Confiança em Sistemas Sensíveis ao Contexto aplicados ao Domínio da Saúde

Marcelo Henrique Monier Alves Júnior[1],
Samyr Beliche Vale[1], **Francisco José da Silva e Silva**[1]

[1]Programa de Pós-Graduação em Ciências da Computação
Laboratório de Sistemas Distribuídos - LSD
Universidade Federal do Maranhão (UFMA)
Av. dos Portugueses 1966, Bacanga, Cep 65.080-805 – São Luis – MA – Brasil

marcelomonier@gmail.com, samyr@deinf.ufma.br, fssilva@deinf.ufma.br

Abstract. *Mobile health or m-health is the name given to the practice of medicine and health care through mobile devices. The MobileHealthNet project is a middleware focused on creating health applications in mobile social networks (RSMs). One of the drawbacks of MobileHealthNet is that its context information don't have QoC, which can cause problems, like a decision made erroneously by a doctor, because of data collected from a sensor with low accuracy. This qualification focuses on developing research to solve a clearly defined problem, which is to implement the QoC parameters in the MonileHealthNet project infrastructure. Our main goal is to provide support to the QoC parameter named Trustworthiness.Finally, a performance evaluation of the trustworthiness of each component used in the project infrastructure will be performed.*

Keywords: *Quality of Context, Context, Middleware, Trustworthiness;*

Resumo. *Saúde Móvel ou m-health é a denominação dada à prática de medicina e cuidados da saúde através de dispositivos móveis. O projeto MobileHealthNet propõe o desenvolvimento de um middleware voltado para a criação de aplicações da saúde em Redes Sociais móveis (RSMs). Um dos inconvenientes do MobileHealthNet é que suas informações de contexto não possuem QoC, podendo gerar certos problemas, a exemplo de uma decisão tomada erroneamente por um médico, em razão de um dado coletado de um sensor com baixo nível de precisão. Esta qualificação centra-se no desenvolvimento de uma pesquisa para solucionar um problema bem definido, qual seja implementar parâmetros de QoC na infraestrutura do projeto MonileHealthNet. O nosso objetivo principal, é fornecer suporte ao parâmetro de QoC denominado Confiabilidade (Trustworthiness). Por fim, será realizada uma avaliação de desempenho da confiabilidade de cada componente aplicado na infraestrutura do projeto.*

Palavras-chaves: *Qualidade de Contexto; Contexto; Middleware; Confiabilidade;*

1. Introdução

Com o aumento da utilização de dispositivos móveis, surgiu igualmente a demanda de aplicações práticas voltadas para esses dispositivos nos mais variados ramos do conhecimento humano, tais como na saúde, na educação, no sistema financeiro, dentre outros. O referido crescimento ocorreu devido à facilidade de acesso à informação de qualquer lugar e em qualquer momento proporcionada pela utilização desses mecanismos. Outro fator relevante que contribuiu para o fenômeno em comento é o fato de tais dispositivos estarem cada vez mais baratos e possuírem mais poder computacional, a exemplo da expansividade no armazenamento, de uma maior quantidade de sensores internos, maior poder de processamento de dados, diferentes interfaces de redes etc., possibilitando, assim, a execução de aplicações muito mais robustas, como, por exemplo, aplicações ubíquas.

Um dos primeiros a trazer à tona o termo "*Computação Ubíqua*" foi [Weiser 1991], definindo-o como um modelo de interação homem-máquina que visa melhorar o uso do computador, através da disponibilização de inúmeros dispositivos interagindo entre si de maneira transparente aos usuários. Aplicações ubíquas são adaptáveis ao ambiente do usuário, pois não necessitam da entrada explicita do mesmo para prover serviços, funções e informações.

De outro lado, quem também aderiu a esse tipo de acesso foram as redes sociais online, pois, com a facilidade de conexão, ficaram mais fáceis o compartilhamento de informações e a conectividade entre os usuários. Como resultado, uma nova tendência operou-se no campo da sociabilidade entre os indivíduos, as chamadas Redes Sociais Móveis (RSMs), que atraíram consideravelmente a atenção das comunidades acadêmicas e da indústria [Karam and Mohamed 2012]. Essas redes são consideradas uma subclasse de redes sociais, às quais os usuários móveis podem acessar, publicar ou compartilhar conteúdo gerado ou obtido através de sensores no dispositivo móvel para a interação com os seus contatos na rede social[Ari 2013].

[Teles et al. 2013] definem RSM como uma combinação de três áreas de conhecimento: Computação Móvel, Redes Sociais e Ciência de Contexto. Podemos observar esta definição na figura 1.

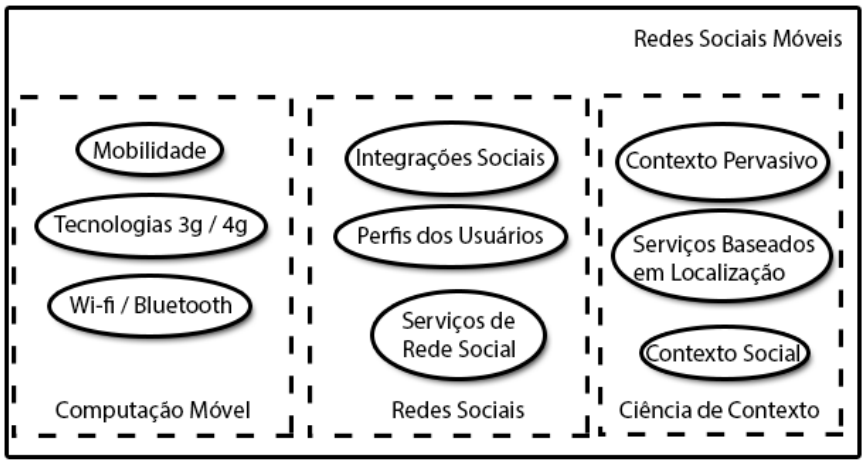

Figura 1. Definição de RSMs baseado em [Teles et al. 2013]

O suporte à mobilidade é obtido pelos dispositivos portáteis e pela conectividade sem fio. Assim, o usuário é capaz de permanecer sempre online. Redes Sociais possibilitam a criação de perfis e a interação entre eles, podendo representar indivíduos, sistemas ou organizações. A Ciência de Contexto é responsável por adaptar as aplicações e funcionalidades das redes sociais, permitindo, desse modo, que se ofereçam recursos de acordo com informações de contexto.

