Context-Aware Trustworthy Service Evaluation and Recommendation in Social Internet of Things

By

Maryam Khani

Supervised by: A/Prof. Yan Wang

A thesis submitted to Macquarie University
for the degree of Master of Research
Department of Computing
June 2018

Examiner's Copy

Typeset in LaTeX 2_ε.

Declaration

I certify that the work in this thesis entitled CONTEXT-AWARE TRUSTWORTHY SERVICE EVALUATION AND RECOMMENDATION IN SOCIAL INTERNET OF THINGS has not previously been submitted for a degree nor has it been submitted as part of the requirements for a degree to any other university or institution other than Macquarie University. I also certify that the thesis is an original piece of research and it has been written by me. Any help and assistance that I have received in my research work and the preparation of the thesis itself have been appropriately acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Maryam Khani

Acknowledgements

First and foremost, I would like to express my sincere appreciation to my supervisor, A/Prof. Yan Wang, who supported me throughout my thesis. In addition, I would like to express my deepest appreciation to him for his kindness and patience. He has always helped to put me on the right direction during my studies, not only with his knowledge and experience, but also with attitude for high quality of research. Literally, without his continuous support and endless guidance, this work would not have been possible for me. It is my great fortune to have him as my supervisor at Macquarie University.

I am also thankful to the admirable staff in the Department of Computing for their administrative help. I would like to highly appreciate Macquarie University for International Macquarie University Research Excellence Scholarship (iMQRES) to make me accomplished my thesis.

I would like to thank Dr. Keith Imrie who proofread my thesis and suggested some improvement to English expression.

More importantly, I would like to thank my family, my parents, Abolghasem Khani and Tahereh Yousefi who have always been there for me. Their love, support and encouragement have been the foundation during whole my life. Without their love, unwavering support and inspiration, this work could never have been accomplished.

Abstract

In Social Internet of Things (SIoT) environments, to share SIoT-based services, a large number of users and Internet of Things (IoT) based devices are connected to each other. IoT-based devices establish social relations with each other according to the social relations of their owners in Online Social Networks (OSNs). In such an environment, a big challenge is how to provide trustworthy service evaluation and recommendation. Currently, the prevalent trust management mechanisms employ QoS-based trust and social-relation based trust to evaluate the trustworthiness of service providers. However, the existing trust management mechanisms in SIoT environments do not consider the different contexts of trust. Therefore, dishonest SIoT devices, based on their owners' social relations, can succeed in advertising low-quality services or exploiting maliciously provided services.

In this thesis, we first propose three contexts of trust in SIoT environments including status and the environment of devices, and the task type. The experiments demonstrate that our models can select the most trustworthy services with high quality and recommend them with high accuracy to service-consuming devices.

Contents

List of Figures

List of Tables

List Abbreviation

TABLE 1: Notations used in Chapter 1 and 2

Abstract	**Representation**	**First occurrence**
SIoT	Social Internet of Things	Section 1.1
IoT	Internet of Things	Section 1.1
OSNs	Online Social Networks	Section 1.1
P2P	Peer-to-Peer	Section 1.1
QoS	Quality of Service	Section 1.1
TC	Trust Composition	Section 2.1
TF	Trust Formation	Section 2.1
TU	Trust Update	Section 2.1
TP	Trust Propagation	Section 2.1
TA	Trust Aggregation	Section 2.1
SPA	Self-Promoting Attacks	Section 2.1
BMA	Bad-Mouthing Attacks	Section 2.1
BSA	Ballot-Stuffing Attacks	Section 2.1
OOA	On-Off Attacks	Section 2.1

TABLE 2: Notations used in Chapter 2 (continued)

MDT	Multi-Dimensional Trust	Section 2.3.1
CAT	Context-Aware Trust	Section 2.3.1
MF	Matrix Factorization	Section 2.3.2
CMF	Context-aware Matrix Factorization	Section 2.3.2
CSL	Contextual Sparse Liner	Section 2.3.2
CSL_MCS	CSL with Multidimensional-Context Similarity	Section 2.3.2

