificação é criada e a recomendação calculada, o nível de confiança pode ser atribuído, sendo a base para a seleção ou não da entidade.
- Seleção da entidade: nesta fase uma entidade seleciona outra a partir de uma lista, as quais oferecem o mesmo serviço. Cada uma delas possui uma pontuação e classificação atribuídas conforme os passos anteriores. Nesta etapa normalmente a entidade com a maior pontuação significa maior índice de confiança.
- Transação: a partir deste ponto a transação pode ser realizada entre as entidades onde uma prove o serviço solicitado.
- Recompensa ou punição: no último passo as entidades classificam a transação baseadas na sua experiência. Para isso, definem-se fatores nos quais a avaliação deve ser baseada.

Com relação a arquitetura para sistemas de confiança e reputação, existem dois tipos básicos: arquitetura centralizada e arquitetura descentralizada (JOSANG et al., 2007).

- Arquitetura centralizada: a característica específica de sistemas de confiança e reputação centralizados é que a pontuação e classificação da experiência em primeiro nível é coletada por um ponto central o qual então gera a reputação a partir dessas informações. Essa classificação fica disponível para toda a rede, onde os participantes podem solicitar informações neste ponto central sobre entidades com as quais desejam realizar transações e assim fazer suas considerações. Esses passos podem ser vistos na Figura 4 a seguir:

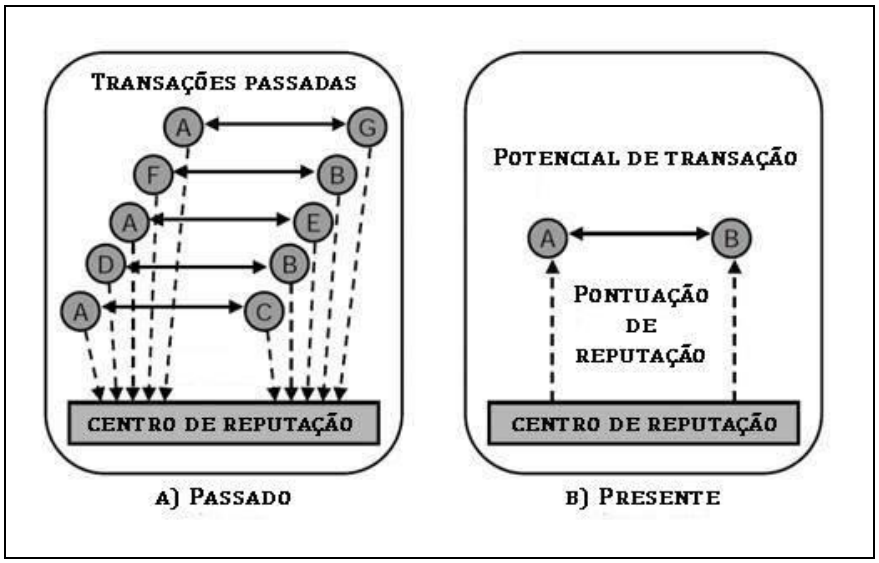

Figura 4. Arquitetura centralizada.

Fonte: Adaptado de (JOSANG et al., 2007).

- Arquitetura descentralizada: em arquiteturas descentralizadas de confiança e reputação cada entidade computa e armazena as informações de classificação sobre transações passadas. As entidades então devem solicitar e coletar essas informações de outras entidades para que possa utilizar essas avaliações como base para sua tomada de decisões. Essas informações podem ser obtidas por entidades periodicamente contatando-se mutuamente para trocar valores de reputação e confiança. Essa arquitetura pode ser vista na Figura 5 a seguir:

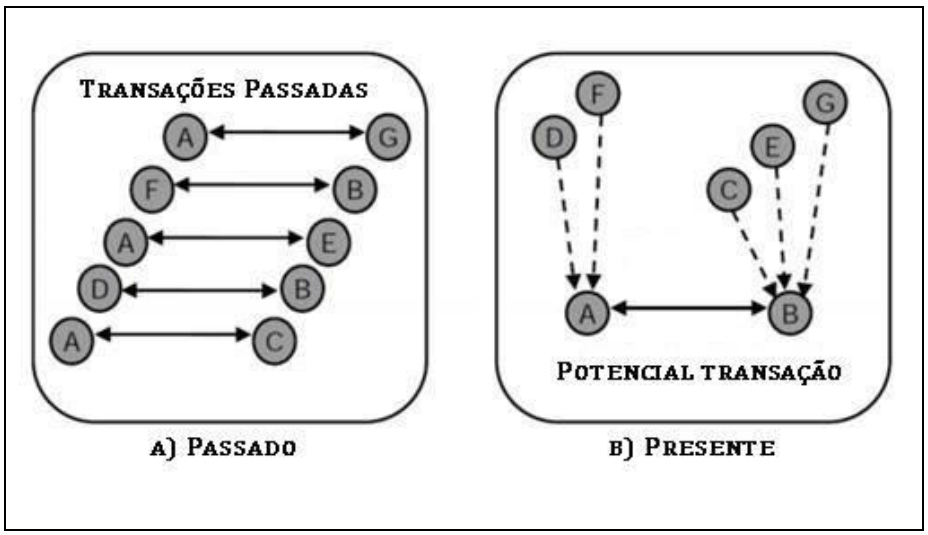

Figura 5. Arquitetura descentralizada.

Fonte: Adaptado de (JOSANG et al., 2007).

Essas arquiteturas são utilizadas como base para a criação de sistemas de confiança e reputação em diversas aplicações online e de comercio eletrônico, sistemas colaborativos e multi-agentes, redes distribuídas e IoT.

3.2. GESTÃO DE CONFIANÇA EM IOT

Gestão de confiança é um mecanismo que permite que os objetos estabeleçam conexões com um nível pré-definido de confiança entre eles, contribuindo assim para a segurança da IoT (CHO et al., 2011)

Em redes 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 estabilidade da rede.

Um grande número de aplicações e serviços para IoT estão emergindo em várias áreas, entretanto sem o desenvolvimento de mecanismos de segurança e privacidade específicos para essas redes podem ocorrer ataques e mal funcionamento, prejudicando seu desempenho (ROMAN et al., 2011).

Mecanismos de gestão de confiança são considerados fundamentais em IoT pois visam facilitar a identificação de mal funcionamento em trocas de serviços nas redes IoT e estabelecer colaboração entre os objetos de forma apropriada. Deste modo é possível prover serviços de qualidade, oferecendo privacidade para os usuários e informações seguras (YAN et al., 2014).

Estudos vêm sendo desenvolvidos no sentido de solucionar problemas relacionados à gestão de confiança entre objetos em redes IoT, selecionando conexões entre objetos confiáveis a partir de diversas estratégias.

Em modelos tradicionais como Peer-to-Peer (P2P) proposto em (KAMVAR et al., 2003), a avaliação é baseada em interações entre pares e investiga questões como pares ou objetos maliciosos na rede e suas relações de confiança. Para calcular a confiança de um par, um sistema armazena informações sobre reputação, estimula o compartilhamento dessa informação entre os pares e define regras a partir da reputação, oferecendo níveis de confiança entre pares. Essas regras podem ser observadas na Tabela 3, a seguir:

Tabela 3: Estratégias usadas em recomendação por reputação.

Armazenamento	**Compartilhamento**	**Processamento**
Centralizado	Local	Media
Distribuído	Parcial	Media do peso
Baseado em taxa (rater based)	Global	Estimativa probabilística

Fonte: Adaptado de (KAMVAR et al., 2003).

Existem diferentes abordagens que podem ser utilizadas para armazenamento de informações sobre confiança. Como descrito em (RESNICK et al., 2000), toda informação pode ser armazenada em um local central para alimentar o compartilhamento e facilitar o processamento. Entretanto, isso converge facilmente para um único ponto de falha. Em (KAMVAR et al., 2003), a informação é distribuída através de pares que a armazenam. Outras abordagens trabalham baseadas em taxa de armazenamento (SELCUK et al., 2004), quando cada par armazena informações sobre confiabilidade sobre os pares que ele tem observado. O armazenamento baseado em rateio (SHERWOOD et al., 2006) utiliza um modelo onde cada par armazena sua própria reputação registrada durante as últimas transações.

Para um sistema de reputação é importante incentivar os pares a cooperarem e resolverem alguns problemas bem conhecidos, como *Free-riders* (ADAR; HUBERMAN,

2000) e *Tragedy commons* (FELDMAN et al., 2000). Uma solução possível foi proposta em (JURCA; FALTINGS, 2000) onde um par pode comprar e vender informações sobre reputação de um para outro par e perder crédito se ele se comporta maliciosamente. Quando um par decide compartilhar sua informação, o sistema deve atuar de forma efetiva para compartilhar essa informação. Esse problema pode ser administrado de diferentes formas: compartilhamento local, compartilhamento parcial compartilhamento global.

No compartilhamento local, cada par somente gerencia a informação na qual ele está envolvido (MARTI; GARCIA-MOLINA, 2003). No compartilhamento parcial, cada par compartilha a informação com uma quantidade definida de pares específicos. Em (SELCUK et al., 2004) os autores propuseram compartilhar informações através de uma cadeia de reputação entre conhecidos e vizinhos, o qual mostrou-se mais resistente do que utilizando pares randômicos (SELCUK et al., 2004; SHERWOOD et al., 2006). E em (ZHOU et al., 2008) os pares podem periodicamente trocar suas informações, a partir de um tempo pré-estabelecido. No compartilhamento global, um mecanismo é adotado para coletar a informação de todos os pares. Isso pode ser feito tanto por meio de um armazenamento central ou por armazenamento distribuído (RESNICK et al., 2000; KAMVAR et al., 2003).

Uma vez que a informação é coletada, é importante usar um sistema computacional que seja capaz de extrair um valor assertivo de confiança. Um mecanismo simples incorre no uso de uma média aritmética (LIANG; SHI, 2003) sobre todos os valores de reputação recebidos por um par. Outros modelos aplicam um peso para os valores de reputação de diferentes formas: os autores de (WANG; VASSILEVA, 2003) usam pesos diferentes para avaliar a reputação de pares conhecidos e pares estranhos; em (YU, 2004) os pesos são escolhidos baseando-se no último valor de reputação que um par recebeu; os autores em (XIONG; LIU, 2004) consideram as similaridades entre dois pares em termos de feedback conhecido como peso para reputação.

Em (KAMVAR et al., 2003) os autores assumem a existência de um grafo de ligações sociais entre os pares, onde os valores de reputação são atribuídos às ligações a partir das transações entre os pares conectados às ligações. Além disso, alguns algoritmos fazem uso de técnicas de estimativas probabilísticas (COMMERCE et al., 2004; DESPOTOVIC; ABERER, 2004), para encontrar os valores de reputação dentro da probabilidade de um par cooperar com outro.

Existem alguns trabalhos sobre gestão de confiança específicos para redes IoT, a qual trata-se de uma área de pesquisa emergente com grande potencial para o desenvolvimento de novas propostas. Em (CHEN et al., 2011), os autores propõem um modelo baseado em reputação utilizando lógica *Fuzzy*, com avaliação de confiança para permitir a cooperação de objetos em uma rede de sensores sem fio, a qual é parte de uma rede IoT, baseando-se em seus comportamentos.

Outro trabalho apresenta um modelo bayesiano de tomada de decisão para controle de acesso em ambientes IoT em larga escala, com uma abordagem objetiva para solucionar os problemas de gestão de confiança (KURNIAWAN; KYAS, 2015).

Em (BAO et al., 2011), foram utilizados parâmetros para avaliar confiança social e confiança na qualidade de serviço (QoS), de acordo com um protocolo de gestão de confiança hierárquico. Os autores de (LIU et al., 2010) por sua vez usaram uma tabela para estimativa de classificação de serviço para avaliar a confiança do usuário. Aspectos sociais em IoT foram estudados em (BAO; CHEN, 2012; CHEN et al., 2015) onde modelos baseados em confiança dos usuários de uma rede social é usada para apoiar a composição dos serviços entre objetos.

3.3. GESTÃO DE CONFIANÇA EM REDES SOCIAIS

Nos últimos anos as redes sociais vêm se tornando cada vez mais populares, consequentemente vem sendo propostos diversos métodos para calcular a confiança e muitas vezes a desconfiança entre duas pessoas (DUBOIS et al. 2011), assim como aplicações que permitem usuários manterem seus dados seguros (CARMINATI et al., 2012a). Nesse cenário, considera-se que uma pessoa (Maria) confia em outra pessoa (José), sendo suas ações baseadas na crença de que o comportamento de José a levará a um bom resultado.

Entretanto, alguns trabalhos (JOSANG, 1997) adicionam outra dimensão ao modelo tradicional de probabilidade de crença e descrença, considerando ignorância como uma parte essencial do comportamento humano.

Os autores em (LIU et al., 2009) classificam redes sociais online em três gerações baseando-se no nível de sociabilidade que elas apresentam, e mostram mecanismos de relação de confiança para cada geração. A primeira geração é caracterizada como fraca socialidade, onde o relacionamento entre os participantes é implícito e os participantes não podem fazer um

novo amigo com um amigo do amigo. A segunda geração tem media socialidade e o relacionamento entre os participantes é apenas binário (amigo ou não amigo), mas os participantes têm a possibilidade de estender sua lista de relacionamento ao adicionar amigos de amigos se estão dentro da mesma plataforma de rede social. Na terceira geração de rede social, existem diferentes tipos de relacionamentos e os participantes podem estabelecer novos relacionamentos e conduzir atividades em diferentes redes sociais. Além disso, múltiplos tipos de relacionamentos entre usuários têm levado ao desenvolvimento de técnicas baseadas em relacionamentos para a gestão da confiança em redes sociais (FONG, 2011; CARMINATI et al., 2012b). De acordo com essa definição, é possível considerar SIoT pertencente a terceira geração com explícito relacionamento não binário entre os participantes.

As principais características relacionadas à confiança estão bem definidas e muitos trabalhos contribuem para descrevê-las (GOLBECK, 2005; GOLBECK; HENDLER, 2005; JOSANG et al., 2006; JOSANG; POPE, 2005; CHRISTIANSON; HARBISON, 1997). Uma das mais importantes e controversas diz respeito à transitividade, baseada no conceito de recomendação de alguém que não é diretamente conhecido, i.e, se Maria confia em José e José confia em João, então Maria confia em João. Além disso, foi demonstrado em (CHRISTIANSON; HARBISON, 1997) que na vida real a confiança não é sempre transitiva mas depende da solicitação de um serviço em particular. Em (JOSANG; POPE, 2005) a confiança pode ser considerada transitiva pois vai depender do propósito a ser avaliado. Nesse caso, devem ser construídas matrizes diferentes para armazenar a reputação de cada serviço, uma vez que se Maria confia em José para consertar seu carro, ela pode não confiar em José para indicar um bom restaurante.

Outra propriedade importante é chamada composabilidade, a qual é a habilidade de compor recomendações provenientes de diferentes amigos em um único valor e então decidir se confia ou não. Com valores diferentes de recomendações de confiança vindos de diferentes amigos, uma função de composição é necessária para se obter resultados mais acurados.

Considerando-se que a confiança está relacionada com a experiência passada de uma pessoa, outra propriedade importante em redes sociais é a personalização. Dessa forma, não é incomum que duas pessoas tenham diferentes opiniões sobre uma mesma pessoa. Por essa razão, confiança é assimétrica, i.e, duas pessoas ligadas através de um relacionamento podem ter diferentes níveis de confiabilidade uma com a outra.

Em uma rede de comunicação, os objetos podem se relacionar de forma cooperativa e de forma individualista. Um objeto pode atuar de forma individualista e ainda assim não ser considerado malicioso, ou seja, pode parar de prover serviços em função de não ter uma forte relação social com o objeto solicitante. Por outro lado, um objeto malicioso procura se inserir na rede para quebrar a cadeia de serviços entre os objetos IoT (BAO; CHEN, 2012).

Ainda segundo (BAO; CHEN, 2012), um objeto malicioso ou duvidoso pode atuar, conforme os comportamentos a seguir:

1. Ataques de autopromoção: o objeto pode promover sua importância na rede a partir de boas recomendações sobre si mesmo, sendo selecionado como um provedor de serviços e então parar de prover o serviço ou prover um serviço com falhas.
2. Ataque de má reputação: o objeto pode prejudicar a reputação de outros objetos com boa reputação na rede, a partir de más recomendações a respeito de objetos bem-intencionados, diminuindo as chances desses objetos serem selecionados como provedores de serviços na rede.
3. Ataque de boa reputação: o objeto pode espalhar boa reputação de objetos maliciosos pela rede, aumentando assim as chances desses objetos serem selecionados como provedores de serviços.

Um objeto malicioso ou duvidoso pode interromper as funções básicas de uma rede IoMT e a troca de dados entre os objetos. Na engenharia biomédica esse quadro é crítico e merece atenção especial principalmente quando os objetos trocam dados biomédicos coletados a partir de funções colaborativas. Se algum desses objetos é afetado, muitos outros poderão ficar fora de serviço, impossibilitados de transmitir ou receber dados, interferindo diretamente em funções de monitoramento, diagnóstico e suporte à vida.