Neste cenário, surgiram vários tipos de aplicações para RSMs. Estas definem-se como publicadoras de informações de contexto às Redes Sociais, pois os dispositivos móveis são capazes de sensorear dados físicos do ambiente e, com isso, possibilitar que uma aplicação possa combinar dados de contexto para inferir uma situação do usuário. Diferentes áreas começaram a criar aplicações deste tipo, incluindo, como visto, as que são voltadas ao domínio da saúde.

Estas aplicações são conhecidas como *m-health* ou *Mobile Health* (Saúde Móvel). Tal denominação é dada à prática de medicina e cuidados da saúde através de dispositivos móveis [Ist 2006], que, nesse sentido, conferem uma nova perspectiva à relação profissional existente nesse campo, por uma simples razão: aplicações de *m-health* possibilitam aos profissionais de saúde o acompanhamento dos pacientes sem a necessidade de um espaço físico em comum; em outros termos, é possível que médicos, enfermeiros e outros profissionais procedam ao tratamento/acompanhamento de seus pacientes à distância, por intermédio da utilização dos mencionados dispositivos.

Esse novo enfoque à relação profissional implica considerável redução de custos, permitindo uma posição mais confortável aos envolvidos na relação, de maneira que é perfeitamente viável a hipótese de uma consulta médica na qual o profissional da saúde e o paciente estejam em suas respectivas residências, ou em localidades distintas. Um exemplo para esse tipo de situação são as aplicações de RSMs, pois podem prover o compartilhamento de informações, integração e colaboração social entre todos os envolvidos no processo de atendimento à saúde [BATISTA 2013].

Em observância a esta demanda, foi criado o projeto *Mobile Social Networks for Health Care in Offside Regions* (MobileHealthNet), que consiste na criação de um *middleware* para auxiliar no desenvolvimento de aplicações no domínio da saúde. Através do middleware é possível, por exemplo, estabelecer uma RSM por intermédio da qual profissionais da saúde, pacientes e a comunidade em geral possam trocar informações e experiências sobre determinado tratamento, medicações, campanhas de saúde, entre outros. Desse modo, o acompanhamento médico pode ser realizado remotamente e por equipes multidisciplinares, nas quais profissionais de diversas especialidades poderão contribuir no tratamento de diferentes pacientes.

2. Caracterização do problema

Os serviços de contexto disponibilizam uma infraestrutura de suporte para coleta, gerenciamento e distribuição das informações de contexto sobre uma série de temas, que podem estar relacionados ao usuário, a objetos ou até mesmo ao ambiente. Tais serviços adquirem informações de contexto de várias fontes - coletadas por terceiros -, as quais geralmente fornecem os dados contextuais.

Esses dados necessitam de qualidade, principalmente quando envolvidos no âmbito da saúde. Aplicações de *m-health* não podem receber dados sem um alto nível de

qualidade, pois as tomadas de decisões dos profissionais da saúde baseadas nesses dados são cruciais, atingindo diretamente o estado de saúde do paciente, podendo-se falar, inclusive, em risco de morte. Como exemplo, considere um paciente com Hipertensão Arterial[1] que necessita de acompanhamento em tempo real. As informações enviadas aos profissionais da saúde deverão ser as mais recentes, pois se houver atraso nas informações recebidas, haverá uma tomada de decisão equivocada, influenciando diretamente no quadro de saúde do paciente. O parâmetro de qualidade de contexto relacionado a esta questão é conhecido por Atualidade (*Freshness*), que define a idade da informação recebida, ou seja, o tempo decorrido desde que a informação foi coletada até a sua entrega ao consumidor.

Outra importante questão a ser levada em consideração são as limitações dos consumidores para processar a quantidade de mensagens que os provedores conseguem enviar. Suponhamos que uma aplicação só consiga processar cada mensagem com um intervalo de três segundos, mas que as mensagens sejam a ela enviadas a cada segundo. Além de causar um tráfego desnecessário na rede, a aplicação pode perder desempenho devido a quantidade de mensagens a serem processadas. Nesse contexto a qualidade é relevante, pois é necessário saber a demanda da aplicação, ou seja, o quanto a aplicação quer e pode consumir. Os parâmetros de qualidade de contexto Frequência (*Frequency*), que define a quantidade de atualizações que a aplicação deseja receber a cada intervalo de tempo; e Taxa de atualização (*Refresh Rate*), que define a quantidade de atualizações recebidas que aplicação deseja processar a cada intervalo de tempo independente da frequência com a qual essas atualizações são produzidas, estão relacionados a esta questão.

Qualidade de Contexto (QoC) é qualquer informação que descreve a qualidade da informação que é usada como informação de contexto. Assim, QoC refere-se à informação, não ao processo e nem ao componente de hardware que possivelmente fornece as informações [Buchholz and Schiffers 2003]. Diversos parâmetros de QoC foram definidos em trabalhos constantes da literatura, tais como Manzoor [Manzoor 2010], Huebscher et al. [Huebscher and McCann 2004] e Sheikh et al. [Sheikh et al. 2007].

Um parâmetro de qualidade de contexto de particular interesse ao trabalho de mestrado proposto nesta qualificação é conhecido por Confiabilidade (*Trustworthiness*). As aplicações geradas por um *middleware* que possuem enfoque no desenvolvimento de aplicações na área da saúde, como é o caso do MobileHealthNet, necessitam de informações de contexto dotadas de alto nível de confiança, pois que podem envolver circunstâncias, de certa forma, delicadas, como um sistema de acompanhamento de pacientes com problemas cardíacos. Outra grande dificuldade que merece ser lembrada é a qualidade das redes móveis, pois existem várias limitações, como a largura da banda, intermitência do sinal, menor área de cobertura, dentre outros.

No entanto, a incorporação de mecanismos adequados para prover confiabilidade aos dados de contexto produzidos por aplicações em execução no MobileHealthNet é uma tarefa desafiadora. Apesar da definição mais citada na literatura sobre o termo confiabilidade (tradução literária para trustworthiness) ser de Smith [Smith 1976], a qual define que é a probabilidade de um dispositivo operar adequadamente para o período de tempo pretendido sob as condições de operação encontradas, adota-se conceitualmente no pre-

[1]Hipertensão Arterial são níveis pressóricos iguais ou acima de 140 mmHg (máxima) ou de 90 mmHg (mínima), devidamente avaliados pelo médico, em momentos diferentes. - http://www.intermedica.com.br/qualivida/doencas-cronicas/hipertensao-arterial

sente trabalho a de Neisse et al. [Neisse et al. 2008], qual seja a de que confiabilidade de um serviço sensível ao contexto depende do relacionamento de confiança entre as entidades, tais como provedores e consumidores de contexto, distribuidores destas informações, enfim, todos os componentes que cooperam para o funcionamento do sistema.