TABLE 3: Notations used in Chapter 3

Abstract	**Representation**	**First occurrence**
M	number of devices	Section 3.1
N	number of users	Section 3.1
d_i	device with index i	Section 3.1
u_i	user with index i	Section 3.1
t_i	time	Section 3.1
l_i	location	Section 3.1
s	service	Section 3.1
SC	set of all Service-Consuming devices	Section 3.1
SP	set of all Service-Providing devices	Section 3.1
SC_i	Service-Consuming device i	Section 3.1
SP_j	Service-Providing device j	Section 3.1
R_k	Service Recommender device k	Section 3.1
C_S	Context of Status of device	Section 3.2
C_E	Context of Environment (time and location) of device	Section 3.2
C_T	Context of Task type	Section 3.2

TABLE 4: Notations used in Chapter 3 (continued)

Abstract	Representation	First occurrence
$Variance^{C_S,C_E,C_T}_{SC_i \to SP_j}(K)$	Variance of Contextual Feedback of Trust SC_i toward SP_j at status and environment contexts of device and the task type context in its K latest transactions	Section 3.3.2
$Variance^{C_S,C_E,C_T}_{SP_j \to SC_i}(K)$	Variance of Contextual Feedback of Trust SP_j toward SC_i at status and environment contexts of device and the task type context in its K latest transactions	Section 3.3.2
$ExQoS$	Expected Quality of Service	Section 3.3.1
$\overrightarrow{ExQoS}^{C_S,C_E}_{SCi}$	Expected Quality of Service is requested by a service-consuming device i at status and environment contexts of device	Section 3.3.1
$AdQoS$	Advertised Quality of Service	Section 3.3.1
$\overrightarrow{AdQoS}^{C_S,C_E}_{SP_j}$	Advertised Quality of Service provided by service-providing device j at status and environment contexts of device	Section 3.3.1
$SSimFre^{C_T}_{SC_i,SP_j}$	Social Similarity Friendship between the user of a service-consuming device i and the user of a service-providing device j at the task type context	Section 3.3.2
$SSimCom^{C_T}_{SC_i,SP_j}$	Social Similarity Community between the user of a service-consuming device i and the user of a service-providing device j at the task type context	Section 3.3.2
$SSimR^{C_T}_{SC_i,SP_j}$	Social Similarity Relation between a service-providing device j with a service-consuming device i at the task type context	Section 3.3.2
CFT	Contextual Feedback of Trust	Section 3.3.2
$CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}(n-1)$	Contextual Feedback of Trust indicates the previous direct feedback of a service-providing device j toward a service-consuming device i at status and environment contexts of device and the task type context	Section 3.3.2

TABLE 5: Notations used in in Chapter 3 (continued)

Abstract	Representation	First occurrence
$CFT^{C_S,C_E,C_T}_{SC_i \to SP_j}(n-1)$	Contextual Feedback of Trust indicates the previous direct feedback of a service-consuming device i toward a service-providing device j at status and environment contexts of device and the task type context	Section 3.3.2
K	K latest transactions of a device	Section 3.3.2
n	number of transaction between a SC_i and a SP_j	Section 3.3.2

TABLE 6: Notations used in Chapter 4

Abstract	Representation	First occurrence
δ	weight parameter $(0 \leq \delta \leq 1)$	Section 4.2
w_1, w_2, w_2	the normalized weight parameters	Section 4.1.1.1
σ	weight parameter $(0 \leq \sigma \leq 1)$	Section 4.1.1.2
MCTSM	Mutual Context-aware Trustworthy Service Management	Section 4.1
MCTSE	Mutual Context-aware Trustworthy Service Evaluation	Section 4.2
MCTSR	Mutual Context-aware Trustworthy Service Recommendation	Section 4.3

TABLE 7: Notations used in Chapter 4 (continued)