No trabalho posposto, o objetivo é identificar objetos suspeitos que possam danificar a troca de serviços em rede. A proposta abordará 3 tipos de situações que podem acontecer devido a ocorrências com objetos suspeitos na rede, conforme a Figura 6 abaixo:

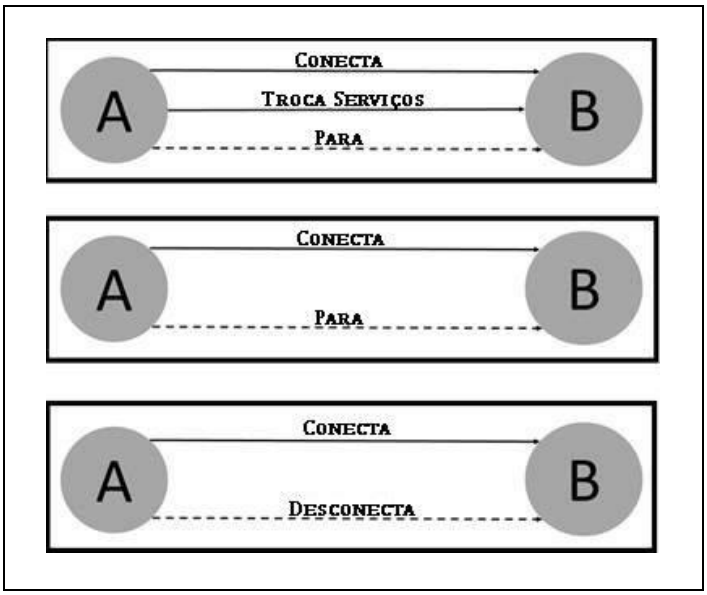

Figura 6. Efeitos de ocorrências com objetos duvidosos.

Fonte: Autoria própria.

No primeiro caso, um objeto A se conecta com o objeto B, troca serviços e subitamente para, provocando quebra de serviços sem perder sua conexão. Deste modo, fica ocioso impedindo que outro objeto estabeleça novo relacionamento para outra troca de serviços.

O segundo caso apresenta uma ocorrência onde o objeto A se conecta com B, sem realizar troca de serviços, novamente impedindo que o objeto B possa se conectar com outro objeto para outra troca de serviços.

O terceiro caso mostra a situação em que o objeto A se conecta com B e subitamente se desconecta, provocando falha na troca de serviços.

Os três casos podem ocorrem em situações de conexão entre apenas dois objetos (1→ 1) ou em caso de um objeto estar conectado com vários (1→N).

3.4. CONCLUSÃO DO CAPÍTULO

Gestão de confiança é uma proeminente área de pesquisa com aplicação em diversos segmentos. Com relação a redes IoT, a elaboração de propostas deve levar em consideração aspectos específicos, pois são compostas por elementos heterogêneos com características como: (i) menor capacidade de processamento, memória e energia, (ii) operam de forma colaborativa

e (iii) executam atividade em rede, compondo um conjunto de elementos que opera com tecnologias diferentes.

Ainda não existem soluções plenamente adequadas para o contexto de IoT, havendo lacunas que devem ser preenchidas com novas propostas de pesquisa. O estudo de questões envolvendo aspectos de confiança em IoT e proposição de suas soluções abrangem algoritmos, técnicas e mecanismos para gestão de IoT. Para tanto é necessário conceber novas propostas capazes de minimizar efeitos danosos à operação dessas redes e defender a integridade das informações gerenciadas.

4. PROTOCOLO DE GESTÃO DE CONFIANÇA PARA IOMT

4.1. DEFINIÇÃO DO PROBLEMA E NOTAÇÃO

Para fins de notação matemática, definiu-se uma rede IoMT como um grupo de objetos $O = \{o_1, o_2, \dots, o_m\}$ com cardinalidade *M*, onde o_i representa um objeto genérico. A rede pode ser descrita como um grafo $R = G(O, E)$ onde $E = \{ e_{jk} \mid \ j, k \in O \ e \ j, k \ se \ relacionam\}$ é um conjunto de ligações (arestas), cada uma representando um relacionamento social entre um par de objetos. Onde $N = \{(o_j, o_k) \mid \ o_j, o_k \in O; \exists \ e_{jk} \in E \ e \ dist(j,k) = 1 \}$ é o conjunto dos objetos vizinhos e $F = \{ (o_i, o_l) \mid \exists \ (e_{ik}, e_{kl}) \in N \times N$ é o conjunto de amigos em comum para um determinado objeto o_i. Essa representação é apresentada no grafo conforme a Figura 7:

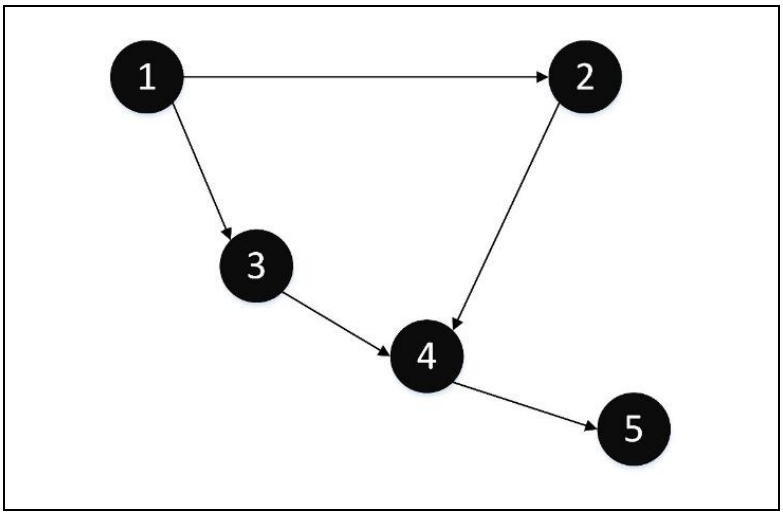

Figura 7. Representação em grafo de objetos em rede IoMT.

Fonte: Autoria própria.

Esse contexto de busca e troca de serviços representa ambientes médicos compostos por muitos tipos de objetos estáticos e móveis, tais como *Tags* RFID para rastreamento de doses de medicamentos e material cirúrgico, dispositivos de comunicação pessoal como smartphones e dispositivos pessoais de monitoramento.

Figura 8. Ambiente médico heterogêneo.

Fonte: Autoria própria.

No ambiente apresentado na Figura 8, muitos tipos de objetos trocam dados. Esses dados podem estar em formatos diferentes, para serem utilizados sozinhos ou em funções de agregação de dados, em cenários cooperativos, assim como em análises de inteligência de contexto. Por exemplo, informações biomédicas de monitoramento de um paciente podem ser recebidas a partir de muitos objetos ao mesmo tempo, correspondendo ao status da saúde do paciente em tempo real.

Quando um objeto solicita uma conexão com outro, algumas suposições podem ser elaboradas, como observado na Figura 9.

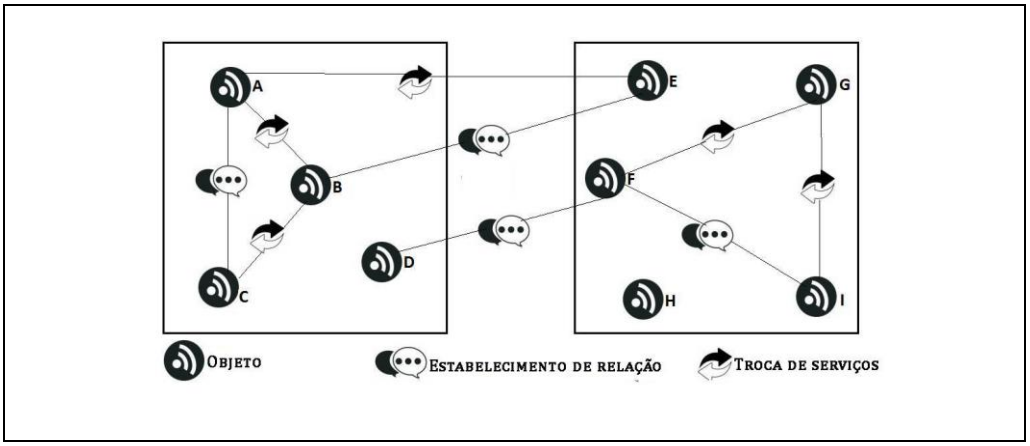

Figura 9: Cenário de solicitação de relacionamentos e troca de serviços.

Fonte: Autoria própria.

Para executar as funções biomédicas de forma apropriada, os objetos necessitam estabelecer relacionamentos e trocar serviços. De modo a garantir a integridade da rede IoMT, é necessária a utilização de mecanismos para realizar a gestão de confiança entre esses objetos. No contexto de uma rede IoMT (Figura 9), o objeto B está trocando serviços com os objetos A e C. A solicita um relacionamento de conexão com C. Nessa situação, pode-se assumir que o objeto B pode recomendar A para C, a partir do relacionamento (amizade) ente A e B. O objeto B está solicitando uma conexão para E, enquanto troca serviços com A. Do mesmo modo que na situação anterior, assume-se que A pode recomendar B para E, baseando-se no relacionamento (amizade) existente entre eles.

Por outro lado, o objeto D não possui relacionamentos estabelecidos nesse cenário e está solicitando uma conexão com F. Nesse caso, pode-se assumir que ninguém (nenhum amigo) pode recomendá-lo, tornando-se mais difícil sua entrada na rede. Pode-se observar também que o objeto H está sozinho (sem conexões), o que dificulta do mesmo modo sua entrada na rede.

Em uma rede IoMT os serviços trocados entre os objetos podem ser exemplificados como dados biomédicos trocados entre sensores para monitoramento de pacientes ou informação sobre medicação fornecida por meio de *Tags*.

Para a área biomédica esse cenário é crítico e merece atenção especial quando devido aos objetos serem coletores de dados biomédicos e possuírem funções colaborativas. Se um desses objetos é afetado, muitos outros poderão ficar comprometidos.

Neste trabalho, assume-se um cenário onde os objetos podem se comunicar mutuamente estabelecendo múltiplas conexões (relacionamentos) para troca de dados e serviços, as quais devem ser executadas de um objeto para outro em ligações ponto a ponto, sem a ocorrência de espalhamento e retransmissão de dados.

Esses relacionamentos podem ser comparados com relacionamentos em redes sociais. De acordo com o tipo de relacionamento, forte ou fraco, as pessoas podem se recomendar mutuamente para novos amigos, ou não, dependendo do conhecimento prévio sobre o outro e com o número de amigos em comum.

4.2. PROPOSTA DE PROTOCOLO DE GESTÃO DE CONFIANÇA

Assume-se uma rede IoMT composta por objetos que realizam interações sociais, como propostos em (ATZORI et al., 2010; ATZORI et al., 2011; ATZORI et al.,2012; BAO et al, 2012; CHEN et al., 2015), em contexto biomédico.

Consideram-se ainda características inerentes a redes sociais (GUIMERÁ et al., 2003), tais como:

i. Cada indivíduo na rede tem capacidade limitada de possíveis amizades

ii. Cada indivíduo possui número balanceado de amizades, equilibrando sua centralidade na rede

iii. Há mudanças nas relações e círculos de amizade ao longo do tempo

Além disso, redes sociais são dinâmicas, onde cada indivíduo possui uma quantidade de tempo disponível assim como de conexões. Os relacionamentos que permanecem devem ter importância para os indivíduos, sendo assim possível definir um limiar de importância para os relacionamentos, conforme o contexto. Esses valores para o limiar de importância ajudarão a calcular o índice de confiança para o modelo proposto.

Para tanto, é apresentada a proposta do Protocolo de Gestão de Confiança – *Trustworthiness Management Protocol* – TMP, com arquitetura descentralizada, a partir de informações distribuídas entre os objetos, os quais consultam uns aos outros para obter recomendações quando da solicitação de novas conexões. Baseia-se nos seguintes critérios:

C1: o índice de confiança é calculado utilizando recomendação indireta entre os objetos

C2: limite de relacionamentos, para gerenciar o número de conexões entre objetos

C3: regras de prioridade, a partir de um fator de relevância biomédica do objeto na rede IoMT

Quando um objeto (k) solicita uma conexão para um objeto (i), o objeto solicitado avalia o índice de confiança $T(i,k)$ do solicitante, consultando seus próprios amigos (N) os quais recomendam ou não a conexão, de acordo com o critério C1, como a seguir:

$$T(i,k) = \sum_{n=1}^{N} R(i,k,n), Onde\ R(i,k,n) = \begin{cases} 1 \\ 0 \\ -1 \end{cases} \quad (1)$$

A Figura 10 ilustra a sequência de passos a serem seguidos em C1:

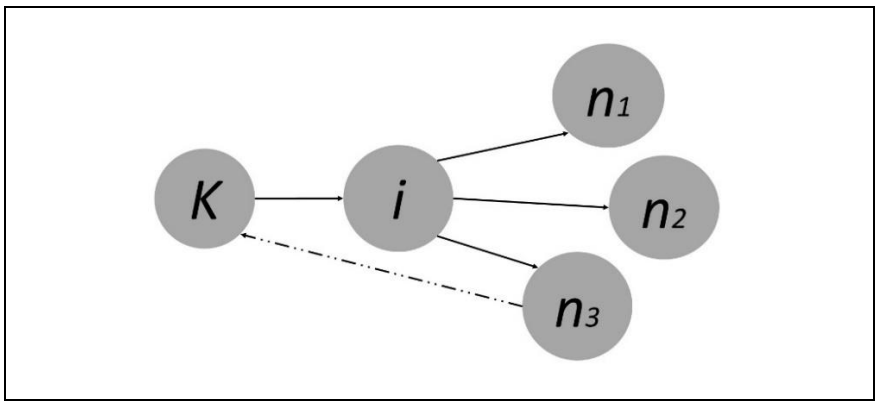

Figura 10: Solicitação de conexão entre *k* e *i*.

Fonte: Autoria própria.

Quando k solicita uma conexão para i, este consulta seus próprios amigos para saber se eles conhecem k e o recomendam. Uma recomendação neutral significa que o objeto n não conhece k ou não tem uma opinião sobre ele. O índice de confiança de k é a soma de todas as recomendações dos amigos de i. O objeto k é aceito para se conectar com i somente se seu índice de confiança é >= 0. Um amigo recomenda outro se seu comportamento está de acordo com o padrão esperado para sua função biomédica, i.e., se é esperado que um objeto envie dados biomédicos em determinado espaço de tempo e ele o faz no tempo esperado, possui uma boa recomendação. Se ele não o faz, forçando seu amigo a esperar mais tempo ser nenhuma resposta, é considerado com comportamento suspeito. Nesse caso, o objeto suspeito possui uma má recomendação.

Se o objeto k possui um índice de confiança aceitável, então o objeto i deve verificar seu próprio número de relacionamentos, de acordo com o critério C2, para garantir que eles podem se conectar:

$$C(i) = C_{Max}(i) - C_t(i) \quad (2)$$

Onde $C(i)$ é o número de conexões disponíveis de i, $C_{Max}(i)$ é o limite de conexões e $C_t(i)$ é o número atual de conexões. Se i não está totalmente conectado ele pode aceitar uma nova solicitação para conexão. Se i já está totalmente conectado, ele deve analisar o status de suas conexões atuais e verificar se ele pode descartar alguma conexão, de modo a aceitar uma nova solicitação.

É necessário então, calcular $D(i,j)$, o índice de descarte:

$$D(i,j) = \frac{\gamma_i}{\Delta T(i,j)} \quad (3)$$

Onde *j* é um objeto já conectado com i. O objeto i descartará a conexão com o objeto *j* com o menor valor *D*, o qual significa a conexão mais inativa em um certo intervalo de tempo ΔT, de acordo com o fator de relevância biomédica γ.

Desta forma i descarta o relacionamento mais inativo e aceita a solicitação de k para conexão em seus relacionamentos.

O fator de relevância biomédica γ em uma rede IoMT é descrito como:

(i) Tipo 3, alta relevância na rede IoMT, como dispositivos de monitoramento e suporte à vida.
(ii) Tipo 2, média relevância na rede IoMT, como dispositivos de rastreamento e RFID/NFC.
(iii) Tipo 1, menor relevância, como dispositivos de informação e comunicação.

Esse fator foi definido a partir da classificação de dispositivos médicos apresentada em (WHO, 2010), conforme a Tabela 4:

Tabela 4: Classificação dos dispositivos médicos.

Contexto de uso	Preventivo	Diagnóstico	Terapêutico	Assistivo
Principais usuários	Profissionais de saúde ou indivíduos saudáveis	Profissionais de saúde ou pacientes	Profissionais de saúde ou pacientes	Profissionais de saúde ou indivíduos
Dispositivos em ambientes médicos	Rastreadores, dispositivos para esterilização	Dispositivos de teste em laboratório, eletrocardiograma, endoscópios, ultrassom	Implantes ortopédicos, equipamento cirúrgico, *stents*.	Camas hospitalares, próteses e órteses, mesas cirúrgicas
Dispositivos em ambientes domésticos	Pedômetros	Oxímetros, monitores cardíacos, monitores de glicose, medidores de pressão	Dispositivos de infusão, dispositivos de diálise, sistemas de oxigênio.	Cadeiras de roda, lentes de contato, implantes

Fonte: Adaptado de (WHO, 2010).