Por exemplo, eventualmente, os usuários de sistemas sensíveis ao contexto podem não concordar com que suas informações sejam disponibilizadas a terceiros dentro do sistema, priorizando, dessa forma, a sua privacidade. Assim, o provedor de contexto terá que confiar no distribuidor, uma vez que este será o responsável por compartilhar suas informações. Portanto, outro grande desafio relacionado a esta questão é a definição de um modelo de confiança que leve em consideração as diversas entidades envolvidas na coleta, distribuição e consumo de dados de contexto e suas particularidades, ou seja, o gerenciamento da confiança.

3. Objetivos

3.1. Geral

O objetivo geral deste trabalho é o desenvolvimento do suporte para o parâmetro de QoC Confiabilidade (*Trustworthiness*) a ser incorporado ao *middleware* MobileHealthNet.

3.2. Específicos

1. Investigar o estado da arte no provimento de Qualidade de Contexto para aplicações móveis voltadas ao domínio da saúde;
2. Desenvolvimento de uma proposta de um modelo que possa representar a confiabilidade dos dados em sistemas sensíveis ao contexto;
3. Implementar o modelo proposto no middleware MHNCS;
4. Tratar aspectos de segurança para a garantia da troca de informações seguras dentro do *middleware MHNCS*;
5. Testar e avaliar o desempenho do suporte do *Trsutworthiness* a ser desenvolvido.

4. Fundamentação teórica

4.1. MobileHealthNet

O projeto *MobileHelathNet* é fruto de uma parceria entre o Laboratório de Sistemas Distribuidos [1] (LSD) da Universidade Federal do Maranhao (UFMA) e o *Laboratory for Advanced Collaboration* [2] (LAC) da Pontificia Universidade Catolica do Rio de Janeiro (Puc-Rio). Conta-se igualmente com o apoio do Hospital Universitário da UFMA (HU-UFMA), responsável por fornecer o conhecimento da área de saúde necessário para o seu desenvolvimento. Existem duas principais unidades do HU-UFMA que contribuem com a iniciativa: o Programa de Assistencia a Pacientes Asmaticos (PAPA) e a Casa da Dor [BATISTA 2013]. O PAPA está condicionado ao tratamento e monitoramento de pacientes com este tipo de patologia crônica; já a Casa da Dor não faz distinção entre patologias, ficando responsável pelo tratamento de pacientes com qualquer tipo de dor aguda.

O projeto tem sua composição constituída por camadas, como podemos observar na figura 2. A primeira camada é a de comunicação, chamada de *MobileHealthNet*

[1] http://www.lsd.ufma.br
[2] http://lac-rio.com/

Communication Framework, a qual contém todos os mecanismos para facilitar o compartilhamento de dados nas RSMs. Baseia-se no *Scalable Data Distribution Layer* (SDDL) [David et al. 2012] que trabalha com dois protocolos de comunicação: o MRUDP, já citado na seção 2, e o *Data Distribution Service* (DDS) da *Object Manage Group* (OMG). O primeiro é responsável pela comunicação de entrada e saída entre a rede principal e os nós moveis; o DDS, pela comunicação dentro do *MobileHealthNet*. Por ser a camada na qual iremos focar nessa qualificação, separamos um tópico para explicá-la detalhadamente.

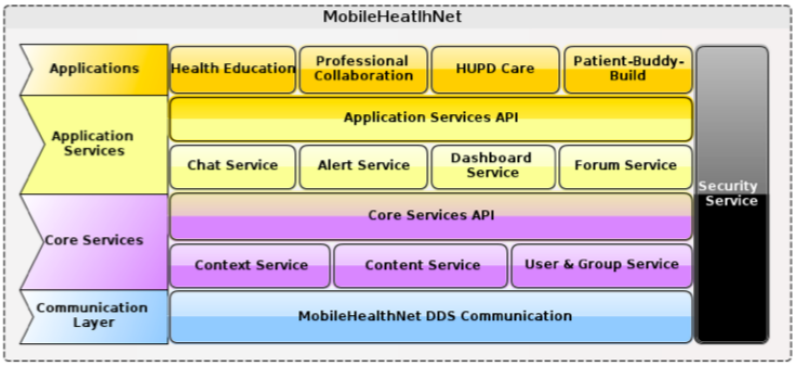

Figura 2. Arquitetura do MobileHealthNet

A camada seguinte é a *Core Services*, através da qual são disponibilizados os serviços básicos que as aplicações e os serviços criados a partir do MobileHealthNet utilizarão. A camada é composta por três serviços, a saber:

- **Context Service** - responsável por armazenar e disponibilizar as informações de contexto;
- **Content Service** - responsável pela publicação de mídias (imagens, vídeos, áudios, textos, etc) nas RSMs. Este serviço permite a nomeação de cada mídia com meta informações definidas pela aplicação (ex.: um modelo de sensor de ECG que um texto referencia);
- **User & Group Service** - serviço que gerencia os usuários e grupos das RSMs.

Já a camada *Application Service* disponibiliza serviços típicos de redes sociais, como o serviço de alertas, chat, fórum e até mesmo um serviço de publicação em murais. Em transversal com todas as camadas, está a camada *Security Services*, tratando de mecanismos de privacidade e segurança. Por fim, tem-se a camada *Applications*, que representa os possíveis tipos de aplicações a serem desenvolvidas.

4.1.1. Arquitetura da Infraestrutura do middleware MobileHealthNet Context Service (MHNCS)

A figura 3 sintetiza os aspectos estruturais do MHNCS.

O MHNCS constitui um conjunto de componentes necessários para auxiliar a integração do dispositivo com o ambiente pervasivo e disponibilizar os serviços necessários que integram a arquitetura. Conforme observamos na Figura 3, o MHNCS é formado por 3 componentes básicos: Módulo de Distribuição (*Context Distribuition Service* (CDS)), que é responsável por gerenciar a distribuição de contexto com os dispositivos móveis em um ambiente pervasivo; Gerenciador de Eventos (*Context Event Service*