Abstract	Representation	First occurrence
$T^{C_S,C_T,C_E}_{SC_i \to SP_j}$	overall Trust Value is computed by SC_i toward SP_j at status and environment contexts of device and the task type context	Section 4.1.1.2
$T^{C_S,C_T,C_E}_{SP_j \to SC_i}$	overall Trust Value is computed by SP_j toward SC_i at status and environment contexts of device and the task type context	Section 4.1.1.2
$MCTSE^{C_S,C_E,C_T}_{SC_i \to SP_j}$	Mutual Context-aware Trustworthy Service Evaluation from service-consuming device i toward service-providing j at status and environment contexts of device and the task type context	Section 4.2
$MCTSE^{C_S,C_T}_{SP_j \to SC_i}$	Mutual Context-aware Trustworthy Service Evaluation from service-providing device j toward service-consuming i at status and environment contexts of device and the task type context	Section 4.2
$MCTR^{C_S,C_T,C_E}_{SC_i \to SP_j}$	Mutual Context-aware Trustworthy Service Recommendation from service-consuming device i toward service-providing j at status and environment contexts of device and the task type context	Section 4.3
$MCTR^{C_S,C_T,C_E}_{SP_j \to SC_i}$	Mutual Context-aware Trustworthy Service Recommendation from service-providing device j toward service-consuming i at status and environment contexts of device and the task type context	Section 4.3
CQoSSTrust	Context-aware QoS Similarity base Trust	Section 4.1.1.1
$CQoSSTrust^{C_S,C_E}_{SC_i,SP_j}$	Context-aware QoS Similarity base Trust between a SC_i and a SP_j at status and environment contexts of device	Section 4.1.1.1

TABLE 8: Notations used in Chapter 4 (continued)

Abstract	Representation	First occurrence
CSSTrust	Context-aware Social Similarity based Trust	Section 4.1.1.1
$CSSTrust^{C_T}_{SC_i,SP_j}$	Context-aware Social Similarity based Trust between a SC_i and a SP_j at the task type context	Section 4.1.1.1
CSim	Context Similarity	Section 4.1.1.1
$CSim(C^{S,E}_{SC_i \to SP_j}, C^{S,E}_{R_k \to SP_j})$	*Context Similarity* which indicates the degree of similarity between the status and environment contexts of device of service-consuming device i ($C^{S,E}_{SC_i \to SP_j}$) and recommender k ($C^{S,E}_{R_k \to SP_j}$) towards service-providing device j	Section 4.1.1.1
$CSim(C^{S,E}_{SP_j \to SC_i}, C^{S,E}_{R_k \to SC_i})$	*Context Similarity* which indicates the degree of context similarity between the status and environment contexts of device of service-providing device j ($C^{S,E}_{SP_j \to SC_i}$) and recommender k ($C^{S,E}_{R_k \to SC_i}$) towards service-consuming device i	Section 4.1.1.1

TABLE 9: Notations used in Chapter 5

Abstract	Representation	First occurrence
MAE	Minimum Absolute Error	Section 5.2
$MCTSM^{C_S}$	MCTSM only considering single context of status of device	Section 5.2
$MCTSM^{C_E}$	MCTSM only considering single context of environment of device	Section 5.2
$MCTSM^{C_T}$	MCTSM only considering single context of task type	Section 5.2
$MCTSM^{SFT}$	MCTSM which Simple Feedback of Trust	Section 5.2

1

Introduction

In recent years, a combination of the Internet of Things (IoT) and Online Social Networks (OSNs) has led to the Social Internet of Things (SIoT) to facilitate the discovery, selection, and composition of services provided by distributed IoT based things [1–5]. Those things include personal devices (*e.g.*, smartphones, tablets), devices fitted with tags (*e.g.*, RFIDs) in our environment, sensors and actuators [4]. In SIoT environments, a device with a specific owner requests services from or provides services to other devices and establishes social relations with other devices based on social rules determined by their owners in an autonomous manner by considering their owners' social networks [1, 2, 6–8]. Then, the devices can exchange their friend lists with each other [1, 2]. Moreover, devices may establish different types of *social relations* with each other including ownership (devices belonging to the same user), co-work (devices collaborating to provide common services), co-location (devices that are always used in the same place), parental (devices belonging to the same manufacturers) and social device relations (devices coming into contact continuously) [1–3].