No contexto de IoMT, esses dispositivos podem apresentar três funções básicas: monitoramento de parâmetros biomédicos, rastreamento e identificação de dispositivos e comunicação. Em um ambiente médico avalia-se ainda a entrada de dispositivos pessoais de comunicação e informação que devem se conectar na rede, compondo a categoria de prioridade 1 no fator de relevância biomédica.

A partir dessas funções na rede IoMT, foram propostas classes de dispositivos médicos, de acordo com o fator de relevância biomédica γ, conforme descrito a seguir:

$$\gamma = \begin{cases} 3,\ alta\ relevância \\ 2,\ média\ relevância \\ 1,\ baixa\ relevância \end{cases} \tag{4}$$

Para compor a recomendação de cada objeto é preciso avaliar o índice de confiança $R(n)$ que corresponde ao Critério C1. São tomados como base os seguintes parâmetros objetivos relacionados ao comportamento dos objetos, por meio de 3 índices: estabilidade, integridade e conectividade.

A estabilidade representa a capacidade de troca de mensagens M entre objetos durante seu tempo de conexão T e é expressa como:

$$\sigma = 1 - \gamma\varepsilon \log\left(\frac{M}{T}\right) \tag{5}$$

Onde σ é o índice de estabilidade e ε é o nível de proteção desejado para a rede IoMT. Os valores de ε podem variar de acordo com o γ, os quais podem ser ajustados para avaliar o comportamento dos objetos na rede IoMT de acordo com suas funções.

Por se tratar de uma área de aplicação com dados críticos, é necessário identificar objetos suspeitos ou danosos o mais rápido possível. Isso pode ser realizado ajustando-se o nível de proteção.

Foram desenvolvidas análises matemáticas para avaliar a consistência das fórmulas propostas, a partir de cenários compostos pelas 3 classes de objetos e níveis diferentes de proteção, conforme demonstrado na Figura 11 abaixo:

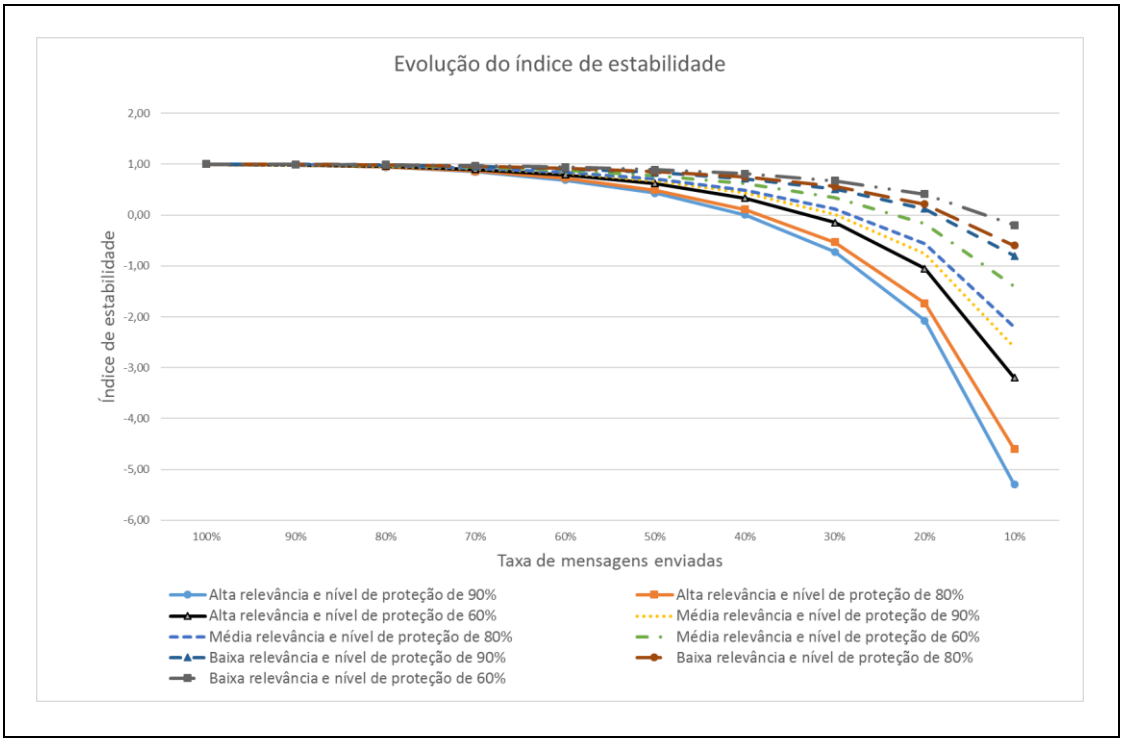

Figura 11: Evolução do índice de estabilidade de acordo com mensagens enviadas.

Fonte: Autoria própria.

O decaimento da taxa de mensagens pode ser considerado como um comportamento suspeito, devido a necessidade constante de troca de dados em IoMT, de modo especial no monitoramento de parâmetros biomédicos. Pode-se observar na Figura 11 que os objetos com maior relevância podem detectar comportamentos suspeitos antes dos outros, computando assim um valor negativo no comportamento do índice de estabilidade, a partir da taxa de 40%. Mesmo quando o nível de proteção corresponde ao valor mínimo de 60% ele percebe comportamentos suspeitos rapidamente. De acordo com o decréscimo da taxa de mensagens trocadas, o índice de estabilidade torna-se negativo.

O segundo índice avaliado corresponde à integridade dos dados do objeto τ, que calcula a quantidade de mensagens descartadas B durante a troca de serviços/mensagens M, descrito por:

$$\tau = 1 - \gamma\varepsilon\frac{B}{M} \tag{6}$$

Considera-se descarte de mensagens como outro comportamento suspeito. Quando a taxa de descarte de mensagens aumenta, os objetos podem atribuir recomendação negativa para o objeto provedor de serviços.

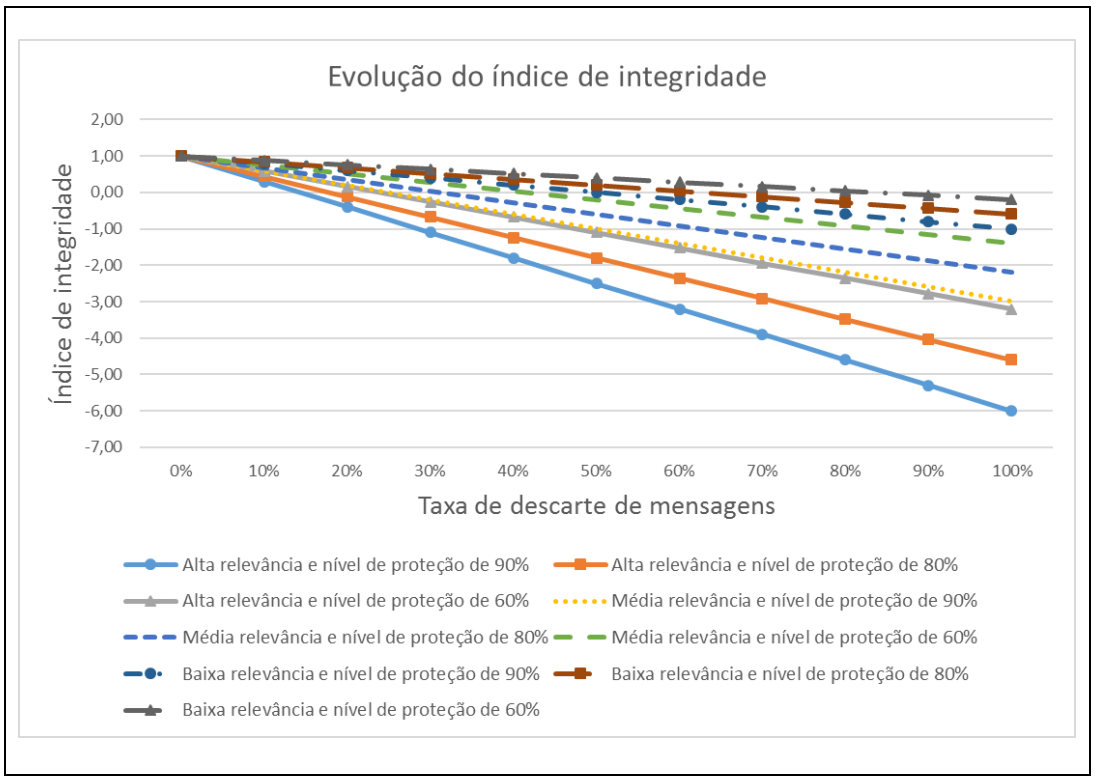

Figura 12: Evolução do índice de integridade de acordo com mensagens descartadas.

Fonte: Autoria própria.

Na Figura 12 observa-se a evolução do índice de integridade de acordo com a taxa de descarte de mensagens, durante troca de serviços entre objetos. Novamente foram aplicados níveis de proteção diferentes variando valores do ε para avaliar o comportamento dos objetos. É possível notar que quanto mais relevante a classe do objeto (relevância 3) mais rápido os objetos identificam comportamentos suspeitos em objetos com crescente taxa de mensagens descartadas.

O terceiro parâmetro considerado trata da conectividade, a qual estima a centralidade do objeto considerando o número médio de suas conexões durante o tempo, considerando sua relevância na rede IoMT e troca de serviços. É descrito por:

$$\theta = \frac{C}{C_{Max}} \tag{7}$$

Onde θ representa a conectividade, considerando a alocação de conexões dos objetos, onde C é o número de conexões do objeto e C_{Max} o limite de conexões.

O cálculo desses três índices compõe a recomendação dos objetos, expressa pelo índice de confiança, conforme a seguir:

$$R = sign(\sigma + \tau + \bar{\theta}) \tag{8}$$

Para evitar discrepâncias, utilizou-se a média de conexões $\bar{\theta}$ e a função `*sign*` para obter somente o sinal da soma resultante. Assim, o valor final será somente -1, 0 ou 1 dependendo do valor de cada índice. Desta forma, é possível computar $R(n)$ e estimar objetos suspeitos na rede IoMT.

Para avaliar a evolução do $R(n)$ foi inferida uma taxa de 50% para θ, sendo possível analisar a taxa de interação entre os objetos, considerando o nível de proteção desejado e a classe dos objetos.

A Figura 13 a seguir mostra que o índice de recomendações cai de acordo com o decréscimo da taxa de interação entre os objetos. A taxa de interação está relacionada com os parâmetros de estabilidade, integridade e conectividade.

A composição de $R(n)$ foi planejada de modo a cobrir os principais aspectos relacionados aos eventos entre objetos durante interações e troca de serviços.

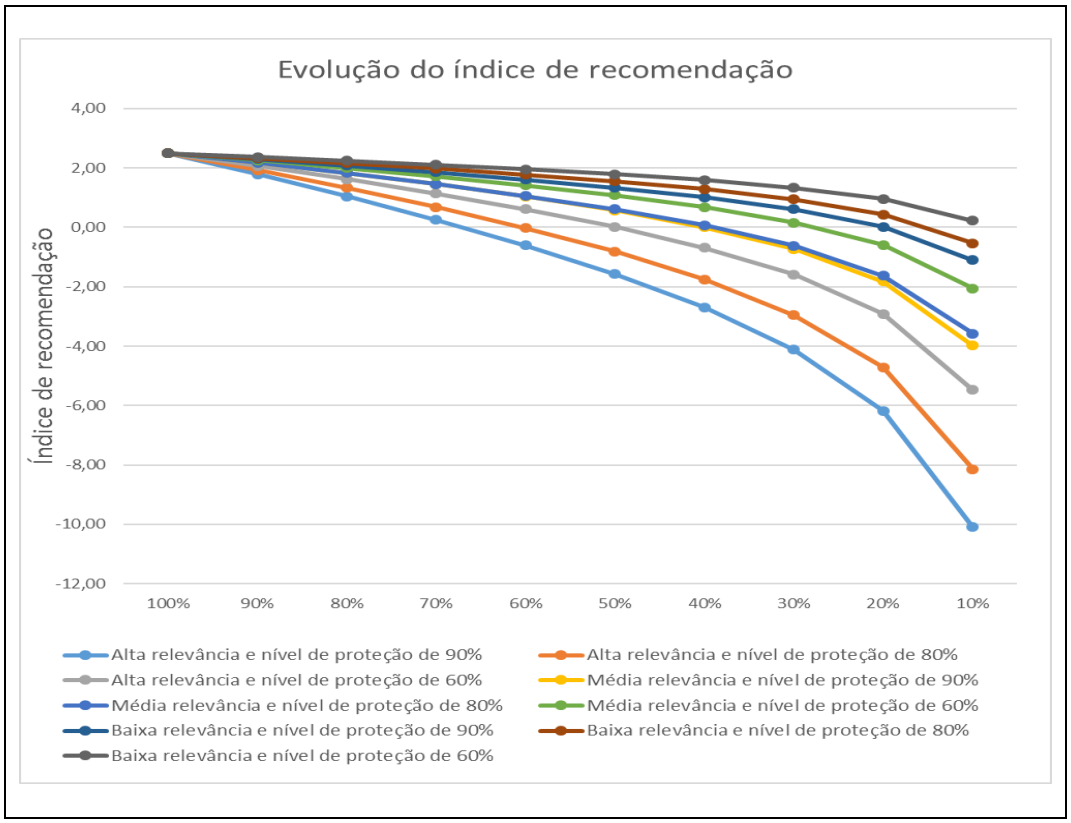

Figura 13: Evolução do índice de recomendação durante interação entre objetos.

Fonte: Autoria própria.

A abordagem proposta no protocolo TMP é determinística ao invés de probabilística. Os eventos propostos para serem avaliados são similares aos que ocorrem em ambientes reais de IoMT, para que as análises sejam próximas de aplicações reais.

A abordagem determinística para gestão de confiança utiliza parâmetros já existentes durante as conexões e trocas de dados entre os objetos, minimizando consumo de energia e capacidade computacional para o cálculo das recomendações. Além disso, não sobrecarrega o canal de comunicação com novos dados avaliados, apenas adicionando critérios sobre os parâmetros que já são utilizados. Considera-se como sendo um diferencial positivo para a adoção do protocolo TMP.

4.3. ANÀLISE COMPARATIVA

A partir da pesquisa bibliográfica realizada nos capítulos anteriores, foi desenvolvida uma análise comparativa da proposta TMP com dois trabalhos relacionados anteriormente, considerados os mais relevantes por utilizarem princípios sociais com propostas de gestão de confiança para IoT. Suas principais características podem ser comparadas com a proposta TMP e são apresentadas na Tabela 5 a seguir:

Tabela 5: Comparação entre algoritmos de gestão de confiança para IoT.

Principais Características	**(Atzori et al, 2011)**	**(Bao et al, 2012)**	**Proposta TMP**
Modelos de algoritmos de gestão de confiança	Subjetivo: a partir da observação e recomendação diretamente de objetos conhecidos (entre objetos); Objetivo: a partir da observação e recomendação em uma tabela local (objetos atualizam periodicamente a informação)	Soma dos resultados de observação direta e indireta entre objetos. Direta: o próprio objeto avalia o comportamento de outro, através de sua observação. Indireta: o objeto solicita recomendações de seus vizinhos próximos confiáveis.	Soma dos resultados de observação direta e indireta entre objetos. Direta: o próprio objeto avalia o comportamento de outro, através de sua observação. Indireta: o objeto solicita recomendações de seus vizinhos próximos confiáveis.
Mobilidade dos objetos	Considera mobilidade a partir da mobilidade física de pessoas em bases de dados reais (CRAWDAD)	Mobilidade física a partir de modelos de redes MANETs	Considera mobilidade de objetos com entrada e saída a partir da mobilidade baseada em pessoas que utilizam dispositivos médicos dispostos em categorias (*World Health Organization*)
Distribuição espacial dos objetos	Distribuição probabilística calculada a partir do tipo de relacionamento estabelecido entre os objetos	Distribuição probabilística dos objetos a partir de uma Cadeia Semi-Markoviana	Distribuição Gaussiana de conexões e movimentação dos objetos
Arquitetura do protocolo de confiança	Arquitetura hibrida, centralizada e descentralizada	Arquitetura descentralizada	Arquitetura descentralizada

Processamento do modelo	O modelo se distribui na camada de aplicação e rede, entre um servidor, gateways e agentes para processamento de informações e busca de serviços.	Todo o modelo concentra-se na camada de rede distribuído entre os objetos	O modelo pode ser ajustado para a camada de aplicação como para a de rede distribuído entre os objetos
Parâmetros de confiança avaliados nos relacionamentos	POR: Relacionamento parental entre objetos pertencentes a mesma origem de produção. C-LOR: Relacionamento entre objetos conforme localização. C-WOR: Relacionamento entre objetos conforme trabalho. OOR: Relacionamento entre objetos conforme propriedade. SOR: Relacionamento social (ocasional) entre objetos.	Honestidade: parâmetro que representa quando um objeto é ou não honesto durante os eventos entre seus pares. Cooperação: avalia como o objeto é cooperativo com seus pares. Comunidade de interesse: representa as ocasiões em que os objetos pertencem às mesmas comunidades/grupos ou as mesmas características (localização, trabalho, origem, etc)	Estabilidade: parâmetro que representa a capacidade de troca de mensagens entre objetos durante seu tempo de conexão. Integridade: calcula a quantidade de mensagens descartadas durante a troca de serviços/mensagens Conectividade: estima a centralidade do objeto considerando o número médio de suas conexões durante o tempo
Modelo de cálculo de recomendações	A partir de modelos de probabilidade de ocorrência de eventos (modelo probabilístico)	A partir de modelos de probabilidade de ocorrência de eventos (modelo probabilístico)	A partir da ocorrência de eventos medidos pela troca de mensagens entre os objetos na rede (modelo determinístico)
Parâmetros de desempenho computacional e funções	Considera o tipo de dispositivo computacional, conforme 4 classes: Classe 1: dispositivos moveis com grande capacidade computacional e de comunicação (*smartphones*, computadores de bordo veiculares, *tablets*). Classe 2: dispositivos estáticos com significante capacidade computacional e de comunicação (*displays*, *setup boxes*, câmeras digitais).	Não há considerações a respeito desses parâmetros	Fator de relevância biomédica, conforme classificação internacional (*World Health Organization*), agrupados em 3 tipos conforme suas funções: Tipo 1: Dispositivos de monitoramento e suporte a vida Tipo 2: Dispositivos de rastreamento e identificação Tipo 3: Dispositivos de comunicação e informação

	Classe 3: dispositivos somente com capacidades de sensoriamento (sensores de ambiente) Classe 4: dispositivos RFID ou NFC	

Fonte: Autoria própria.