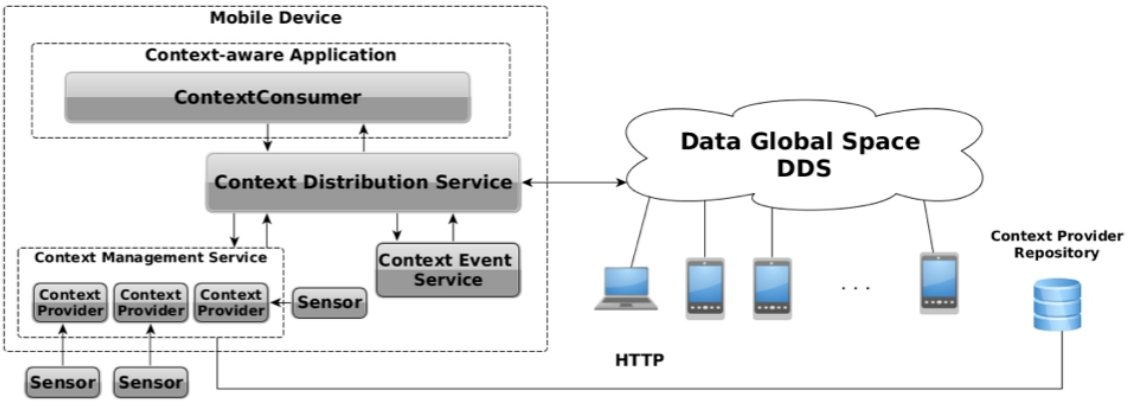

Figura 3. Arquitetura do MHNCS [Pinheiro 2014]

(CES)), que fornece mecanismo avaliadores das informacoes de contexto e notifica as aplicações somente quando as condições definidas forem satisfeitas; e parte da arquitetura proposta e formada por componentes modificados, oriundos de um middleware voltado para o gerenciamento de provedores de contexto denominado *Context Management Service* (CMS) [Malcher et al.].

4.2. Ciência de Contexto

[Dey 2001] define contexto como sendo qualquer informação que pode ser usada para caracterizar a situação de uma entidade. Uma entidade pode ser uma pessoa, lugar ou objeto que seja considerado relevante na interação do usuário com a aplicação. Sistemas sensíveis ao contexto são habilitados para adaptar suas funcionalidades e comportamento de acordo com o contexto atual do usuário, sem sua explícita intervenção.

[Bolchini et al. 2009] descreve as informações de contexto como um conjunto de variáveis que pode ser de interesse para uma entidade, podendo, também, influenciar em suas ações. Por meio deste tipo de informação, é possível o desenvolvimento de sistemas computacionais, os quais podem se reconfigurar ou adaptar a uma determinada situação, ou recomendar ações a partir de análises de informações coletadas do ambiente.

Para [Chen and Kotz 2002] as informações de contexto classificam-se em quatro tipos:

- **Contexto Físico**: informações sobre o mundo real, obtidas por meio de sensores. Por exemplo, sensor de luminosidade, sensor de ruido, temperatura, luminosidade e localização;
- **Contexto Computacional**: informações sobre um sistema computacional, como os seus recursos e características. Por exemplo, nível de bateria, consumo de memória ou processamento e conexões de rede disponíveis;
- **Contexto do Usuário**: informações que caracterizam o usuário, tais como: estado emocional, localização e atividade atual;
- **Contexto de Tempo**: informações relacionadas ao tempo de uma atividade real ou virtual. Está relacionada à dimensão do tempo, como a hora do dia, dia da semana, mês, ano ou uma estação climática.

A utilização de informações de contexto permite que desenvolvedores de sistemas possam enriquecer a usabilidade de sua aplicação e, assim, o sistema sensível ao contexto pode reagir a determinadas situações sem a necessidade da interação com o usuário. Por exemplo, caso o sistema detecte que o nível de bateria está baixo, ele pode realizar ações para economizá-la, seja reduzindo a luminosidade do visor do dispositivo, seja desativando as interfaces de rede ou sensores que não estão em uso no momento.

O Contexto Pervasivo é aquele obtido a partir de sensores de hardware nos dispositivos móveis, os quais podem ser de vários tipos: luminosidade, visual (câmera), áudio, movimento ou acelerômetro, localização, toque, temperatura, físicos (bio-sensores), dentre outros [Baldauf et al. 2007]. Dados gerados a partir desses sensores podem ser usados individualmente ou de forma combinada para inferir a situação do usuário. Essa situação pode ser, por exemplo, a (in)disponibilidade do usuário para realizar alguma atividade, seu estado de saúde ou o lugar em que se encontra (restaurante, residência ou local de trabalho).

O termo Contexto Social é utilizado para caracterizar as possíveis formas de relacionamento e de interações entre pessoas, intermediadas ou não por alguma tecnologia de comunicação [Ling 2008]. A expressão envolve o ambiente social do usuário (uma festa ou uma reunião) e a relação que pode ser estabelecida com outros usuários. A noção de contexto social deve levar em consideração tanto as experiências no mundo real quanto no virtual. Informações de contexto social podem ser extraídas por meio de redes sociais, sensores ou formulários, sendo - tais informações - aspectos de contexto de alto nível relacionados com a dimensão social dos usuários, tais como o perfil do usuário, pessoas próximas, e sua atual situação social [Adams et al. 2008].

Como visto, os conceitos de rede social se unem à computação móvel e ciência de contexto e, a partir disso, [Lubke et al. 2011] desenvolveram o conceito de Contexto Social Pervasivo. Trata-se, basicamente, de um conjunto de informações decorrentes de interações diretas e indiretas entre pessoas que carregam dispositivos móveis equipados com sensores e que estejam conectadas através de uma mesma rede social. Os autores ainda classificaram e diferenciaram várias formas em que o contexto social pervasivo pode ser utilizado baseados nas *W5H Questions*, como visto abaixo:

- Quem - ***W**ho*: expressa quem são os participantes envolvidos no consumo e na produção das informações de contexto;
- O que - ***W**hat*: diz respeito a qual tipo de contexto é utilizado ou se é importante para a aplicação;
- Onde - ***W**here*: relacionado ao espaço físico onde os laços ou interações sociais são estabelecidos;
- Quando - ***W**hen*: caracterização das interações entre usuários e as informações de contexto que eles produziram em uma perspectiva temporal;
- Por que - ***W**hy*: expressa o porquê de uma informação de contexto ser usada, determinando a causa ou razão de sua utilização pela aplicação. Neste caso, isso é bem relacionado ao objetivo da aplicação;
- Como - ***H**ow*: expressa como a informação de contexto (originada a partir do mundo real, mundo virtual ou de ambos) pode influenciar ou comprometer aplicações.

4.3. Qualidade de Contexto

Conforme afirmado na seção 2, o termo QoC foi definido primeiramente por [Buchholz and Schiffers 2003]. Nesse artigo, foram apresentados *trust-worthiness, probability of correctness, precision, resolution e up-to-datedness* como importantes parâmetros de QoC. Além disso, o trabalho comparou o referido conceito com a Qualidade de Serviço (QoS), categoria esta que provê informação sobre o desempenho de um serviço; equiparou-se, igualmente, a referida expressão - QoC - com a Qualidade de Dispositivo (QoD), a qual, por seu turno, qualifica a capacidade e propriedades técnicas de um dispositivo. Após essa relação, os autores ressaltam que essas três métricas, embora independentes, podem influenciar-se mutuamente.