Nowadays, a broad range of Social Internet of Things (SIoT) based applications have emerged [1], such as smart traffic management [9], smart airport [10], smart home [11, 12], *etc.* To find the right source of information in such an SIoT environment, users devices can connect with other devices which are acquired by means of co-location relations. However, devices can be either honest, providing good quality services, or deliberately dishonest, providing poor quality services. Dishonest devices may perform malicious trust-related attacks, such as *Bad-Mouthing Attacks* (BMA), *Ballot-Stuffing Attacks* (BSA), *Self-Promoting Attacks* (SPA), and *On-Off Attacks* (OOA) [13–19]. In such uncertain situations, the issue of trust management in SIoT environments arises and becomes prominent. The first reason for this is that, when a service-consuming device looks for its needed service, some service-providing devices may behave dishonestly and provide low-quality services for their own benefit [20]. The second reason is that the resources of a service-providing device could be maliciously exploited by some dishonest service-consuming devices [21]. The third reason is that dishonest devices may perform trust-related attacks to ruin the reputation of other devices by reputation attacks (BMA and BSA) or to boost their importance by self-interest attacks (SPA and OOA). Therefore, a reliable SIoT environment needs to be built based on an effective trust management mechanism for selecting trustworthy service-providing devices and trustworthy service-consuming devices [22].

1.1 Background and Problem

A variety of trust evaluation and trust recommendation approaches (non-context-aware and context-aware) have been proposed in Service-Oriented applications (*e.g.*, Peer-to-Peer (P2P), online E-commerce, *etc.* [23–30]). However, these approaches are more concerned with trust evaluation and recommendation in service-oriented networks without considering the social relation between service provider and service consumer. Moreover, a variety of context-aware trust evaluation and trust recommendation approaches have been proposed in Online Social Networks (OSNs) [31–37]. These approaches are more concerned with trust evaluation of social participants by considering the social contexts between them. However, they do not consider social relations among devices and the features of Internet of Things (IoT) service computing environments. Furthermore, the existing trust management approaches in IoT [20, 38–42] only consider QoS (Quality of Service) trust metrics, without considering the social relations between devices, which are very important characteristics of SIoT environments.

To select trustworthy service-providing devices or service-consuming devices, a variety of trust service evaluation and trust service recommendation approaches have been proposed in SIoT environments [9, 16–18, 21, 41, 43–47]. To date, SIoT trust management systems use direct evidence, such as QoS-based trust, and indirect experiences, such as social relation based trust, to evaluate trust level of the service-providing devices or the service-consuming devices. Though such trust evaluation mechanisms are applied for indicating a device's trustworthiness in many studies, they do not consider the different contexts of devices (*e.g.,* status and environment) and the types of tasks. Therefore, they cannot ultimately select the most trustworthy service-providing devices or trustworthy service-consuming devices. Moreover, they cannot determine the priority of trustworthy devices to provide the requested service if there are some provided services with the same scenarios and the same social relations. Therefore, they need to be able to differentiate honest and dishonest devices more accurately.

1.2 Motivation

Now let us introduce a motivating example. There are different SIoT-based communities and IoT social networks, and users can register their IoT-based devices to these communities and networks to use different SIoT-based services [1, 2]. **Example 1**: Suppose that users A, B and C register their IoT-based devices (*e.g.*, smartphone, tablet , *etc.*) in the same SIoT-based communities. Then, suppose that the smartphone of user *A*, with low battery, is automatically searching to find the nearest devices to delegate the task of recording an on-line video from an important event. For example, user *B* is on the way to leave the place where user *A* is while user *B* has a smartphone, with a low battery, and user *C* is on the way to reach the place where user *A* is, while user *C* has a tablet with full battery. While the devices of users *B* and *C* provide the same services and have the same social relations with those of user A, the tablet of user *C* is more trustworthy when the status and environment (time and location) of devices are considered. However, the existing trust evaluation mechanisms cannot differentiate user *B*'s device and user *C*'s device in such a context because they do not consider devices' trustworthiness in different contexts, such as the status, the environment, and the task type context [13, 14].