Na tabela foram reunidas as principais características mapeadas entre as propostas apresentadas em (Atzori et al, 2011; BAO et al, 2012). Os tipos de relacionamentos entre objetos propostos no primeiro trabalho são relacionados a comportamentos humanos, onde os objetos devem herdar características e estabelecer seus relacionamentos a partir delas. Em um cenário de rede IoMT deixa uma lacuna ao não tratar parâmetros de prioridade e relevância biomédica, os quais foram propostos no TMP visando contemplar essas necessidades.

O primeiro trabalho propõe ainda um modelo hibrido de armazenamento de informações, composto de agentes em rede, aplicações em servidores e uma tabela de referência de informações sobre reputação. É um modelo interessante que permite realizar outras analises como histórico de transações e atuar na camada de aplicação. É possível implementar esse modelo na proposta TMP, tornando-a mais robusta em trabalhos futuros.

Com relação à arquitetura do modelo de gestão de confiança, o primeiro modelo propôs arquitetura hibrida enquanto o segundo propôs arquitetura descentralizada. O TMP é uma proposta que utiliza descentralizada, podendo adotar arquitetura hibrida ou centralizada em novas implementações, conforme necessidades da aplicação.

Um diferencial importante do modelo TMP é a proposta de considerar parâmetros computacionais como fator de relevância na rede biomédica. O primeiro modelo considera classes genéricas de dispositivos como parâmetros, a partir de dispositivos moveis ou estáticos e capacidade de processamento de dados. O segundo modelo não avalia esses parâmetros, enquanto o modelo TMP propõe a adoção do fator de relevância biomédica em 3 tipos, conforme atuação dos dispositivos.

Há ainda a diferenciação na avaliação de índices de confiança, onde apenas o modelo TMP propõe índices determinísticos, minimizando consumo de energia e esforço

computacional para realização dos cálculos, por fazer uso de parâmetros já utilizados nas operações entre objetos (número de conexões, troca de mensagens).

4.4. CONCLUSÃO DO CAPÍTULO

No presente capítulo foi apresentada a proposta do Protocolo TMP para gestão de confiança em redes IoMT, sua notação e modelagem matemática, assim como uma análise a partir de dados inferidos para validação inicial da proposta. A análise preliminar demonstra resultados positivos sendo possível predefinir níveis de confiança a partir de níveis de proteção para os objetos da rede, favorecendo a interação entre os objetos, de modo particular os que possuem maior relevância na rede.

No próximo capítulo serão apresentados os resultados de simulações e análises detalhadas dos parâmetros utilizados para o cálculo de recomendações entre objetos assim como o comportamento da rede IoMT, levando em consideração diversos cenários e aplicações.

5. SIMULAÇÕES E RESULTADOS

A fim de avaliar a proposta, foram criados cinco cenários para avaliar o Protocolo TMP, a partir de parâmetros diferenciados. Para tanto, foi desenvolvida uma simulação própria utilizando a ferramenta Matlab, visando aplicar os conceitos e analisar o comportamento dos objetos da rede IoMT e o desempenho do Protocolo TMP em face a diversas situações.

Os objetos foram criados para iniciar os processos de relacionamentos sociais enviando solicitações de conexões uns para os outros, representando um ambiente biomédico, conforme apresentado na Figura 14.

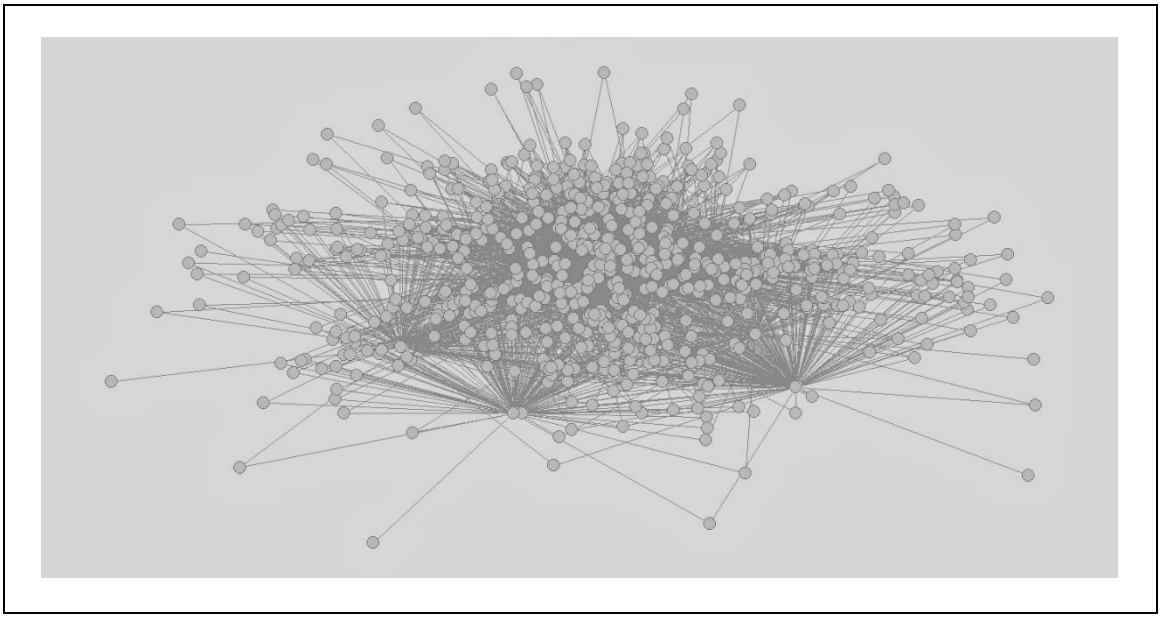

Figura 14. Distribuição espacial da rede IoMT para as simulações.

Fonte: Autoria própria.

Nestes cenários, os objetos podem interagir uns com os outros para estabelecer relacionamentos, visando troca de serviços e mensagens. Não estão sendo consideradas diferenças de protocolos de comunicação e nem padrões físicos e de aplicações.

As simulações foram executadas sobre uma base de eventos gerada para avaliação do protocolo TMP. Primeiramente foram gerados eventos de conexão, desconexão e trocas de mensagens seguindo parâmetros de conformidade (conexões e desconexões dentro de um

intervalo de tempo esperado e trocas de mensagens regulares e integras). Foram inseridos eventos aleatórios de desconexão súbita, conexão sem trocas de mensagens e troca de mensagens inválidas. A partir de então esses eventos foram gravados, observando o comportamento quanto à conectividade dos objetos e sua capacidade de trocar mensagens entre si.

Foram criadas duas rodadas de simulações para cada um dos 5 cenários, a primeira sem aplicação do protocolo TMP e a segunda aplicando-se o protocolo. No primeiro e segundo cenários, foram distribuídos objetos das 3 classes de dispositivos biomédicos conforme o fator de relevância. Tipo 1, dispositivos de comunicação e informação, tipo 2 dispositivos de rastreamento e identificação e tipo 3 dispositivos de monitoramento e suporte à vida. Foi aplicada distribuição uniforme considerando 90% de nível de proteção, ou seja, sensibilidade à identificação de objetos com comportamento suspeito na rede IoMT. O primeiro cenário foi criado com 100 objetos e o segundo com 1000, visando avaliar a o desempenho do protocolo TMP em face a uma rede considerada pequena para ambientes biomédicos, com 100 componentes, e outra considerada grande, composta por 1000 objetos.

Os cenários 3, 4 e 5 foram desenvolvidos para avaliar o comportamento do protocolo TMP em face a predominância de cada tipo de dispositivo na rede, conforme suas classes e fator de relevância. No cenário 3 foram distribuídos de forma uniforme objetos compostos 70% de objetos tipo 3, o cenário 4 foi composto por 70% de objetos tipo 2 e o cenário 5, composto por 70% de objetos tipo 1. A composição dos cenários com predominância de cada objeto foi definida para avaliar a importância da aplicação de gestão de confiança no estabelecimento de conexões entre objetos e na troca de mensagens entre eles.

O algoritmo do protocolo TMP foi descrito conforme apresentado a seguir:

```
1   If k need connect to i then
2       If R(k,i) ≥ 0
3           If  C(i) > 0
4               Connect k
5           Else
6               j = max D(i,j)
7               Disconnect j
8               Connect k
9           End if
10      End if
11  End if
```

Cenário 1: Rede IoMT pequena reproduzindo um ambiente biomédico heterogêneo, composto por objetos das três classes, conforme os seguintes parâmetros:

Quadro 1: Parâmetros para a simulação do cenário 1.

Número de objetos	100
Número de eventos	2.000
Distribuição	Heterogênea e aleatória
Tipos de dispositivos	Distribuição proporcional e uniforme das 3 classes
Nível de proteção	90%

Fonte: Autoria própria.

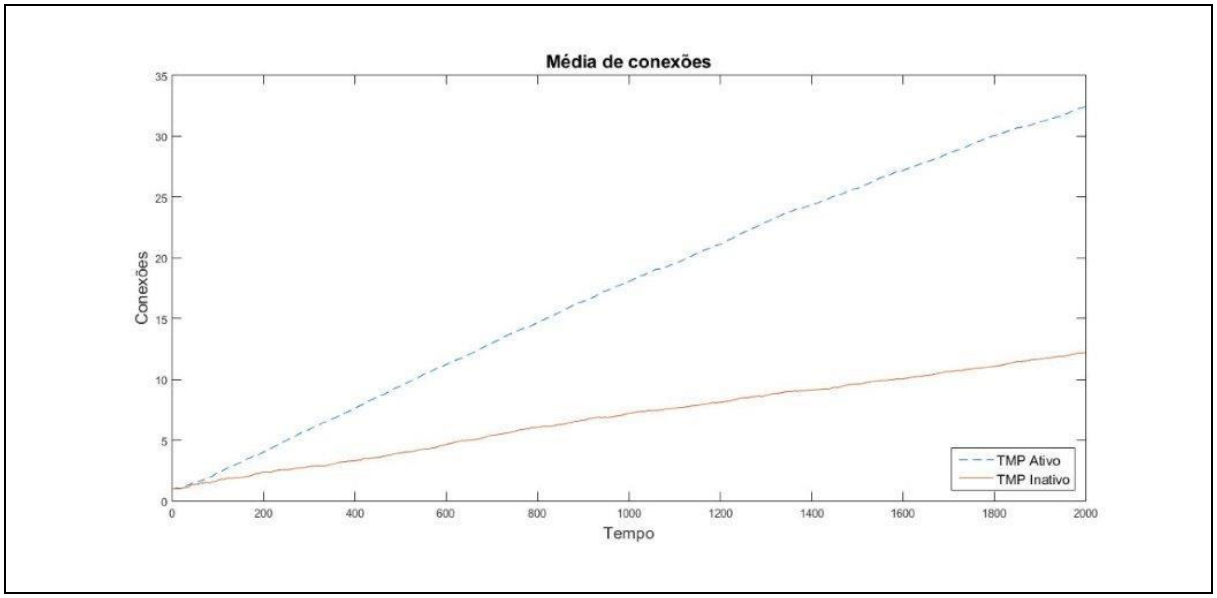

Figura 15: Média de conexões entre objetos em rede IoMT pequena.

Fonte: Autoria própria.

Nas figuras 15 e 16 pode-se verificar que média de conexões entre os objetos é proporcional a evolução das conexões, ambas alcançando taxas maiores quando o protocolo TMP está ativo. Isso demonstra o estabelecimento de conexões mais confiáveis entre os objetos, calculado a partir dos índices de estabilidade avaliados para compor as recomendações.

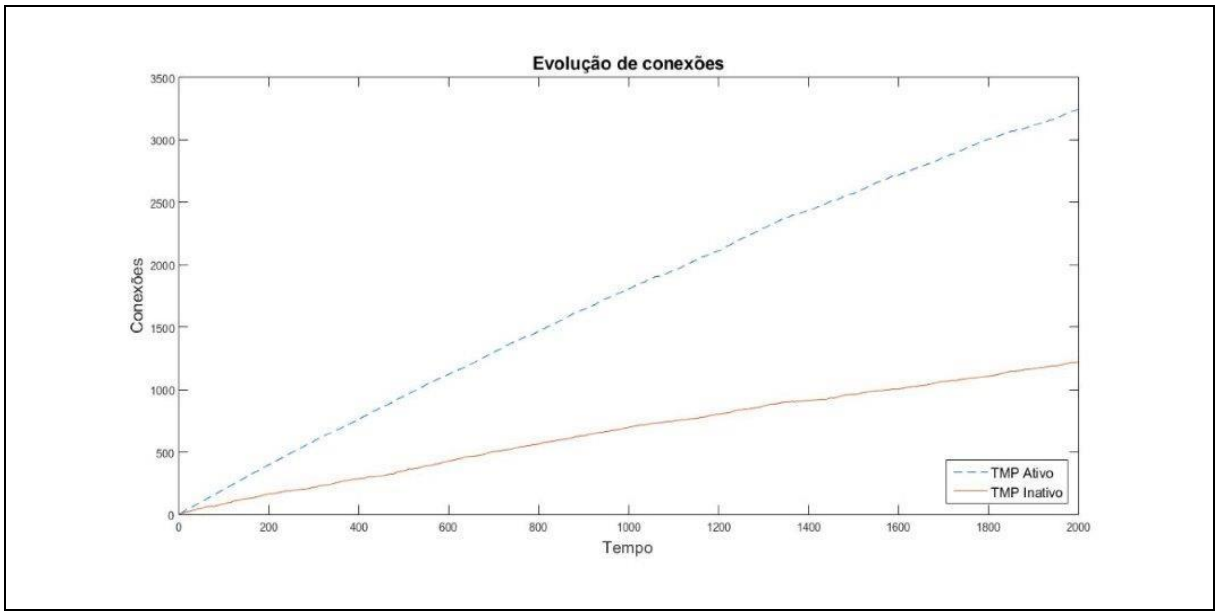

Figura 16: Evolução das conexões entre objetos em rede IoMT pequena.

Fonte: Autoria própria.

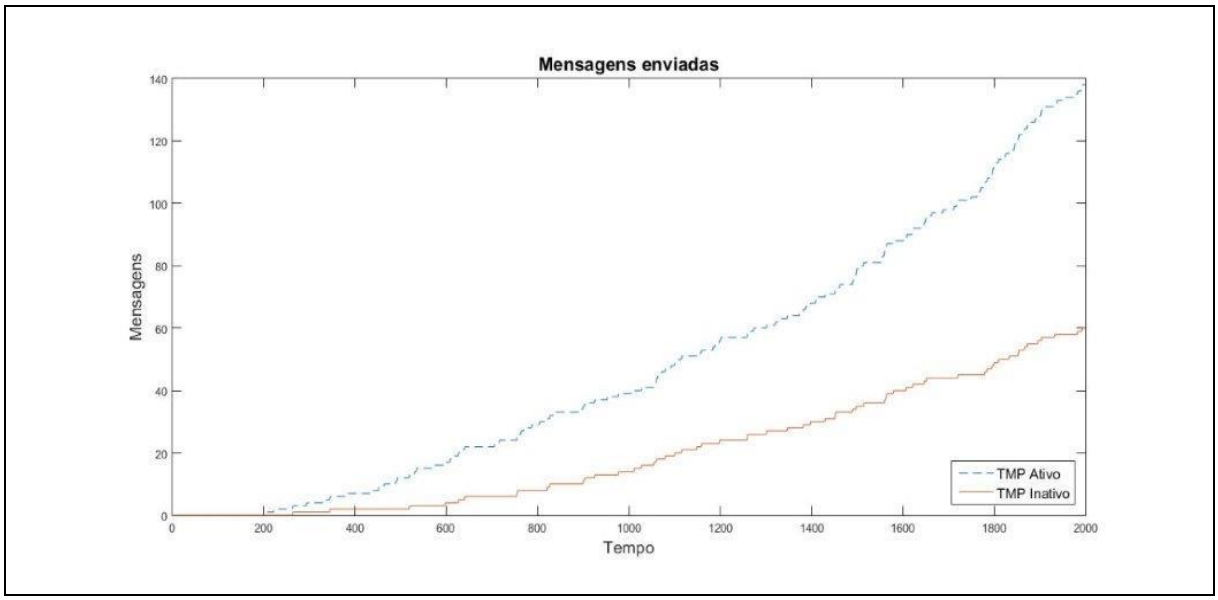

Figura 17: Troca de mensagens entre objetos em rede IoMT pequena.