Conceituação diversa de QoC é feita por [Krause and Hochstatter 2005], os quais afirmam ser o termo qualquer dado inerente que descreve a informação de contexto, a qual pode ser utilizada para determinar o valor de uma informação para uma aplicação específica. Identificam-se as fontes de parâmetros de QoC como as características do sensor, o valor declarado pela própria informação de contexto, verificação específica da situação e a granularidade do formato de representação.

Uma nova definição de QoC é feita por [Manzoor et al. 2011]. Afirma o autor que o termo indica o grau de conformidade da coleta de contexto pelo sensor para a situação prevalente do ambiente e as exigências de um consumidor de contexto específico. Na figura 4.3 [Manzoor et al. 2011] cria um novo modelo de processamento de QoC. Tal modelo possui três diferentes camadas para o processamento das informações com QoC.

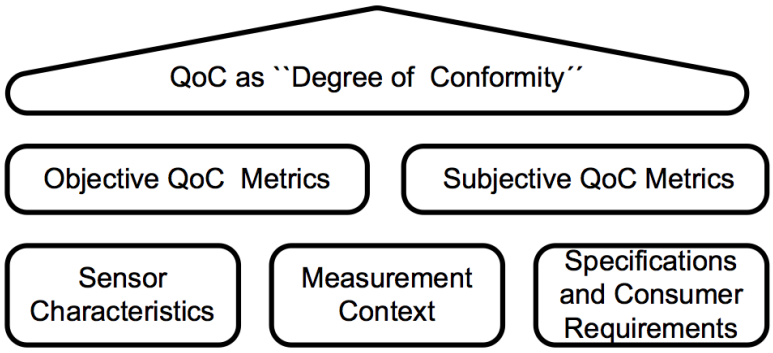

Figura 4. Modelo de processamento de QoC [Manzoor et al. 2011]

A camada mais baixa é a origem da QoC, formada pelos dados utilizados pela camada superior. Compõe-se de três sub-categorias, a saber: i) características do sensor - são informações sobre o sensor que podem afetar a qualidade da informação de contexto fornecido pelo dispositivo, como a acurácia, precisão, granularidade, período de tempo, estado do sensor e o alcance dele; ii) medição do contexto - mostra as informações relacionadas a uma medição específica, a exemplo do tempo de medição, do sensor de localização, das informações de localização de uma entidade, em suma, referentes aos atributos específicos do contexto de um objeto; iii) especificações e exigências do consumidor - o consumidor faz um detalhamento de suas exigências sobre a qualidade das informações de contexto, como o tempo de validade da informação, atributos necessários, valor crítico e nível de acesso.

A camada superior é representada por dois tipos de métricas: as métricas de QoC objetivas e as de QoC subjetivas. As primeiras demonstram a qualidade de contexto como uma quantidade independente e seu cálculo envolve características do sensor e medição do contexto; as subjetivas, a qualidade do contexto para utilização de um consumidor específico para uma determinada finalidade.

Nas subseções a seguir detalhamos os principais parâmetros de qualidade de contexto que podem ser encontrados na literatura.

4.3.1. Accuracy

[Manzoor 2010] afirma que *accuracy* é o grau de exatidão do contexto ou a capacidade do sensor em medir a quantidade aproximada ao valor real. [Web 1999] assinala que *inaccuracy*, ou erro absoluto de um sensor físico, pode ser calculado pela diferença entre o valor real e o valor mensurado pelo sensor. Temos, então, a seguinte equação,

$$E = T - M$$

na qual, *E* é o erro na medição, *T* é o valor real e *M* é o valor mensurado pelo sensor. Geralmente, o valor real é acordado antes da medição ou em alguns casos é uma verdade absoluta. Já a *accuracy* de um sensor físico, tem seu valor calculado através da equação,

$$Accuracy = 1 - \frac{|E|}{T}$$

sendo *E* o valor da *inaccuracy* e *T*, o valor real. Entende-se que a *accuracy* é calculada subtraindo o erro relativo de 1. Outra *accuracy* importante nesta definição é a do sensor virtual, o qual pode ser calculado com a seguinte equação

$$Accuracy = \frac{N\acute{u}mero\ de\ inst\hat{a}ncias\ classificadas\ como\ corretas}{N\acute{u}mero\ total\ de\ inst\hat{a}ncias}$$

4.3.2. Precision

Segundo [Manzoor 2010], precision é o grau de exatidão de uma medição. Isto indica a capacidade de um sensor para dar a mesma leitura que a mesma quantidade de medição sob as mesmas condições. Ao contrário do parâmetro accuracy, que apresenta a proximidade de uma medição do valor real, precision apresenta as proximidades sucessivas das leituras dos sensores da mesma quantidade sob as mesmas condições. Um exemplo de teste de precision é sob o sensor físico, o qual pode ser medido através da repetição dos ensaios em uma série de vezes e examinando a variação dos dados. [Manzoor 2010] utiliza a seguinte equação para avaliar esse parâmetro.

$$Precision = \frac{número\ de\ positivos\ verdadeiros}{número\ total\ de\ positivos\ verdadeiros\ e\ positivos\ falsos} \quad (4)$$

Na equação, o número de positivos verdadeiros representa os casos que tenham sido corretamente reconhecidos como positivos e os positivos falsos, que tenham sido reconhecidos incorretamente como positivos.

4.3.3. Probability of Correctness

Segundo [Buchholz and Schiffers 2003], esse parâmetro mede a probabilidade de uma parte da informação de contexto estar correta. Suponha que exista uma sala com uma rede de sensores de temperatura. Um desses sensores pode falhar e começar a mandar a informação errada, por exemplo, medir 50ºC, enquanto o valor correto é de 25ºC. Com a utilização deste parâmetro, a fonte de informação de contexto original calcula quantas vezes esse sensor irá mandar a informação errada para o provedor de contexto por causa de problemas internos.

Já [Huebscher and McCann 2004], por sua vez, concluem, quanto à medição, através da análise da postura de uma pessoa (em pé, sentado, deitado no chão em perigo), que o parâmetro *Probability of Correctness* tem resultado diferente quando os tipos de sensores são diferentes, como a utilização de uma câmera de vídeo irá expressar um resultado diferente de um sensor de movimento. Os autores também afirmam que os parâmetros *Trust-worthiness* e *Probability of Correctness* são similares. Entretanto, enquanto a *Probability of Correctness* é fornecida pelo provedor de contexto, a *Trust-worthiness* é fornecida por agente externo para o provedor de contexto.