Example 2: Suppose that the smartphones of users A and B are registered in the same SIoT-based Cloud Service community, and also the smartphone of user A and the tablet of user

C are registered in the same SIoT-based Health community. Therefore, the smartphone of user A can trust to the smartphone of user B for the task types like finding a storage place, and can trust to the tablet of user C for the task types like detecting the degree of air pollution. However, the existing trust evaluation mechanisms do not consider devices' trustworthiness in different contexts, such as the task type [13, 14].

In the literature, the existing trust studies only consider a service-providing device's single context, such as a service context. Therefore, they cannot determine the priority of trustworthy devices to provide the requested service if there are some provided services in the same environment (time and location) but with different the status of devices or different social relations between their owners. Therefore, in different scenarios, they need to be able to differentiate honest and dishonest devices more accurately.

but a multi-contextual model may be more accurate to evaluate each device. Moreover, none of the existing studies considers the contextual similarity between the owners of service-consuming devices and service recommenders to receive the most proper recommendations.

1.3 Contributions

To overcome the above-mentioned drawbacks, this thesis proposes a context-aware trustworthy service evaluation and recommendation model for SIoT environments. The characteristics and contributions of our proposed model are summarised as follows:

1. We propose a Mutual Context-aware Trustworthy Service Management (MCTSM) model which consists of a Mutual Context-aware Trustworthy Service Evaluation (MCTSE) model and a Mutual Context-aware Trustworthy Service Recommendation (MCTSR) model in SIoT environments for trust enhanced service evaluation and recommendation, respectively. According to the contexts of trust in OSNs and IoT, we first propose a classification of contexts of trust in SIoT environments including the status of devices, environment (time and location) of devices, and the types of tasks. Based on the context of trust in SIoT environments, we propose a Contextual SIoT Trust Model consisting of independent and dependent metrics. Then, we propose Context-aware QoS Similarity based Trust (CQSST) and Context-aware Social Similarity based Trust (CSST) models. CSST is considered as a coefficient to increase or decrease the effect of the CQSST. In

MCTSE, we apply the weighted sum technique among CQSST, CSST, and contextual feedback metrics.

2. Moreover, in MCTSR, we apply a Contextual Sparse Liner method with a Multi-dimensional Context Similarity based modeling (CSL_MCS) between a service-providing device or a service-consuming device and a service recommender. By considering context similarity, our model can generate the more appropriate recommendations.

3. We conduct experiments on simulations of 600 randomly generated service-consuming devices and service-providing devices to evaluate the effectiveness of our model. The experimental results show that our model can outperform three state-of-the-art models effectively in evaluating the trustworthiness of service-providing devices and service-consuming devices. Then, it can differentiate honest and dishonest devices which perform without attacks or with different types of attacks, with high accuracy. Therefore, our model can select the most trustworthy services with high quality and recommend them to service-consuming devices, with high accuracy and with high resiliency against different malicious attacks of dishonest devices.

1.4 Roadmap of the Thesis

This thesis is structured as follows.

Chapter 2 presents a literature review of the basic concepts of trust in SIoT environments as well as an application-based taxonomy of trust evaluation and recommendation and a technique-based taxonomy of context-aware trust evaluation and recommendation.

Chapter 3 first introduces the relation between devices, their owners, and different contexts of trust to clarify the problem. Then, based on proposed contexts of trust in SIoT environments, we propose independent and dependent metrics of contextual trust which affect service evaluation and service recommendation.

Chapter 4 first describes the design components of our proposed MCTSM model, then describes assessing trust between a service-consuming device and a service-providing device. Finally, we present the MCTSE model and the MCTSR model from the perspective of a service-consuming device or a service-providing device.

Chapter 5 introduces the experiments settings to compare our models with state-of-the-art approaches. The results demonstrate that our model can select the most trustworthy services with high quality and can recommend services with high accuracy, outperforming the state-of-the-art approaches.

Chapter 6 concludes the work in this thesis and discusses some directions of future opportunities.