Fonte: Autoria própria.

A Figura 17 apresenta a evolução da troca de mensagens entre os objetos na rede IoMT. Essa evolução corresponde ao índice de integridade, mostrando as mensagens trocadas ao longo do tempo. Supõe-se que na simulação de eventos onde o protocolo TMP não está ativo, pelo declínio da curva há um número razoável de mensagens descartadas, as quais são adotadas como comportamento suspeito no protocolo TMP. Assim, com a aplicação do protocolo de

confiança, a curva de trocas efetivas de mensagens é maior, caracterizando a utilidade do algoritmo ao evitar a troca de mensagens com objetos suspeitos.

Cenário 2: Rede IoMT grande reproduzindo um ambiente biomédico heterogêneo, composto por objetos das três classes, conforme os seguintes parâmetros:

Quadro 2: Parâmetros para a simulação do cenário 2.

Número de objetos	1.000
Número de eventos	10.000
Distribuição	Heterogênea e aleatória
Tipos de dispositivos	Distribuição proporcional e uniforme das 3 classes
Nível de proteção	90%

Fonte: Autoria própria.

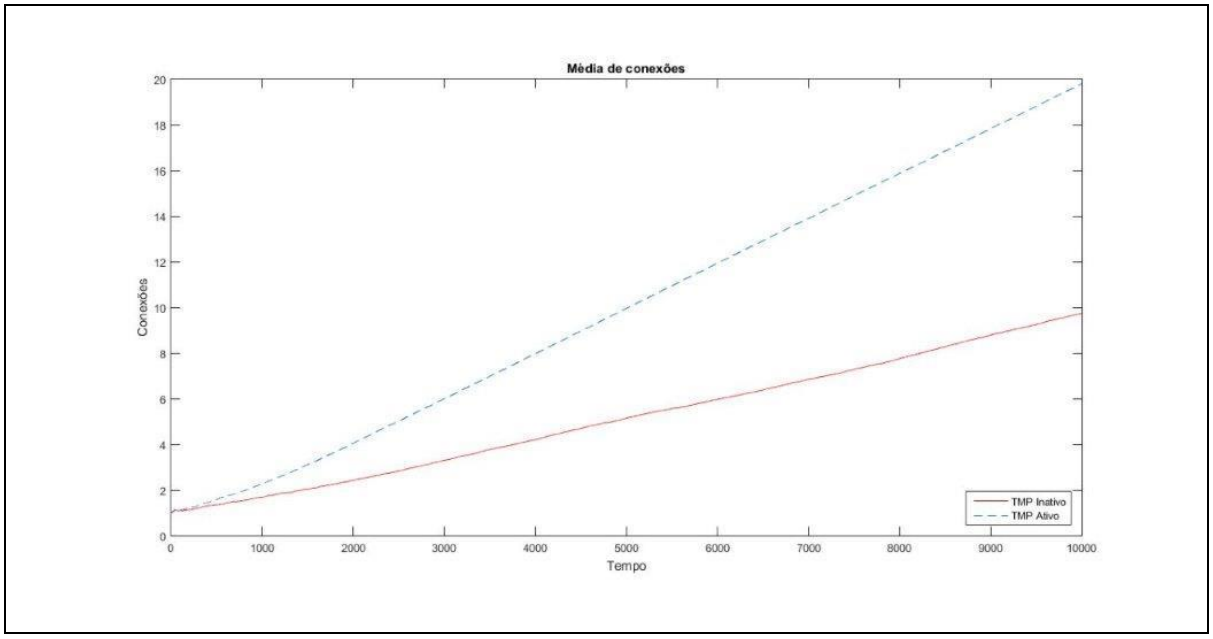

Figura 18: Média de conexões entre objetos em rede IoMT grande.

Fonte: Autoria própria.

As Figuras 18 e 19 seguem uma tendência bastante semelhante, onde a média de conexões entre os objetos é proporcional a evolução das conexões, padrão similar às Figuras 15 e 16. Em todos as curvas, observa-se que as taxas são maiores quando o protocolo TMP está ativo, seja para a rede pequena quanto para a rede grande, validando a eficácia do índice de estabilidade, utilizado para o cálculo das recomendações entre os objetos.

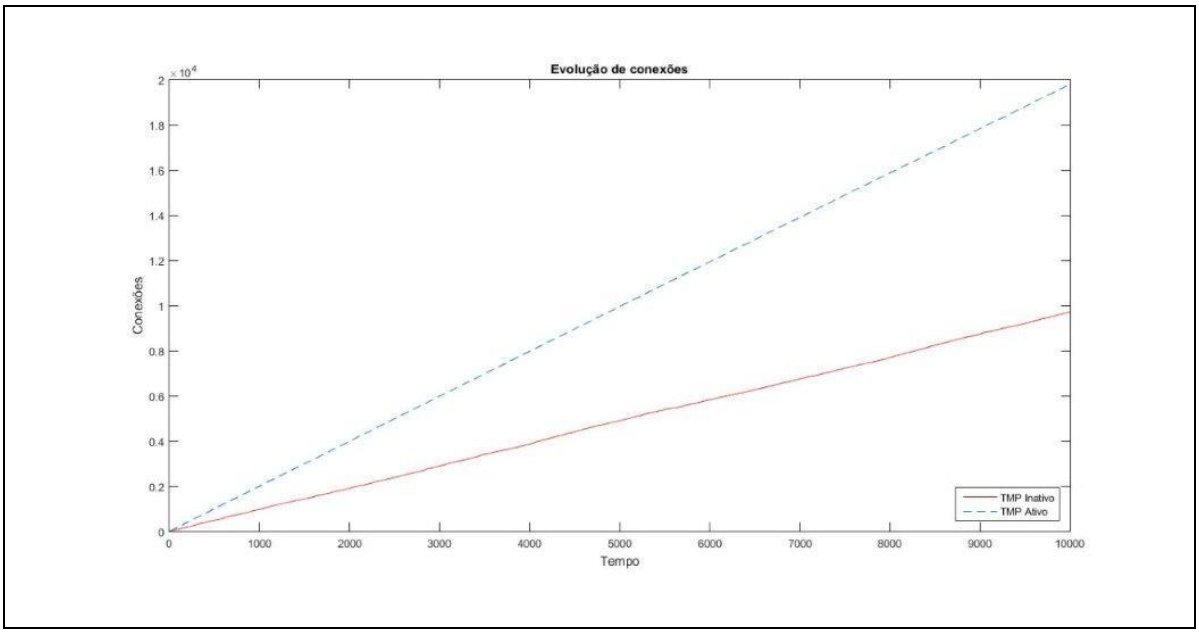

Figura 19: Evolução das conexões entre objetos em rede IoMT grande.

Fonte: Autoria própria.

A figura 20 demonstra as taxas de mensagens trocadas entre os objetos em uma rede IoMT composta por 1.000 objetos. Supõe-se que na rede grande e composta por objetos móveis, há uma variação maior na taxa de troca de mensagens do que apresentada na Figura 17, onde a rede é menor, mais estável e com menos entrada e saída de novos objetos. Observa-se também a melhora no desempenho de troca de mensagens quando o protocolo TMP está ativo.

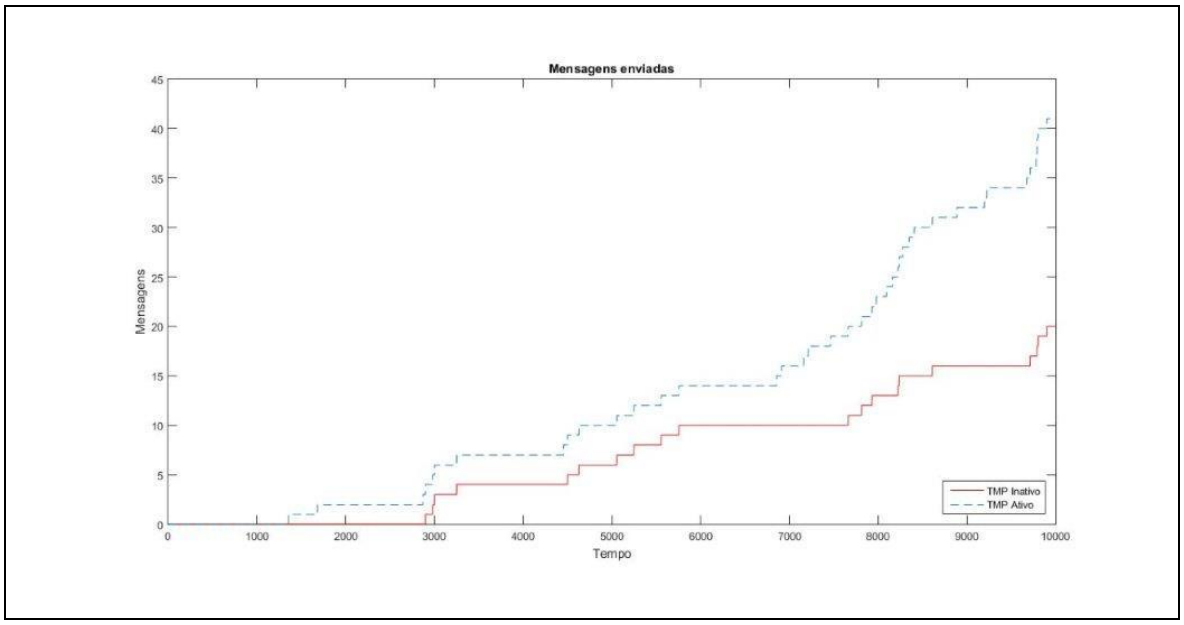

Figura 20: Troca de mensagens entre objetos em rede IoMT grande.

Fonte: Autoria própria.

Cenário 3: Rede IoMT composta por 70% de objetos da classe 3 (dispositivos de monitoramento e suporte à vida) em um ambiente biomédico conforme os seguintes parâmetros:

Quadro 3: Parâmetros para a simulação do cenário 3.

Número de objetos	100
Número de eventos	2.000
Distribuição	Heterogênea e aleatória
Tipos de dispositivos	Distribuição proporcional e uniforme composta de 70% de objetos tipo 3.
Nível de proteção	90%

Fonte: Autoria própria.

Neste cenário supõe-se uma rede IoMT com predominância de objetos classe 3. O objetivo dessa simulação foi verificar, por meio do nível de confiança definido com 90%, a

efetividade do protocolo TMP em face dessa classe de dispositivos, a qual é considerada a mais importante em uma rede IoMT.

As Figuras 21 e 22 mostram a média de conexões e evolução de conexões ao longo do tempo, em uma rede pequena composta por 100 objetos. Pode-se observar uma considerável diferença no desempenho das conexões entre as curvas que representam o funcionamento sem gestão de confiança nas curvas em vermelho (linha), e com a aplicação do protocolo TMP, em azul (pontilhada).

O desempenho apresentado utilizando o protocolo TMP é bastante superior e neste caso, muito importante por se tratar de uma rede com predominância de objetos da classe 3, os mais relevantes em redes IoMT.

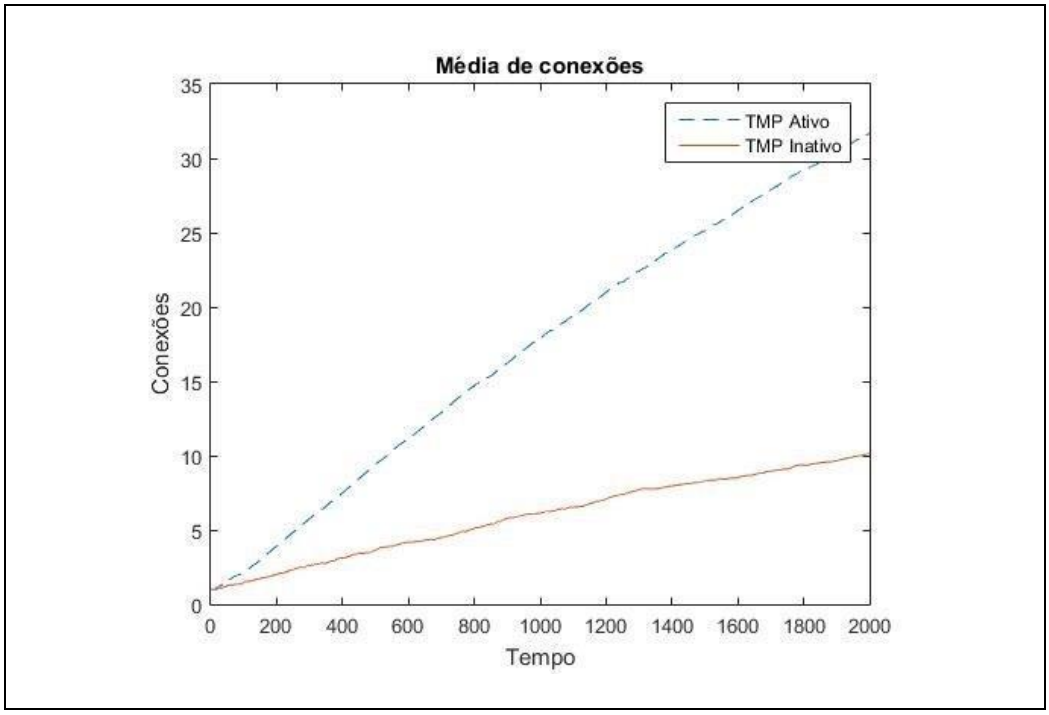

Figura 21: Média de conexões entre objetos em rede IoMT com predominância de dispositivos classe 3.

Fonte: Autoria própria.

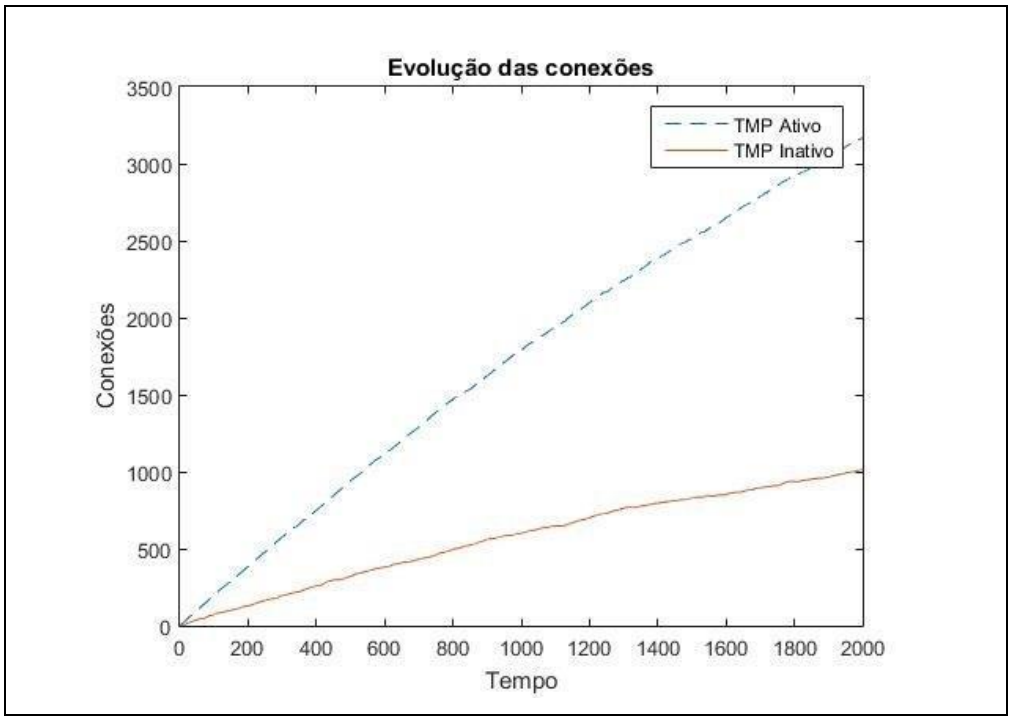

Figura 22: Evolução das conexões em rede IoMT com predominância de objetos da classe 3.