4.3.4. Temporal Resolution

[Sheikh et al. 2007] define este parâmetro como o período de tempo para que uma única instância de informação de contexto seja aplicável. Isso varia devido a duas principais razões: a primeira é que a fonte da informação de contexto pode ser limitada pela sua frequência de coleta (por exemplo, a coleta de temperatura de uma sala é realizada a cada oito horas, então a informação é valida por um período de oito horas após a coleta). A segunda limitação pode ser para proteger a privacidade do usuário (a entrada de um funcionário em uma sala pode ter uma precisão maior do que a saída dele desta sala). A precisão pode ser ofuscada, para garantir a privacidade do funcionário.

4.3.5. Spatial Resolution

Segundo [Sheikh et al. 2007], é a precisão com que é expressa a área física para a qual uma instância de informação de contexto é aplicável. Assim, ela refere-se à área de um espaço físico a que a informação de contexto está associada. Por exemplo, quando dizemos que a temperatura da cidade de São Luís está em 30ºC, isto não quer dizer que toda cidade está com a mesma temperatura.

Da mesma forma, quando se tem um conjunto de sensores em uma sala, tendo-se a temperatura maior registrada em um sensor localizado ao lado da janela e a temperatura menor, em um sensor ao lado do ar condicionado, deve-se atentar para o fato de que ambas as medições de temperatura podem não refletir corretamente a temperatura real do ambiente. Uma característica importante desse parâmetro é a garantia da privacidade do usuário em uma determinada região, por exemplo, em um sistema de monitoramento de localização, a informação será transmitida com um grau menor de precisão, então a informação será exibida dentro de um raio aceitável da região, garantindo, dessa forma, a privacidade do usuário.

4.3.6. Trustworthiness

Segundo Russell [Rus 2002] *trustworthiness* está relacionada ao indivíduo que recebe a confiança, ou seja, ao Trustee. A confiança é a expectativa que o Trustor terá no comportamento do Trustee, isto é, se o Trustee irá se portar de maneira que ele considera confiável. Não nos aprofundaremos aqui neste assunto, pois separamos um seção para abordar a confiança.

4.4. Confiança computacional

4.4.1. Definição

[Bezemer 2005] afirma que a psicologia descreve confiança como uma relação em três partes: A confia em B a respeito de X, no qual A representa quem dará a confiança (Trustor); B, quem vai receber a confiança (Trustee); e X, o assunto de confiança. Exemplificando: o usuário (A) confia em um sensor B para lhe fornecer a localização (X), no momento em que o mesmo está parado. Entretanto, não confia no mesmo para lhe fornecer a mesma informação quando ele está em movimento.

Para que haja um depósito de confiança no Trustee, deve-se ter a oportunidade de trair a confiança do trustor, e, ao mesmo tempo, não querer fazê-lo. [Bezemer 2005]. Nesse sentido, se o Trustor quiser garantir a prestação de serviço do Trustee, ele irá introduzir um elemento chamado ”controle”. Após tal procedimento, a confiança será removida do relacionamento. O controle é todo elemento utilizado para forçar o trustee a ser confiável, limitando ou removendo por completo a oportunidade de traição do mesmo.

Suponhamos: Uma empresa X contrata um serviço de armazenamento em nuvem de uma empresa Y, para suas informações. Nesse momento, a empresa X está confiando na empresa Y para gerenciar suas informações. No entanto, no contrato consta que, se a empresa Y fornecer ou alterar essas informações, a mesma pagará uma multa de U$ 20.000.000. Essa multa representa o controle de confiança que a empresa X terá com a empresa Y.

Outra forma de estabelecer a confiança é através da reputação. Esta é fornecida por meio da opinião de terceiros, ou seja, a confiança dada ao Trustee irá depender das informações passadas ao Trustor por terceiros que já com ele interagiram anteriormente.

Uma outra forma de confiança constante da literatura é a dependência. Cuida-se de uma forma mais fraca de confiança, na qual a oportunidade que o Trustee tem de trair

o Trustor não existe. Ela ocorre quando a quebra de confiança resulta na decepção do Trustor, não chegando, entretanto, o mesmo a prejudicar-se. Podemos exemplificar da seguinte forma: dois indivíduos concordam em se encontrar para uma partida de futebol e um deles não aparece, então caracteriza-se dependência. Porém, emprestar uma quantia em dinheiro para outro indivíduo, indica um caso de confiança.

4.4.2. Condições de confiança

Na literatura o conceito de condição de confiança se sobrepõe com o conceito de grau de confiança. Conforme [Rus 2002] condição de confiança pode ser vista como o que o Trustor espera de um Trustee para ser fiel. Já grau de confiança, por sua vez, é um conjunto de condições de confiança para saber se o Trustee terá mais ou menos confiança em um determinado assunto.

Podemos citar novamente o exemplo de confiança do sensor de movimento, em que o usuário A confia em um sensor B para lhe fornecer sua localização, desde que o mesmo esteja parado e não em movimento, a movimentação do usuário é a condição de confiança.

4.4.3. Construindo a confiança

A confiança é dada ao outro através do conhecimento prévio ou através de um histórico de interações. Dessa forma, é impossível estabelecer confiança quando nunca houver interação, pois, como sabemos, a confiança precisa ser construída. Entretanto, a literatura discute sobre três interações iniciais entre indivíduos: confiança generalizada, controle e reputação. A primeira é utilizada quando o risco de prejudicar-se é muito baixo; já o controle e a reputação são utilizados para mitigar o risco do Trustor.[Stark 2014]

Como citado acima, a confiança é construída aos poucos, então julgamos prudente aplicar a confiança generalizada para iniciarmos o processo de construção da confiança no Trustee, pois nela o nível de prejuízo do Trustor é baixo. Com isso, podemos saber através de pequenas doses de confiança se o Trustee é ou não confiável.

4.4.4. Gerenciamento de confiança

Conforme [øsang:2005], gerenciamento de confiança é a atividade de criação de sistemas e métodos que permitem com que partes confiantes possam fazer avaliações e tomar decisões a respeito da confiabilidade das transações que envolvem alguns potenciais riscos, viabilizando igualmente que os usuários e proprietários do sistema possam aumentar e representar corretamente a confiabilidade de si mesmos e de seus sistemas.