2

Literature Review

Trust is a complicated subject including the belief, competence, truth and reliability between a trustor and a trustee. After recognising its importance, trust management systems have been studied extensively in different application environments such as Service-Oriented applications [23–30], OSNs [31–37, 48], and IoT [38–42]. Moreover, with the fast development of SIoT environments, providing trustworthy service management has become a critical issue [13, 14, 49]. Therefore, it becomes necessary to define a different mechanism of trust evaluation and trust recommendation for both service-providing devices and service-consuming devices [13, 14, 21]. In SIoT environments, an effective trust management system can help both service-providing devices and service-consuming devices obtain the maximum benefit [13, 14, 21]. On the one hand, when a service-consuming device looks for its needed service, some service-providing devices may behave dishonestly and provide low-quality services for their own benefit [20]. On the other hand, the resources of a service-providing device could be maliciously exploited by some dishonest service-consuming devices [21]. Moreover, dishonest devices may perform trust-related attacks to ruin the reputation of other devices or to boost their importance. Therefore, over recent years, the issue of trust in SIoT environments has received much attention from researchers to select trustworthy service-providing devices and trustworthy service-consuming devices [22]. In this chapter, from the perspective of the overview of trust in SIoT environment to specific perspective of context-aware trust evaluation and context-aware trust recommendation, we present a review.

This chapter is organised as follows: Section 2.1 introduces the design components of trust management and related attacks in SIoT environments. Section 2.2 reviews trust evaluation and recommendation models (non-context-aware and context-aware) applied in different application environments including Service-Oriented applications *e.g.,* Peer-to-Peer (P2P), E-commerce, OSNs, IoT, that are related to our work. We then review existing trust management techniques in SIoT studies and compare them. Section 2.3 reviews the existing context-aware trust evaluation and context-aware trust recommendation techniques. Finally, Section 2.4 summaries our work in this chapter.

2.1 Overview of Trust in the Social Internet of Things

In SIoT environments, there are some trust properties including QoS trust properties and social trust properties, and some other trust properties including context-dependent, dynamic, *etc.* [13–15, 41, 50]. QoS trust properties include computational capability, transaction service quality and competence, and social trust properties include relations factor (ownership, co-location, *etc.*), credibility, honesty, similarity and friendship. Beside considering QoS and social trust properties for trust evaluation and recommendation in SIoT environments [13–15], the property of context-dependent trust should be considered, because the trust values of device i towards device j in different contexts are different [13, 14, 41]. In order to have a global picture of trust management in SIoT environments, we first introduce the design components of trust management and some related attacks of trust in SIoT environments.

As the design components of trust management in SIoT environments, there are five design components to evaluate and recommend trust value of devices in SIoT environments [13–15]. These components have been studied by different trust models [16–18, 21, 43, 51, 52], which are described as follows: **(1) Trust Composition (TC)**: TC component includes *OoS Trust* [39, 43] which refers to the performance of an IoT device in providing quality service and *Social Trust* [17, 53] which derives from social relations between the owners of IoT devices.

TABLE 2.1: Trust-related attacks in SIoT environments

Trust-Related Attacks	**Description**
Bad-Mouthing Attacks (BMA)	A dishonest device can ruin the reputation of a well-behaved device to decrease the chance of that device being selected as a service provider.
Ballot-Stuffing Attacks (BSA)	A dishonest device can promote the reputation of a bad device to increase the chance of that bad device being selected as a service provider. Dishonest devices can boost the trust of each other by using this attack.
Self-Promoting Attacks (SPA)	A dishonest device can boost its importance (by providing a good recommendation for itself) to be selected as a service provider, but then provide malfunctioned services.
On-Off Attacks (OOA)	A dishonest device performs bad services on and off randomly to avoid being selected as a low-trust device to effectively perform bad-mouthing and ballot-stuffing attacks.