Fonte: Autoria própria.

A troca de mensagens também apresenta um desempenho bastante superior quando utilizado o protocolo TMP, conforme observado na Figura 23. Em ambientes com alta prioridade compostos por dispositivos de classe 3 com necessidade de disponibilidade de constante de informações, a aplicação do TMP pode ser bastante útil para melhorar a confiança entre os objetos, para que os mesmos possam efetuar conexões mais estáveis.

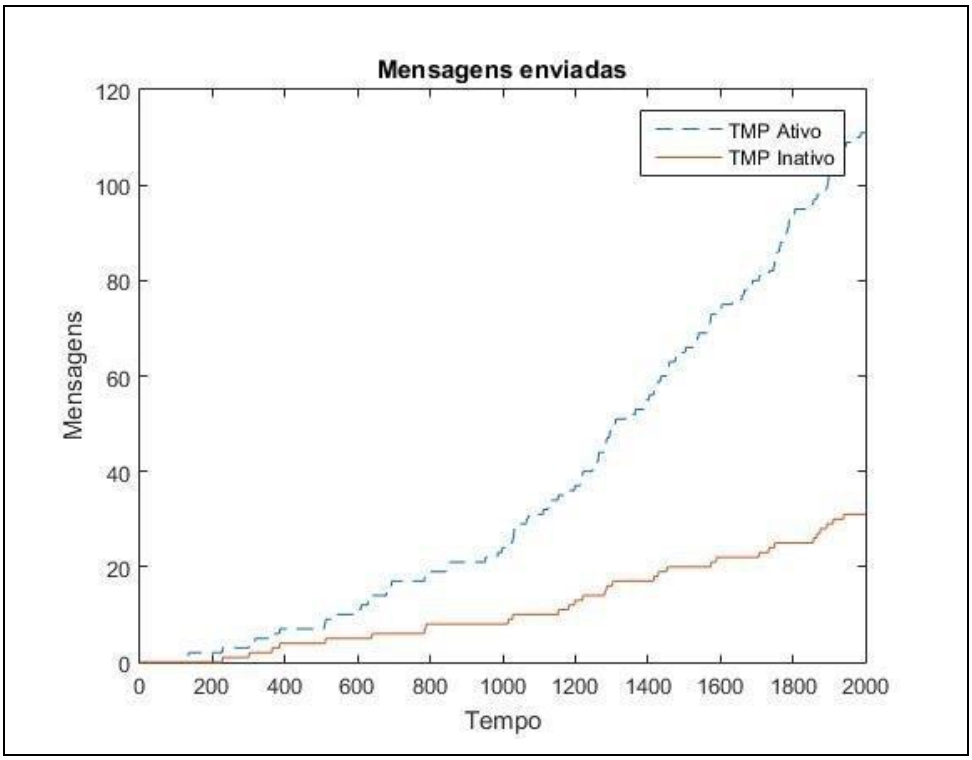

Figura 23: Troca de mensagens entre em rede IoMT com predominância de objetos da classe 3.

Fonte: Autoria própria.

Cenário 4: Rede IoMT composta por 70% de objetos da classe 2 (dispositivos de rastreabilidade e identificação) em um ambiente biomédico conforme os seguintes parâmetros:

Quadro 4: Parâmetros para a simulação do cenário 4.

Número de objetos	100
Número de eventos	2.000
Distribuição	Heterogênea e aleatória
Tipos de dispositivos	Distribuição proporcional e uniforme composta de 70% de objetos tipo 2.
Nível de proteção	90%

Fonte: Autoria própria.

Neste cenário supõe-se uma rede IoMT com predominância de objetos classe 2. O objetivo dessa simulação foi verificar, por meio do nível de confiança definido com 90%, a efetividade do protocolo TMP em face dessa classe de dispositivos, a qual possui relevância intermediaria em uma rede IoMT.

As Figuras 24 e 25 demonstram que a média e a evolução de conexões ao longo do tempo apresentam a mesma tendência. Pode-se observar diferença no desempenho da rede quando comparadas as curvas com a aplicação do TMP e sem nenhum protocolo de confiança.

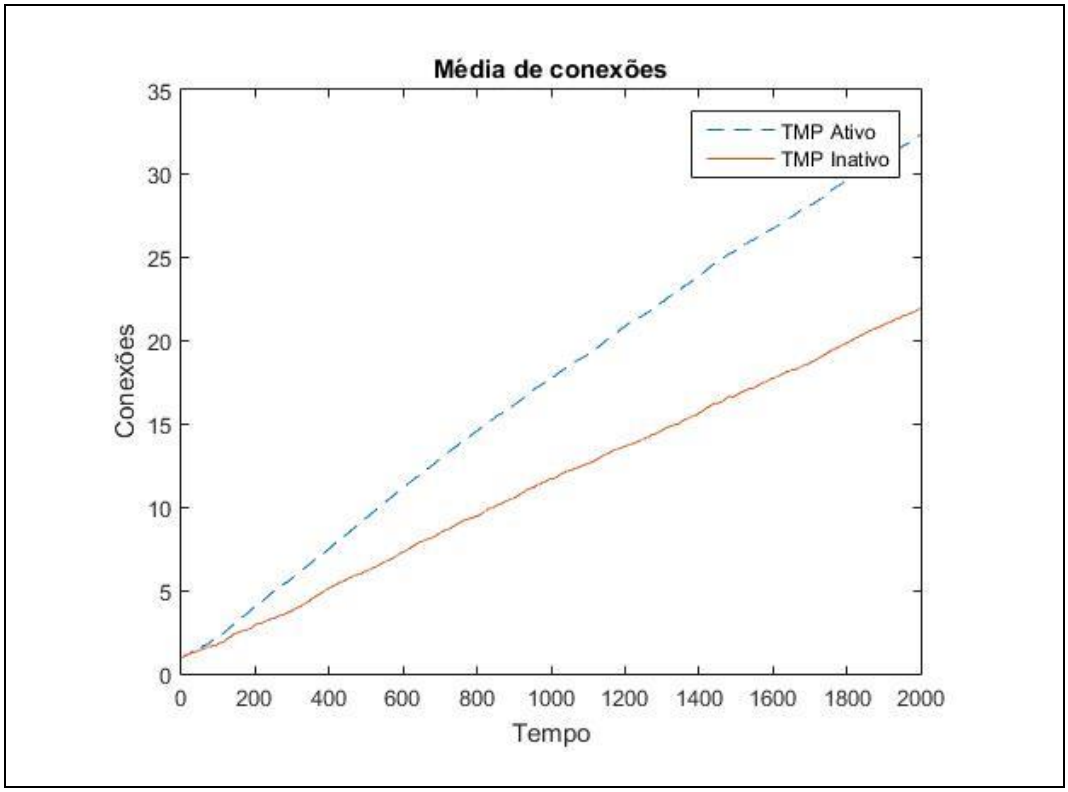

Figura 24: Média de conexões entre objetos em rede IoMT com predominância de dispositivos classe 2.

Fonte: Autoria própria.

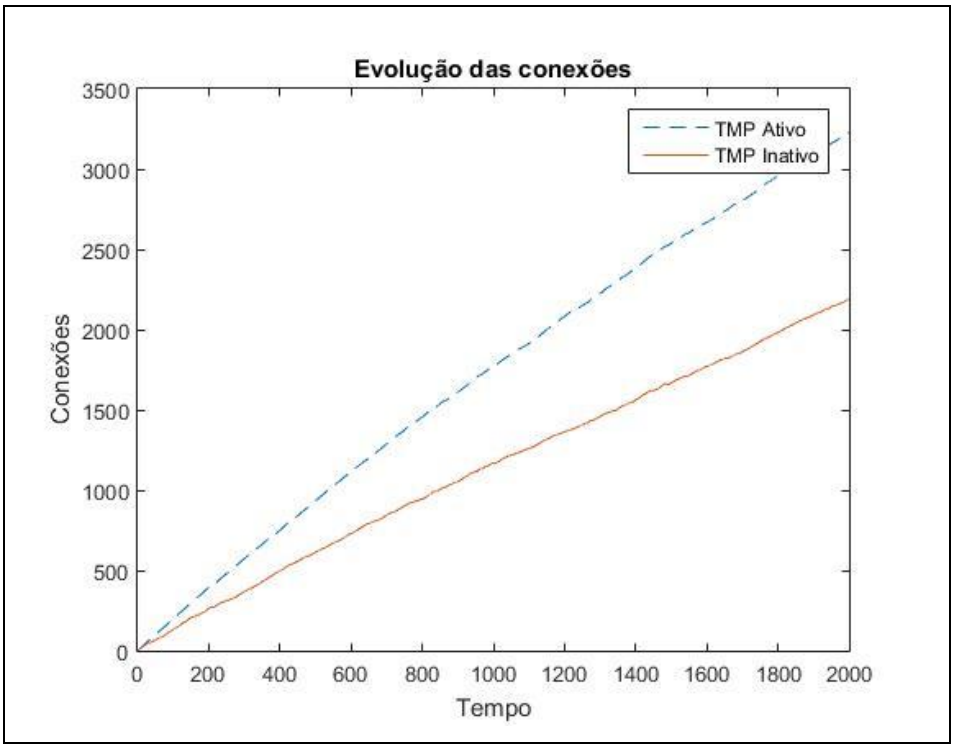

Figura 25: Evolução das conexões em rede IoMT com predominância de objetos da classe 2.

Fonte: Autoria própria.

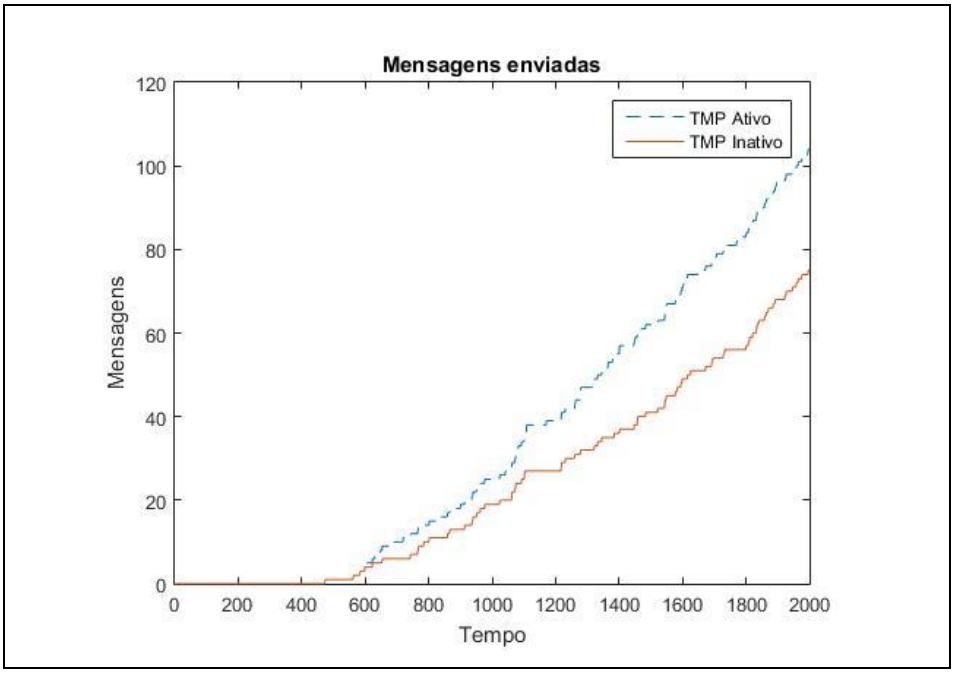

Figura 26: Troca de mensagens entre objetos em rede IoMT com predominância de objetos da classe 2.

Fonte: Autoria própria.

Na Figura 26 pode-se verificar que as trocas de mensagens entre os dispositivos desta classe apresentam melhor desempenho quando da utilização do protocolo TMP.

Cenário 5: Rede IoMT composta por 70% de objetos da classe 1 (dispositivos de informação e comunicação) em um ambiente biomédico conforme os seguintes parâmetros:

Quadro 5: Parâmetros para a simulação do cenário 5.

Número de objetos	100
Número de eventos	2.000
Distribuição	Heterogênea e aleatória
Tipos de dispositivos	Distribuição proporcional e uniforme composta de 70% de objetos tipo 1.
Nível de proteção	90%

Fonte: Autoria própria.

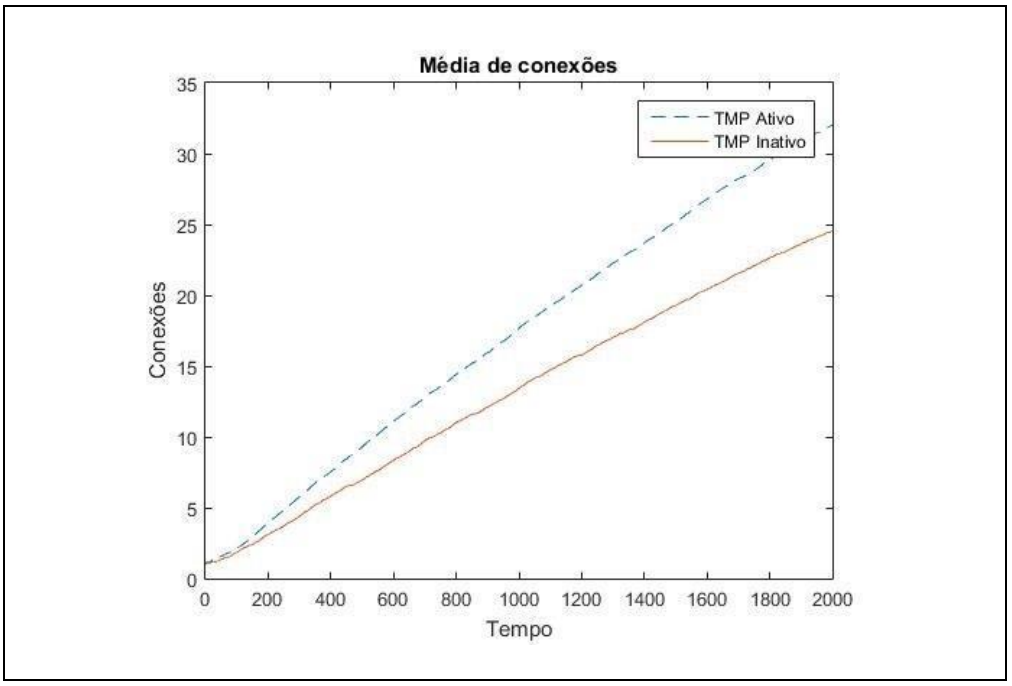

Figura 27: Média de conexões entre objetos em rede IoMT com predominância de dispositivos classe 1.

Fonte: Autoria própria.

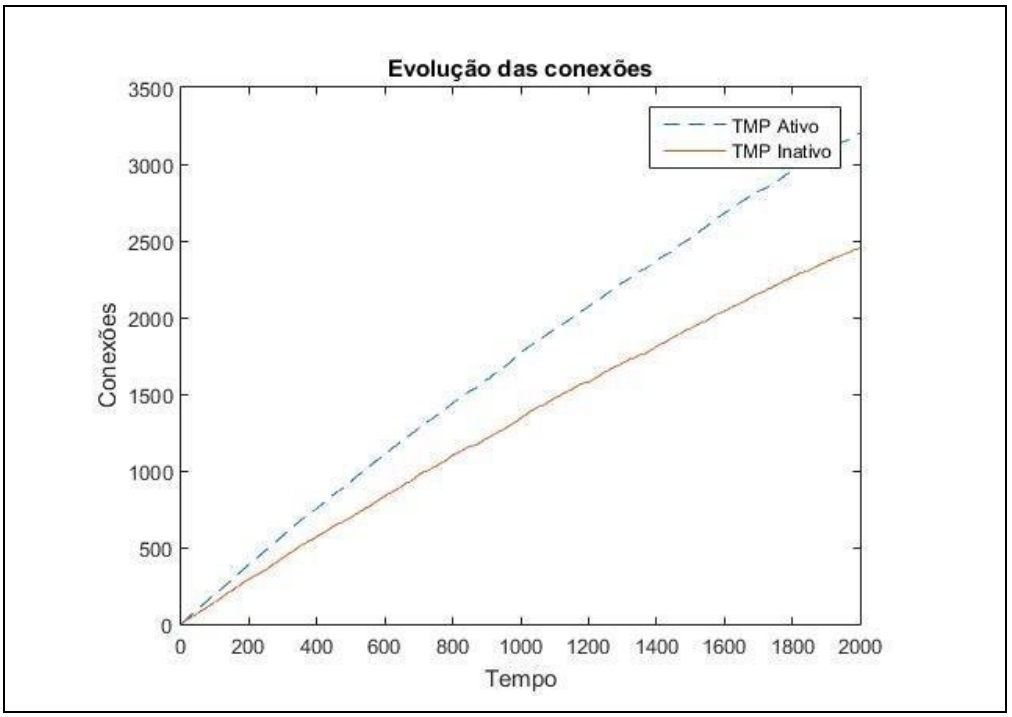

Figura 28: Evolução das conexões em rede IoMT com predominância de objetos da classe 1.