Neisse [Neisse 2012] classifica o gerenciamento de confiança em 3 partes, senão vejamos:

1. Autorização e autenticação distribuída: valores de confiança associados a identidades e credenciais são computadores em um sistema distribuído e utilizam juntos um conjunto de regras para decidir se as ações solicitadas pelos assuntos devem ser autorizadas ou negadas;

2. Medições de reputação e confiabilidade: valores de confiança com foco em aspectos específicos são calculados com base em experiências diretas ou indiretamente, através de recomendações de terceiros. Estes valores de confiança são utilizados para apoiar a seleção de entidades, serviços ou produtos;
3. Atestando e checando a integridade, utilizando a prova de alteração do hardware: utiliza soluções técnicas que são, teoricamente, ou praticamente comprovadas seguras, tais como, Chips de computação confiável (*Trusted Platform Module* (TPM)) e soluções de cartões inteligentes.

5. Trabalhos Relacionados

No que diz respeito à literatura especializada, o termo confiança é abordado a partir de três perspectivas distintas, quais sejam: *(i) Técnico*: que se refere à segurança proporcionada por um sistema de criptografia; *(ii) Informacional*: pertinente às definições e sentidos atrelados à confiança no mapeamento do sistema; *(iii) Social*: relativo à compreensão do usuário acerca do sistema. [Berendt et al. 2005]. Nossa qualificação tem por objeto temático o nível informativo de confiança.

Neisse et al. [Neisse et al. 2008] propõe um método para mensurar o nível de confiança em SSC, baseado no *feedback* do usuário, ou seja, *feedback* positivo e negativo em relação à adaptação de serviços sensíveis ao contexto, os quais são enviados aos provedores de contexto, que, por sua vez, influenciarão diretamente no comportamento da aplicação. O *feedback* positivo é nomeado como ”honesto, competente ou confiável”. Já o *feedback* negativo, como ”desonesto, incompetente ou não confiável”.

Uma dos principais problemas deste método é que para cada interação com um serviço sensível ao contexto, o sistema deve coletar o *feedback* dos usuários, para que haja a análise da confiança dos provedores de contexto, reduzindo, assim, a transparência e a adaptação do sistema sensível ao contexto ao ambiente.

Um outro estudo acerca da definição e gerenciamento da confiança em sistemas sensíveis ao contexto foi feito por Daskapan et al. [Neisse et al. 2006]. Seu principal alvo é o aspecto da privacidade e o provimento de um modelo heurístico para avaliar a confiança dos consumidores de informações contextuais, a fim de influenciar as decisões de politicas de privacidade do usuário.

Se a confiança é definida em um determinado nível, há uma necessidade do consentimento do usuário para confirmá-la. Caso não haja tal confirmação, o provedor decide automaticamente em nome do usuário se as informações de contexto devem ou não ser fornecidas, embasado no valor de confiança calculado. Daskapan et al. [Neisse et al. 2006] define confiança como uma função de experiências anteriores e a probabilidade da desconfiança no Trustee.

Apesar de o *Pervasive Trust Model* (PTM) de Almenárez et al. [árez04ptm:a] não possuir o foco em sistemas sensíveis ao contexto, tem-se que aborda o gerenciamento da confiança através das interações diretas e indiretas, ou seja, pelo conhecimento prévio das entidades envolvidas e com base em recomendações de terceiros. O nível de confiança final é calculado por intermédio da média das interações diretas e apenas as recomendações confiáveis.

6. Conclusão

Constata-se, atualmente, um crescimento significativo na utilização de aplicações Ubíquas, o qual resultou na mudança das atividades diárias das pessoas. Aplicações para ambientes ubíquos obrigam-se a atender um conjunto de novos desafios, tal como a capacidade da aplicação se adaptar ao ambiente do usuário, ou seja, torná-las sensíveis ao contexto. Uma das proposta iniciais do projeto *MobileHealthNet* é reduzir o esforço no desenvolvimento de aplicações desse tipo.

Aplicações sensíveis ao contexto necessitam de qualidade em suas informações, principalmente as que são voltadas ao domínio da saúde, pois que serão cruciais para a tomada de decisão dos profissional da saúde em relação ao acompanhamento de pacientes. Visto isso, a implementação de parâmetros de QoC tornou-se essencial na infraestrutura do projeto.

Um dos grandes desafios do projeto é implementar o nível de confiança em cada entidade do sistema, ou seja, aplicar um um parâmetro de QoC denominado *Trustworthiness*. Apesar de ser considerado um parâmetro de QoC, [Neisse 2012] afirma que não existem muitas soluções na literatura sobre modelagem de QoC, que tenham como foco a confiança.

Uma das contribuições deste trabalho foi a implementação de provedores de contexto na infraestrutura do projeto - específicos da saúde -, tais como o provedor de frequência cardíaca, frequência respiratória, temperatura corporal e posição. Já fora realizado um levantamento bibliográfico para auxiliar na criação de um modelo matemático e computacional da nossa proposta.

7. Cronograma

O cumprimento dos objetivos a serem trabalhados para a execução da Dissertação segue o seguinte cronograma:

1. Aquisição da fundamentação teórica sobre sistemas cientes de contexto e QoC
2. Estudo do DDS / MobileHealthNet
3. Levantamento do estado da arte sobre sistemas de computação móvel para área da saúde que utilizam dados de contexto e QoC
4. Desenvolvimento de provedores de contexto para: frequência cardíaca, frequência respiratória, temperatura corporal e posição
5. Projeto do suporte ao trustworthiness no middelware MobileHealthNet
6. Implementação do suporte ao trustworthiness no middelware MobileHealthNet
7. Testes e avaliação de desempenho do suporte ao trustworthiness no middelware MobileHealthNet
8. Escrita da dissertação: introdução e fundamentação teórica (redes sociais móveis)
9. Escrita da dissertação: fundamentação teórica (sistemas cientes de contexto)
10. Escrita da dissertação: Mecanismos de QoC para o middelware MobileHealthNet
11. Escrita da dissertação: Avaliação do parâmetro de QoC trustworthiness no middleware MobileHealthNet
12. Escrita da dissertação: conclusões
13. Escrita de artigo científico
14. Depósito da dissertação
15. Defesa da dissertação

	2014												**2015**
Etapas	**Jan**	**Fev**	**Mar**	**Abr**	**Mai**	**Jun**	**Jul**	**Ago**	**Set**	**Out**	**Nov**	**Dez**	**Jan**
1	**x**												
2		**x**											
3			**x**										
4			**x**	**x**	**x**								
5						**x**	**x**	**x**					
6								**x**					
7									**x**	**x**			
8							**x**						
9								**x**					
10									**x**				
11										**x**			
12										**x**	**x**		
13										**x**	**x**		
14												**x**	
15													**x**

Referências

[Web 1999] (1999). *The measurement, instrumentation, and sensors handbook*. Berlin: Springer.