(2) Trust Formation (TF): The TF component includes *Single-trust* [13, 14], referring to the fact that only one trust property is considered, and *Multi-trust* [13, 14], referring to the fact that multi-trust properties for trust formation are considered. **(3) Trust Update (TU)**: The TU component includes the *Event-Driven* method (after each transaction or event, trust data are updated) and the *Time-Driven* method (trust observations are collected periodically) [51, 54]. **(4) Trust Propagation (TP)**: The TP component includes a *Centralised* manager and *Distributed* manager, in which IoT devices propagate trust observations to other IoT devices they face without using a *Centralised* manager [43, 46]. **(5) Trust Aggregation (TA)**: The TA component refers to the main aggregation techniques investigated to aggregate trust observation, which are classified into *Static-Weighted Sum (SWS)* [43], *Dynamic-Weighted Sum (DWS)* [17], *Bayesian Inference (BI)* [17, 52] and *Fuzzy Logic (FL)* [39]. Moreover, in SIoT environments, establishing, contracting, updating and revoking trust among devices are vital tasks, with the main difficulty related to engagement of dishonest devices. A dishonest device in SIoT environments aims to perform some trust-related attacks which are described in Table 2.1 [13–19].

2.2 Application-based Taxonomy of Trust Evaluation and Recommendation

2.2.1 Trust Models in Service-Oriented Applications

In the studies of trust evaluation, Nitti *et al.* [55] proposed EigenTrust that the objective is to compute the global trust value of a given peer in P2P networks by collecting the local trust values of all peers. Xiong *et al.* [56] proposed PeerTrust, which considers three necessary trust parameters including the total number of transactions, feedback from other peers, and the credibility of the feedback sources. Vu *et al.* [23] proposed a trust model for QoS-based service selection where the trust information is obtained by comparing the advertised service and the delivered service qualities. Chen *et al.* [57] proposed a trustworthy service management in Ad Hoc Networks which considers both social based trust (*e.g.*, intimacy and honesty) and QoS based trust (*e.g.*, energy level and cooperativeness) for trust evaluation. Moreover, Meng *et al.* [26] proposed an attribute vector, which reflects the service provider's abilities in different attributes of service, and a requester's expectation vector, which reflects the quantitative ordered preferences of the requester. Then these vectors are applied for trust evaluation by the requester. However, the issue of peer feedback distribution and the fact that P2P systems are on a dynamic growth are not addressed in the available studies.

In the studies of trust recommendation, Malik *et al.* [25] proposed the RATEWeb model to facilitate trust-oriented service-provider selection by aggregating consumers' ratings. Moreover, Wang *et al.* [58] applied a fuzzy-logic-based method to determine reputation ranks, that differentiates new service providers and old ones. In P2P networks, Dewan *et al.* [59] proposed a model that the past behaviour of the peer is summarised in its digital reputation then it is used to predict the future actions of the peer. For increasing the accuracy of trustworthiness, Can *et al.* [27] proposed three main trust metrics: reputation, service trust, and recommendation trust. Moreover, importance, recentness, and peer-satisfaction parameters are applied to evaluate the trustworthiness of interactions and recommendations.

Though existing trust evaluation and trust recommendation models have been effectively applied in service-oriented applications, they do not share some common features such as considering the social relation between service provider and service consumer. Therefore, they are not directly applicable in SIoT environments.

2.2.2 Trust Models in Online Social Networks (OSNs)

In the studies of trust evaluation in OSNs, some qualitative approaches have been proposed. As a single-context trust evaluation, Kuter *et al.* [31] consider the confidence calculated by a person toward another in FilmTrust, a movie recommendation system, but it is unclear how they calculate this context factor. As multi-context trust evaluation, Liu *et al.* [60] proposed a complex online social network structure with a new concept called "Quality of Trust" to introduce the evaluation of the trustworthiness of a service provider along with a certain social trust path from the service consumer to the service provider.

In the studies of trust recommendation, Wang *et al.* [34] applied contextual social networks which consider contextual information such as social intimacy, expertise in domains, *etc.* to obtain more accurate recommendation results in online social networks. In addition, Ma *et al.* [35] applied social contextual information such as social tags and social networks for item recommendation to provide better recommendations. Zhan *et al.* [36], in online multimedia social networks, used credible feedback of digital contents, a feedback weighting factor, and user share similarity to evaluate a direct or recommended trust between users. Guo *et al.* [37] suggested that both explicit and implicit influence of both ratings and of trust information should be considered to predict the unknown items for users in a recommendation model.