Fonte: Autoria própria.

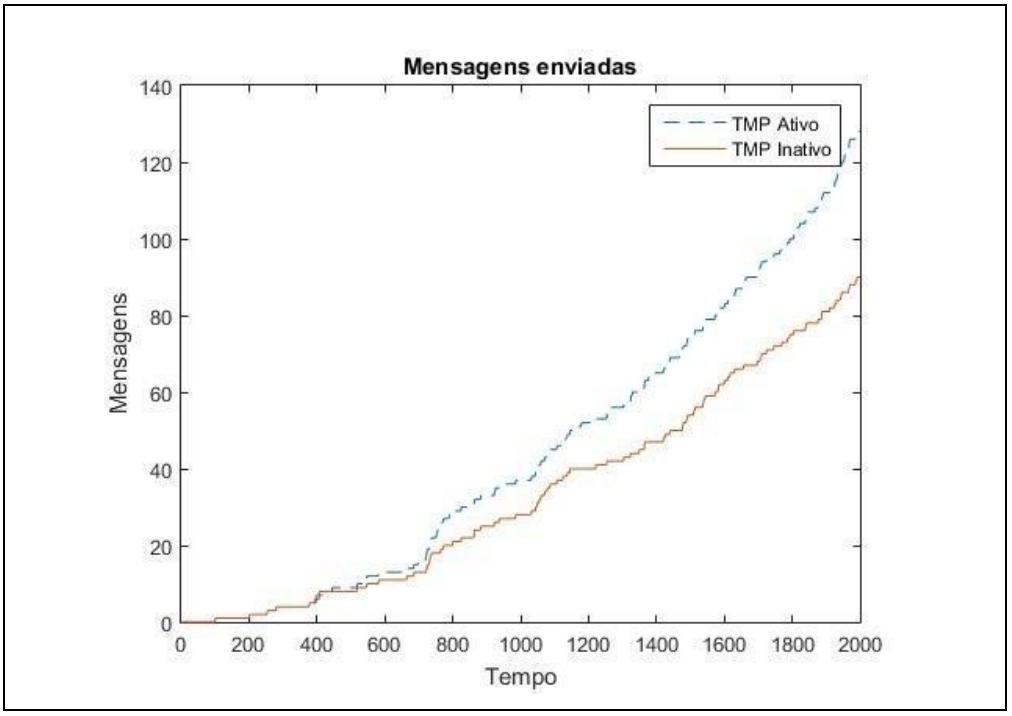

Figura 29: Troca de mensagens entre objetos em rede IoMT com predominância de objetos da classe 1.

Fonte: Autoria própria.

Nas figuras 27 e 28 observa-se novamente a atuação do protocolo TMP durante o estabelecimento de conexões entre objetos e sua evolução. Percebe-se a melhora no desempenho da rede IoMT quando o protocolo é utilizado, conforme visualizado nas curvas em azul.

Na Figura 29 é apresentada a avaliação de desempenho das trocas de mensagens entre os objetos. Novamente o protocolo TMP apresenta resultados melhores comparados a simulação representada pela curva em vermelho, onde não existe protocolo de confiança aplicado.

5.1. CONCLUSÃO DO CAPÍTULO

As propostas e resultados preliminares apresentados neste capítulo compõe os objetivos propostos para serem alcançados nesta etapa da pesquisa. A viabilidade de aplicação do modelo proposto foi investigada, apresentando resultados satisfatórios condizentes com sua proposta inicial.

É possível observar que seu melhor desempenho é apresentado no cenário 3 que é composto predominantemente por objetos da classe 3, os quais possuem maior relevância biomédica por se tratarem de dispositivos de monitoramento e suporte à vida. Essa relação é coerente com a proposta TMP que visa priorizar os objetos com mais relevância para sua área de aplicação, sendo portanto, um protocolo com parâmetros focados em redes IoMT.

No próximo capítulo serão apresentadas as discussões relacionando os resultados encontrados com os trabalhos pesquisados para o desenvolvimento da proposta TMP, assim como os direcionamentos para a sequência de atividades futuras.

6. DISCUSSÃO E CONCLUSÕES

6.1. DISCUSSÃO

Com a análise dos resultados assume-se ser possível identificar comportamentos suspeitos conforme as interações entre os objetos durante a troca de mensagens e serviços, colaborando para minimizar prejuízos na rede IoMT.

Outras abordagens têm sido utilizadas em propostas de gestão de confiança tomando como base conceitos de relacionamentos sociais (ATZORI et al.,2012; CHEN et al., 2015). Na proposta TMP, aplicou-se a teoria de redes sociais para avaliar a centralidade dos objetos, calculando de forma determinística o número médio de conexões entre os objetos, sua taxa de troca de mensagens e padrões de conexão e desconexão, utilizando índices de estabilidade, integridade e conectividade.

Em (ATZORI et al.,2012) os autores propuseram um modelo probabilístico generalista para dispositivos pessoais baseado em parâmetros como localização, propriedade, parentesco, forma de trabalho e encontros ocasionais, com avaliação via simulações criadas a partir de dados sobre mobilidade humana. Em (CHEN et al., 2015) também foram propostos algoritmos probabilísticos para gestão de confiança em redes dinâmicas genéricas, considerando aspectos como honestidade, cooperação e comunidade de interesse, com validações realizadas por meio de análises matemáticas utilizando um modelo de cadeia Semi-Markoviana.

Essas abordagens utilizaram modelos probabilísticos, o modelo proposto para o TMP é determinístico, calculado a partir dos índices de estabilidade, integridade e conectividade para alcançar os resultados, os quais se baseiam em parâmetros já utilizados nas operações entre os objetos, minimizando assim o consumo de energia para novos cálculos assim como a capacidade computacional dos objetos.

A proposta apresentada em (ATZORI et al.,2012) considera parâmetros computacionais conforme 4 classes: dispositivos móveis com grande capacidade computacional, dispositivos estáticos com significante capacidade computacional, dispositivos somente com capacidade de sensoriamento e dispositivos RFID ou NFC. Esse modelo foi projetado para atuar na camada de aplicação, utilizando um servidor, gateways e agentes. Em (CHEN et al., 2015) não foram

considerados parâmetros relacionados a capacidade computacional e o modelo proposto foi projetado para atuar na camada de rede distribuído entre os objetos.

O modelo TMP propõe o fator de relevância biomédica com foco no gerenciamento de confiança entre relacionamentos para redes IoMT, composto por 3 tipos: dispositivos de monitoramento e suporte à vida, dispositivos de rastreabilidade e identificação e dispositivos de comunicação e informação. É possível ainda ser ajustado para a camada de aplicação e camada de rede, com processamento distribuído entre os objetos.

Nos gráficos que apresentam as análises de desempenho, pode-se observar a importância do fator de relevância biomédica proposto no protocolo TMP. Diferente dos outros protocolos, propõe-se avaliar o nível de proteção necessário para identificar comportamentos suspeitos de objetos na rede, assim como programar níveis de tolerância dessas ocorrências, de acordo com o tipo e função do dispositivo na rede IoMT. Por exemplo, se a predominância dos objetos é de monitoramento e suporte a vida (tipo 3), pode-se aumentar o nível de proteção pois esse tipo de objeto possui mais relevância no contexto de IoMT. Assim, pode-se configurar níveis de proteção para determinadas áreas ou setores dentro de ambientes biomédicos, conforme a predominância dos dispositivos. Áreas com predominância de dispositivos de monitoramento e suporte à vida podem ter proteção maior, em torno de 90%, outras com maior número de dispositivos de comunicação e informação podem ter 50% de proteção.

O protocolo TMP também contribui para o gerenciamento e manutenção dos relacionamentos entre objetos, mesmo quando objetos com comportamento duvidoso se apresentam na rede IoMT. Diferente das outras propostas apresentadas, calcula os índices para obter resultados objetivos, a partir de eventos que podem ser computados na rede IoMT. Isso minimiza o consumo computacional e de energia dos objetos, os quais geralmente possuem limitação desses recursos. Desta forma é possível evitar prejuízos nas trocas de serviços entre os objetos e melhorar a distribuição das conexões, com particular importância em ambientes com redes IoMT compostos por objetos com trocas de serviços que não podem parar.

A evolução das curvas nos gráficos apresentados apresenta o mesmo padrão, demonstrando que os parâmetros computados contribuem para indicar comportamentos suspeitos dos objetos durante sua atividade na rede IoMT. Essa identificação se torna mais apurada conforme se aumenta o nível de proteção da rede, conforme observado nas Figuras 11-13 das análises matemáticas.

Pode-se inferir a partir dos dados obtidos na análise matemática e simulações de cenários que o protocolo TMP apresenta contribuições para o gerenciamento das redes IoMT, permitindo predefinir o nível de proteção conforme os tipos de objetos que realizam troca de serviços. Isso pode ser observado na análise matemática relacionada ao nível de proteção em cada uma das classes de objetos, de acordo com sua função na rede. Quanto mais relevante a função do objeto, mais rapidamente comportamentos suspeitos são identificados, conforme análise dos cenários simulados e diferentes níveis de proteção (60%, 80% e 90%).

Realizar troca de serviços em um ambiente composto por objetos confiáveis é um desafio em redes IoMT. Neste trabalho foi apresentada a proposta do protocolo TMP visando mitigar essa lacuna, melhorando o estabelecimento de conexões confiáveis entre os objetos a partir do comportamento relacionado a estabilidade, integridade e conectividade, gerando recomendações.

É uma contribuição para o desenvolvimento de ambientes, plataformas e aplicações mais seguras e confiáveis para pacientes e profissionais, assim como para a criação de uma nova geração de objetos autônomos, os quais representam a evolução da tecnologia como a conhecemos.

6.2. CONTRIBUIÇÕES E TRABALHOS FUTUROS

A principal contribuição deste trabalho é o protocolo TMP para melhorar a gestão de confiança em redes IoMT. Os resultados obtidos com esta proposta são considerados importantes para o desenvolvimento de aplicações IoMT em ambientes hospitalares, assim como vida assistida e monitoramento usando tecnologias vestíveis.

Todos os objetos que compõem essas aplicações precisam trocar serviços entre si e dependem de protocolos baseados em confiança para garantir o estabelecimento de conexões seguras. No futuro próximo, todos estes objetos terão mais autonomia e possivelmente não precisarão de intervenção humana executar suas ações.

Os objetivos iniciais desta pesquisa foram alcançados, além da proposta TMP e sua avaliação também foi realizado o mapeamento e comparação entre principais modelos de protocolos de gestão de confiança baseados em conceitos sociais para IoT encontrados no horizonte desta pesquisa.

Por se tratar de um tema bastante recente, existem ainda poucos estudos de gestão de confiança específicos para o paradigma IoT, em especial no que se refere especificamente ao contexto de IoMT. Diante desse cenário, houveram diversas dificuldades relacionadas a escolha de trabalhos relevantes ao tema e comparação com modelos similares assim como na escolha de ferramentas para avaliação do protocolo por meio de simulação.

Pretende-se dar prosseguimento ao trabalho de pesquisa utilizando ferramentas de simulação especificas para IoT para investigar novos cenários com o protocolo TMP, realizando adaptações necessárias para ambientes IoMT com novas contribuições.

O modelo proposto possui limitações que deverão ser implementadas em novos trabalhos, para evolução do modelo. Deverão ser desenvolvidos métodos para avaliação de histórico de comportamento dos objetos para evitar que objetos confiáveis com problemas de hardware ou comunicação sejam marcados como suspeitos, além de mecanismos de recompensa e punição conforme comportamento e atuação entre objetos.

Estudos futuros devem ainda contemplar outros aspectos a serem cobertos pelo protocolo TMP, tais como: (i) propor uma extensão do protocolo TMP para detectar a presença de objetos na rede IoMT e evitar novas conexões utilizando modelos de aprendizagem de máquina; (ii) desenvolver outra versão do protocolo para aumentar a resiliência da rede IoMT, utilizando uma tabela local com registros sobre recomendações entre objetos com arquitetura centralizada.

Deverá ainda ser criado um grupo de pesquisa sobre IoMT para vincular os próximos trabalhos, desenvolvendo novas contribuições acadêmicas e possivelmente, introduzindo em aplicações para o mercado.

REFERÊNCIAS BIBLIOGRÁFICAS

ADAR, E., HUBERMAN, B. A., **Free riding on gnutella**, 2000.

AKYILDIZ, I.F., CAYIRCI, E. SANKARASUBRAMANIAM, Y, SU, W.: **Wireless sensor networks: A survey.** Computer Networks, 38:393–422, March 2002.

AMARAL, L. A. N., OTTINO, J. M., **Complex networks. augmenting the framework for the study of complex systems**, European Physical Journal B, vol. 38, pp. 147–162, March 2004.

ANURAG, G., BATTITI, R., CASCELLA, R., MONTRESOR, A., BRUNATO, M., **BIONETS**, WP 4 - SECURITY, D4.1 Trust and Reputation Management System Definition, June 18, 2007

ATZORI, L., IERA, A., MORABITO, G., **The Internet of Things: A survey. Computer Networks**, Vol. 54. No 15, Oct. 2010a, p. 2787-2805.

ATZORI, L., IERA, A., MORABITO, G., **From "Smart Objects" to "Social Objects": The Next Evolutionary Step of the Internet of Things**, Vol. 54. No 15, Oct. 2010b, p. 2787-2805.

ATZORI, L. IERA, A., MORABITO, G., **Siot: Giving a social structure to the internet of things**, Communications Letters, IEEE, vol. 15, 2011.

ATZORI, L., IERA, A., MORABITO, G., **The Social Internet of Things – (SIoT) – When Social Networks Meet the Internet of Things: Concept, Architecture and Network Characterization**, Computer Networks, 2012, Vol. 56, no 16.

BAO, F., CHEN, I-R., CHANG, M., CHO, J-H., Hierarchical trust management for wireless sensor networks and its application to trust-based routing, in ACM Symposium on Applied Computing, 2011.

BAO, F., CHEN, I-R., **Trust management for the internet of things and its application to service composition**, in World of wireless, Mobile and Multimedia Networks (WoW-MoM), 2012 IEEE International Symposium, 2012, p. 1-6.

BLEECKER, J., **A manifesto for networked objects – cohabiting with pigeons, arphids and aibos in the internet of things – why things matter what' s a blogject ? what about spimes?** in Proc. of the 13th International Conference on Human-Computer Interaction with Mobile Devices and Services, MobileHCI, 2006.

BOGU, M., KRIOUKOV, D., CLAFFY, K., **Navigability of Complex Networks**, Nature Physics, vol. 5, no. 1, pp. 74–80, Jan 2009.

BRITTES, M.P., SCHNEIDER, B.J., **A Collaborative Approach to Manage and Share Elderly Biomedical Information,** XXIV Brazilian Congress on Biomedical Engineering – CBEB, 2014.

BROLL, G., **Perci: pervasive with the internet of things**, IEEE Internet Computing, vol. 13, pp. 74-81, Dec. 2009.

CARMINATI, B., FERRARI, E., GIRARDI, J., **Trust and share: Trusted information sharing in online social networks**. in ICDE. IEEE Computer Society, 2012a, pp. 1281–1284.

CARMINATI, B., FERRARI, E., VIVIANI, M., **A multi-dimensional and event-based model for trust computation in the social web**, in Social Informatics. Springer, 2012b, pp. 323–336.

CASAGRAS: Coordination and Support Action for Global RFID-related Activities and Standardization, **RFID and the Inclusive Model for the Internet of Things**, CASAGRAS Final Report, 2009.

CHEN, D., CHANG, D., SUN, J., LI, J., JIA, J., WANG, X., **TRM-IOT: A trust management model based on fuzzy reputation for internet of things**. Computer Science Inf, Syst, 2011, Vol. 8, no 4, p. 1207-1228.

CHEN, I-R., BAO, F., GUO, J., **Trust-based service management for social internet of things.** IEEE Transactions on dependable and secure computing, DOI 10.1109/TDSC.2015.2420552, 2015.

CHO, J. H., SWAMI, A., CHEN, R. A survey on trust management for mobile ad hoc networks. Communications Surveys & Tutorials, IEEE, 2011, 13(4), 562-583.

CHRISTIANSON, B., HARBISON, W. S., **Why isn't trust transitive** in Proceedings of the International Workshop on Security Protocols. Springer-Verlag, 1997, pp. 171–176.

COLESCA, C. E., DOBRICA, L., **The *e-Health* concept**. Management, vol 12, n 1, 2009.

COMISSION OF THE EUROPEAN COMMUNITIES, **Internet of things – an Action Plan for Europe**, Brussels, Jun. 18, 2009

CONTI, J.P. **THE INTERNET OF THINGS,** COMMUN.ENGINEER**.** VOL. 4,PP.20-25,2006

DING, L., SHI, P., LIU, B., **The clustering of internet, internet of things and social network**, in Proc. of the 3rd International Symposium on Knowledge Acquisition and Modeling, 2010.

DUBOIS, T., GOLBECK, J., SRINIVASAN, A., **Predicting trust and distrust in social networks**, in Privacy, security, risk and trust, 2011 IEEE third international confer-ence on and 2011 ieee third international conference on social computing (socialcom). IEEE, 2011, pp. 418–424.