[Rus 2002] (2002). *Trust and Trustworthiness*. Series on Trust.

[Ist 2006] (2006). *M-Health: Emerging Mobile Health Systems*. Springer Science Business Media, Inc., 233 Spring Street, New York, NY 10013, USA.

[Ari 2013] (2013). *Redes Sociais Moveis: Conceitos, Aplicações e Aspectos de Segurança e Privacidade*, chapter 2.

[Adams et al. 2008] Adams, B., Phung, D. Q., and Venkatesh, S. (2008). Sensing and using social context. *TOMCCAP*, 5(2).

[Baldauf et al. 2007] Baldauf, M., Dustdar, S., and Rosenberg, F. (2007). A survey on context-aware systems. *Int. J. Ad Hoc Ubiquitous Comput.*, 2(4):263–277.

[BATISTA 2013] BATISTA, R. C. (2013). Uma infraestrutura de comunicacao centrada em dados para redes sociais moveis. Mestrado, LSD, Universidade Federal do Maranhão.

[Berendt et al. 2005] Berendt, B., Günther, O., and Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. *Commun. ACM*, 48(4):101–106.

[Bezemer 2005] Bezemer, D. (2005). Bart nooteboom, trust. forms, foundations, functions, failures and figures, edward elgar, cheltenham, uk, and northhampton, ma, usa, 2002, xii + 231 pages, with tables and figures, hardback $95, paperback25$, isbn 1 86064 545 8.elias khalil (ed.), trust, series 'critical studies in economic institutions', edward elgar, cheltenham, uk, and northhampton, ma, usa, 2003, xxxii + 772 pages, with tables and figures, hardback $300, isbn184064737x. Journal of Behavioral and Experimental Economics (formerly The Journal o$ $421 - -424.$

[Bolchini et al. 2009] Bolchini, C., Curino, C., Orsi, G., Quintarelli, E., Rossato, R., Schreiber, F. A., and Tanca, L. (2009). And what can context do for data? *Commun. ACM*, 52(11):136–140.

[Buchholz and Schiffers 2003] Buchholz, T. and Schiffers, M. (2003). Quality of context: What it is and why we need it. In *In Proceedings of the 10th Workshop of the OpenView University Association: OVUA'03*.

[Chen and Kotz 2002] Chen, G. and Kotz, D. (2002). Solar: A pervasive-computing infrastructure for context-aware mobile applications. Technical Report TR2002-421, Dartmouth College.

[David et al. 2012] David, L., Vasconcelos, R., Alves, L., Andre, R., Baptista, G., and Endler, M. (2012). A communication middleware for scalable real-time mobile collaboration. In *Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2012 IEEE 21st International Workshop on*, pages 54–59.

[Dey 2001] Dey, A. K. (2001). Understanding and using context. *Personal Ubiquitous Comput.*, 5(1):4–7.

[Huebscher and McCann 2004] Huebscher, M. C. and McCann, J. A. (2004). Adaptive middleware for context-aware applications in smart-homes. In *Proceedings of the 2Nd*

Workshop on Middleware for Pervasive and Ad-hoc Computing, MPAC '04, pages 111–116, New York, NY, USA. ACM.

[Karam and Mohamed 2012] Karam, A. and Mohamed, N. (2012). Middleware for mobile social networks: A survey. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 1482–1490.

[Krause and Hochstatter 2005] Krause, M. and Hochstatter, I. (2005). Challenges in modelling and using quality of context (qoc). In Magedanz, T., Karmouch, A., Pierre, S., and Venieris, I., editors, *Mobility Aware Technologies and Applications*, volume 3744 of *Lecture Notes in Computer Science*, pages 324–333. Springer Berlin Heidelberg.

[Ling 2008] Ling (2008).

[Lubke et al. 2011] Lubke, R., Schuster, D., and Schill, A. (2011). Mobilisgroups: Location-based group formation in mobile social networks. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on*, pages 502–507.

[Malcher et al.] Malcher, M., Aquino, J., Fonseca, H., David, L., Valeriano, A., and Endler, M. A middleware supporting adaptive and location-aware mobile collaboration. In *Mobile Context Workshop: Capabilities, Challenges and Applications, Adjunct Proceedings of UbiComp*.

[Manzoor 2010] Manzoor, A. (2010). *Quality of context in pervasive systems: models, techniques, and applications*. PhD thesis, Computer Science.

[Manzoor et al. 2011] Manzoor, A., Truong, H.-L., and Dustdar, S. (2011). Quality of context: Models and applications for context-aware systems in pervasive environments. *The Knowledge Engineering Review, Special Issue on Web and Mobile Information Services*.

[Neisse 2012] Neisse, R. (2012). *Trust and privacy management support for context-aware service platforms*. PhD thesis, University of Twente, Enschede.

[Neisse et al. 2006] Neisse, R., Wegdam, M., and van Sinderen, M. (2006). Context-aware trust domains. In *Proceedings of the First European Conference on Smart Sensing and Context*, EuroSSC'06, pages 234–237, Berlin, Heidelberg. Springer-Verlag.

[Neisse et al. 2008] Neisse, R., Wegdam, M., and van Sinderen, M. (2008). Trustworthiness and quality of context information. In *9th International Conference for Young Computer Scientists, ICYCS 2008*, pages 1925–1931, Los Alamitos, CA, USA. IEEE Computer Society Press.

[Pinheiro 2014] Pinheiro, D. N. (2014). Mhncs: Um middleware para o desenvolvimento de aplicacoes moveis cientes de contexto com requisitos de qoc. Master's thesis, Universidade Federal do Maranhão.

[Sheikh et al. 2007] Sheikh, K., Wegdam, M., and van Sinderen, M. (2007). Middleware support for quality of context in pervasive context-aware systems. In *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2007*, pages 461–466. IEEE Computer Society Press.

[Smith 1976] Smith, C. O. (1976). *Introduction to reliability in design*. New York : McGraw-Hill. Includes index.

[Stark 2014] Stark, J. E. (2014). Trust in distributed computing. Master's thesis, The University of Guelph.

[Teles et al. 2013] Teles, A., da Silva e Silva, F. J., and Batista, R. (2013). *Security and Privacy in Mobile Social Networks*. Lecture Notes in Social Networks. Security and Privacy Preserving in Social Networks, Springer.

[Weiser 1991] Weiser, M. (1991). The computer for the twenty-first century. *Scientific American*, 9:94–100.