EPCGLOBAL, **The EPCglobal Architecture Framework** (final version 1.3, 2009).

EPOSS: INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems Groups in co-operation with the RFID working Group, **Internet of Things in 2020,** 2008.

FAST, A., JENSEN, D., LEVINE, B. N., **Creating social networks to improve peer-to-peer networking**, in *Proc. of ACM KDD'05*, August 2005.

FELDMAN, M., LAI, K., CHUANG, J., **Quantifying disincentives in peer-to-peer networks**, in 1st Workshop on Economics of Peer-to-Peer Systems. 2000.

FINISH STATEGIC CENTER FOR SCIENCE AND INNOVATION: For information and communications (ICT) services, businesses, and technologies – internet of things strategic research agenda (IoT–SRA), September 2011

FISKE, A. P, **The four elementary forms of sociality: framework for a unified theory of social relations**, Psychological review, vol. 99, pp. 689–723, 1992.

FONG, P. W., **Relationship-based access control: protection model and policy language**, in Proceedings of the first ACM conference on Data and application security and privacy. ACM, 2011, pp. 191–202.

GAMBETTA, D., **Can We Trust Trust?**, in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, chapter 13, pp. 213-237, 2000.

GOLBECK, J. A., **Computing and applying trust in web-based social networks**, Ph.D. dissertation, 2005.

GOLBECK, J., HENDLER, J., **Inferring binary trust relationships in web-based social net-works**, ACM Trans. Internet Technol., vol. 6, no. 4, pp. 497–529, Nov. 2005

GUIMERÁ, R., DANON, L., DIÁZ-GUILERA, A., GIRALT, F., ARENAS, A., **Self-similar community structure in a network of human interactions**, 2003.

GUINARD, D., FISCHER, M., TRIFA, V., **Sharing using social networks in a composable web of things**, in PERCOM Workshops, 2010.

HASLAM, N., **The four elementary forms of sociality: framework for a unified theory of social relations**, Cognition, vol. 53, pp. 59–90, 1994.

HOLMQUIST, L. E., MATTERN, F., SCHIELE, B., ALAHUHTA, P., BEIGL, M., GELLERSEN, H.-W., **Smart-its friends: A technique for users to easily establish connections between smart artefacts**, in *Proceedings of the 3rd international conference on Ubiquitous Computing*, ser. UbiComp ’01. Springer-Verlag, 2001, pp. 116–122.

HUANG, Y. M., HSIEH, M. Y., CHAO, H.C., HUNG S.H., PARK J.H., **Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks**, IEEE Journal on Selected Areas in Communications, vol. 27, pp. 400-411, 2009.

ISTEPANIAN, R. S. H, PHILIP, N. Y., SUNGOOR, A., HU, S., **The potential of Internet of m-health Things m-IoT for non-invasive glucose level sensing**. In. Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2011, p.5264-5266. doi: http://dx.doi.org/10.1109/IEMBS.2011.6091302.

ITU, "The Internet of things," **ITU International Reports**, 2005.

JAMSHIDI, M., **From large scale systems to cyber-physical systems**, Journal of Internet Technology, vol. 12, no. 3, pp. 367-374, 2011.

JARA, A. J. ZAMORA, M. A., SKARMETA A. F. G., **An ambient assisted living system for telemedicine with detection of symptoms.** Third International Work-Conference on the Interplay Between Natural and Artificial Computation. Lecture notes, 2009, pp. 75-84.

JARA, A. J. ZAMORA, M. A., SKARMETA A. F. G., **An architecture based on internet of things to support mobility and security in medical environments**. IEEE CCNC 2010 proceedings, in press.

JIAN, A., XIAOLIN, G., WENDONG, Z., JINHUA, J., **Nodes social relations cognition for mobility-aware in the internet of things**, in Proc. of the 4th International Conference on Cyber, Physical and Social Computing, October 2011.

JIAN, A., XIAO-LIN, G., JIAN-WEI, Y., WEN-DONG, Z., JIN-HUA, J., **Research on a Mobile-Aware service model in the Internet of Things**, KSII Transaction on Internet and Information Systems, 2013, Vol. 7 no 5.

JOSANG, A., **Artificial reasoning with subjective logic**, in Proceedings of the Second Australian Workshop on Commonsense Reasoning, 1997.

JOSANG, A., POPE, S., **Semantic constraints for trust transitivity**, in Proceedings of the 2nd Asia-Pacific conference on Conceptual modelling. Australian Computer Society, Inc., 2005, pp. 59–68.

JOSANG, A., HAYWARD, R., POPE, S., **Trust network analysis with subjective logic**, in Proceedings of the 29th Australasian Computer Science Conference. Australian Computer Society, 2006, pp. 85–94.

JOSANG, A., IMAIL, R., BOYD, C. A., **A survey of trust and reputation systems for online service provision**. Decision Support Systems 43(2): pp 618-644, 2007.

JURCA, R., FALTINGS, B., **An incentive compatible reputation mechanism**, in Proceedings of the second international joint conference on Autonomous agents and multiagent systems. ACM, pp. 1026–1027. 2000.

KAMVAR, S. D., SCHLOSSER, M. T., GARCIA-MOLINA, H., **The eigentrust algorithm for reputation management in p2p networks**, in Proceedings of the 12th international conference on World Wide Web. ACM, 2003, pp. 640–651.

KIM, J., VALDEZ-RAMIREZ, G., BANDODKAR, A. J., JIA, W., MARTINEZ, A., RAMIREZ, J., MERCIER, P., WANG, J., b **Non-invasive Mouthguard Biosensor for Continuous Salivary Monitoring of Metabolites**, Analyst, 139, 1632-1636 (received Dec 2013, first published online Jan 2014). DOI: 10.1039/C3AN02359A

KLEINBERG, J., **Navigation in a small world**, Nature, vol. 406, p. 845, 2000.

KLEINBERG, J., **The small-world phenomenon: an algorithmic perspective**, in Proceedings of the thirty-second annual ACM symposium on Theory of computing, ser. STOC ’00. New York, NY, USA: ACM, 2000, pp. 163–170. [Online]. Available: http:// doi.acm.org/10.1145/335305.335325.

KLEINBERG, J., **Small-world phenomena and the dynamics of information**, in In Advances in Neural Information Processing Systems (NIPS) 14. MIT Press, 2001, p. 2001.

KLEINBERG, J., **The convergence of social and technological networks**, Communications of the ACM, vol. 51, no. 11, pp. 66 – 72, November 2008.

KRANZ, M., ROALTER, L., MICHAHELLES, F., **Things that twitter: social networks and the internet of things**, in Proc. of What can the Internet of Things do for the Citizens (CIoT) Workshop at Pervasive’10, May 2010.

KURNIAWAN, A., KYAS, M., **A Trust Model-Based Bayesian Decision Theory in Large Scale Internet of Things.** IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore, 7-9 April, 2015.

LEE, M. B., OUYANG, J., **Application Protocol adapted to health awareness for Smart Healthcare Service**, Proceedings of international workshop of Multimedia, Advanced Science and Technology Letters, 2013, Vol. 34.

LIANG, Z., SHI, W., **Enforcing cooperative resource sharing in untrusted p2p computing environments**, Mobile Networks Appl., vol. 10, pp. 971–983.2003.

LIU, G., WANG, Y., LI, L., **Trust management in three generations of web-based social networks,** in Proceedings of the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, ser. UIC-ATC '09. IEEE Computer Society, 2009, pp. 446–451.

LIU, Y., CHEN, Z., XIA, F., LV, X., BU, F., **A trust model based on service classification in mobile services**, in Green Computing and Communications (GreenCom), IEEE/ACM Int´l Conference on Int´l Cyber, Physical and Social Computing (CPSCom), 2010, p. 572-577.

LORINCZ, K., MALAN, D. J., FULFORD-JONES, T., NAWOJ A., CLAVEL A., SHNAYDER V., MAIKAND G., WELSH M., MOULTON **S., Sensor Networks for emergency response: challenges and opportunities**, IEEE Pervasive computing, vol. 3, n 4, 2004.

MA, Y.W., LAI, C.F., HU, C.C., CHEN, M.C., HUANG, Y.M., **RFID-based seamless multimedia services for smart homes**, International Journal of Internet Protocol Technology, vol. 4, no. 4, pp. 232-239, 2009.

MARSH, S., **Formalising Trust as a Computational Concept**, Department of Computing Science and Mathematics University of Stirling, April 1994

MARTELETO, R. M., **Análise de redes sociais – aplicação nos estudos de transferência da informação.** Ciência da Informação, Abr. 2001, Vol. 30, no 1, p. 71-81.

MARTI, S., GARCIA-MOLINA, H., **Identity crisis: Anonymity vs. reputation in p2p systems**, in Proceedings of the 3rd International Conference on Peer-to-Peer Computing. IEEE Computer Society, 2003, p. 134.

MARTI, S., GANESAN, P., GARCIA-MOLINA, H., **Sprout: P2p routing with social networks**, in *Proc. of EDBT 2004*, March 2004.

MILLAN, J.; PARK, S. -E.; KIEFER, S.; MEYER, J. -U., **TOPCARE - Implementation of a telematic *homecare* platform in cooperative health care provider networks.** Conference: Engineering in Medicine and Biology, 2002. 24th Annual Conference and the Annual Fall Meeting of the Biomedical Engineering Society EMBS/BMES Conference, 2002. Proceedings of the Second Joint, Volume: 3.

MISLOVE, A., GUMMADI, K. P., DRUSCHEL, P., **Exploiting social networks for internet search**, in *Proc. of ACM HotNets 2006*, November 2006.

MOEHR, J.R., SCHAAFSMA J., ANGLIN C., PANTAZI, S.V., GRIMM N.A., ANGLIN S., **Success factors for telehealth - A case study. International Journal of Medical Informatics**, 2006, p. 755-763.

NAZZ, E., SOKOLER, T., **Walky for embodied microblogging: sharing mundane activities through augmented everyday objects**, in Proc. of the 13th International Conference on Human-Computer Interaction with Mobile Devices and Services, MobileHCI, 2011.

NING, H., NING, N., QU, S., ZHANG, Y., YANG, H., **Layered structure and management in Internet of things**, Future Generation Communication and Networking, vol. 2, pp. 386-389, Dec.2007.

NING, H., WANG, Z., **Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?** IEEE Communication Letters, vol. 15, No 4, Abr.2011

NING, H., WANG, Z., **Future internet of things architecture: Like mankind neural system or social organization framework?** Communications Letters, IEEE, vol. 15, no. 4, pp. 461 –463, 2011.

NSF/DOC – Sponsored Report, **Converging Technologies for improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science**, June 2002.

OLLA, P., MORAR S., TAN J., PAUL R., Integrating Mobility into the Health Care Sector: The Next Generation of Mobile Health Applications. Special Issue of the International Journal of Electronic Health, InderScience Publishers, 2007, p. 1-7.

OSTERMAIER, B., ROMER, K., MATTERN, F., FAHRMAIR, M., KELLERER, W., **A real-time search engine for the web of things**, in Internet of Things (IOT), 2010, 2010, pp. 1–8.

THIESSEPASCHE, S., ANGELONI, R. ISCHER, M. LILEY, J. LUPRANO, G. VOIRIN, **Wearable Biosensors for Monitoring Wound Healing**, Advances in Science and Technology, 57, 80, 2008.

RENAULT, E., **Toward a security model for the future network of information**, in Proc. of 4th International Conference on Ubiquitous Information Technologies & Applications, Dec. 2009.

RESNICK, P., KUWABARA, K., ZECKHOUSER, R., FRIEDMAN, E., **Reputation Systems**, Communications, ACM, 2000, Vol. 43, p. 45-48.

ROMAN, R., NAJERA P., LOPEZ, J., **Securing the internet of things.**, Computer networks, 2011, 44(9): 51-58.

SARIT, A., MANIK, L., D., **Internet of Things – A paradigm shift of Future Internet Applications**, Institute of Tehcnology, Nirma University, 2011.

SELCUK, A.A., UZUN, E., PARIENTE, M.R., **A reputation-based trust management system for p2p network** in Proceedings of the 2004 IEEE International Symposium on Cluster Cumputing and Grid. IEEE Computer Society, 2004, p. 251-258.

SHERWOOD, R., LEE, S., BHATTACHARJEE, B., **Cooperative peer groups in nice**, Computer Networks., vol. 50, pp. 523–544, 2006.

SHOU, L., CHAO, H. C., **Multimedia traffic security architecture for the internet of things**, IEEE Network, vol. 25, pp. 35-40, 2011.

STEG, H., **Europe Is Facing a Demographic Challenge – Ambient Assisted Living Offers Solutions.** In: VDI/VDE/IT, Berlin, Germany, 2006

SUROWIECKI, J., **The wisdom of crowds**. Doubleday, 2004.

THIESSE, F., FLOERKEMEIR, C., HARISSON, M., MICHAHELLES, F., RODUNER, C., **Technology, standards, and real-world deployments of the EPC network**, IEEE Internet Computing, vol. 13, pp. 36-43, Mar. 2009.

TRANSPARENCY MARKET RESEARCH, **Biosensors Market (Electrochemical, Optical, Piezoelectric & Thermistor) - Global Industry Analysis, Size, Share, Growth, Trends and Forecast**, **2012 – 2018**, 2013.

TRAVERS, J., MILGRAM, S., **An experimental study of the small world problem**, Sociometry, vol. 32, pp. 425–443, 1969.

TSELENTIS, G., GALIS, A., GAVRAS, A., KRCO, S., LOTZ, V., SIMPERL, E., STILLER, B., ZAHARIADIS, T., **Towards the future internet-emerging trends from European research**, IOS Press, 2010.

VAZQUEZ, J. I., **Communication architectures and experiences for we-connected physical smart objects**, in Proc. Of 2010 IEEE International Conference on Pervasive Computing and Communications Workshop, pp. 684-689, 2010.

VERMESAN, O., FRIESS, P., **Internet of things – From Research and Innovation to Market Deployment**, Rivers Publishers, Denmark, 2014.

WANG, Y., VASSILEVA, J., **Bayesian network-based trust model**, in Proceedings of the 2003 IEEE/WIC International Conference on Web Intelligence, ser. WI03. IEEE Computer Society, 2003, pp. 372.

WANG, H., TAN, C. C., LI Q., **Snoogle: A search engine for pervasive environments**, Parallel and Distributed Systems, IEEE Transactions on, vol. 21, no. 8, pp. 1188–1202, 2010.

WANG, Y., LI, K., **Topology mining of sensor networks for smart home environments**, International Journal of Ad Hoc and Ubiquitous Computing, vol. 7, no.3 pp. 163-173, 2011.

WATTS, D. J., STROGATZ, S. H., **Collective dynamics of small-world networks,** nature, vol. 393, no. 6684, pp. 440–442, 1998.

WHITWORTH, R., **Analytical Tattoo**, The Analytical Scientist, 10, 9, 2013.

WHO, World Health Oeganiation., **Medical Devices: Managing the Mismatch, an Outcome of the Priority Medical Devices Project,** ISBN 9789241564045, Geneva, 2010.

XIONG, L., LIU, L., **Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities**, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGI-NEERING, vol. 16, pp. 843–857, 2004.

YAN, L., ZHANG, Y., LAURENCE, T.Y., NING, H., **Internet of things: From RFID to the Next-Generation Pervasive Networked Systems**, Auerbach Publications, 2008.

YAN, Z., ZHANG, P., VASILAKOS, A. Z., **A Survey on trust management for Internet of Things**. Journal of network and computer applications, 2014, 42: 120-134.

YAP, K.-K. SRINIVASAN, V., MOTANI, M., **Max: human-centric search of the physical world.** in SenSys, J. Redi, H. Balakrishnan, and F. Zhao, Eds. ACM, 2005, pp. 166–179. [Online]. Available: http://dblp.uni-trier.de/db/conf/sensys/sensys2005.html#YapSM05

YU, B., SINGH, M. P., SYCARA, K., **Developing trust in large-scale peer-to-peer systems**, in Proceedings of First IEEE Symposium on Multi-Agent Security and Survivability, 2004, pp. 1–10.

YU, H., KAMINSKY, M., GIBBONS, P. B., FLAXMAN, A., **Sybilguard: defending against sybil attacks via social networks**, in *Proc. of IEEE SigComm 2006*, September 2006.

ZHONG, N. Z, **Research Challenges and Perspectives on Wisdom Web of Things (W2T)**, Journal of Supercomputing, DOI: 10.1007/s11227-010-0518-8, 2010.

ZHOU, R., HWANG, K., CAI, M., **Gossiptrust for fast reputation aggregation in peer-to-peer networks**, IEEE Trans. on Knowl. and Data Eng., vol. 20, pp. 1282–1295, 2008.

ZHU, Q., WANG, R., CHEN, Q., LIU, Y., QIN, W., **IOT Gateway: bridging wireless sensor network into internet of things**, in Proc. of international Conference on Embedded and Ubiquitous Computing (EUC), pp.347-352, Dec. 2010.