Though context-aware trust evaluation and trust recommendation approaches have been proved to be effective in OSNs, they are not directly applicable in SIoT environments.

2.2.3 Trust Models in Internet of Things (IoT)

In IoT environments, there have been a few studies on trust management models. Sicari *et al.* [40] categorised the security aspects of IoT into three classes: security requirements, privacy, and trust. The categorising of trust remains unclear due to the lack of classification of the listed research activities in an obvious sorting logic. Razzaque *et al.* [42] proposed different architectures of the IoT, the relevant research challenges in communications problems and information gathering problems. However, they did not propose any solution for the treated security and privacy problems. Moreover, Zheng *et al* [41] indicated that trust contains more meanings than security. Trust in IoT is built based on not only security, but also many other important factors such as honesty, goodness, competence, reliability, and ability. Sfar *et al.* [38] reported that trust management systems could be defined as deterministic (includes policy-based mechanism and certificates systems) and non-deterministic (includes recommendation-based, reputation-based systems, prediction-based, and social network based systems). Recently, Chen *et al.* [39] proposed a trust computation model based on fuzzy reputation in IoT systems. For trust composition, QoS trust parameters such as end-to-end packet forwarding ratio, energy consumption, and packet delivery ratio are considered. However, contextual information in both trust evaluation and trust recommendation has not been considered yet.

Those IoT trust management systems share common features with SIoT environments to provide services with different devices. However, the existing studies on trust management in IoT systems do not consider the social aspects of the owners of IoT devices.

2.2.4 Trust Models in Social Internet of Things (SIoT)

In SIoT environments, the existing trust management systems can be broadly categorised into non-contextual methods, single contextual methods (one or two simple contexts are applied to trust evaluation) and multi-context (more complicated contexts are applied to trust evaluation).

As a non-context trust management model, Bao *et al.* [51, 61] consider social relations in trust management for IoT. For trust composition, they consider both QoS trust properties including honesty, cooperativeness, and social trust such as community interest. Therefore, they consider multi-trust properties for trust formation. However, the proposed factors for computing cooperativeness based on the percentage of common friends is very simple. For trust update, propagation and aggregation, they consider both event-driven and time-driven, distributed and static-weighted sum techniques respectively. Moreover, Bao *et al.* in [52] improve the trust management protocol proposed in [51]. However, they use the same measures for social trust evaluation. Chen Z. *et al.* [44] proposed an access service recommendation scheme for effective service composition as well as resistance against malicious attacks. For trust composition, they consider QoS trust metrics such as quality reputation and energy status. Also, social trust is considered by some social similarities. Therefore, they consider multi-trust properties for trust formation. For trust update, propagation and aggregation, they consider both event-driven and time-driven, distributed and static-weighted sum techniques respectively. However, Chen *et al.* did not consider some trust properties such as contextual and dynamic characteristics.

Chen I.R. *et al.* [17] proposed an adaptive and scalable trustworthy service composition in SOA-based IoT systems. For trust composition, they use a QoS trust metric to rate a service provider, and a social trust metric to rate a recommender based on the concept of collaborative filtering. They only apply a single QoS trust to rate a service provider, therefore, they proposed a single-trust property for trust formation. For trust update, propagation and aggregation, they consider both event-driven and time-driven, distributed, Bayesian inference with dynamic-weighted sum techniques respectively. However, the social relations between devices are not considered. In addition, the trust values of all devices owned by the same person are the same, but the different characteristics may influence the trust values differently.

As a single-context trust management model, Nitti *et al.* [43, 46] proposed a trust computation method which considers both direct and indirect trust. For trust composition, QoS based trust (includes transaction service quality and computational capability) and social relation based trust (includes centrality, relation factor) are applied. Therefore, they consider multi-trust properties for trust formation. For trust update, propagation and aggregation, they consider event-driven, both distributed and centralized, and static-weighted sum techniques respectively. In this model, trust is context-dependent but only factors such as the number of transactions in a QoS based trust are considered as a context. In addition, Saied *et al.* [18] proposed a contextual trust computation model which only considers the type of services and node capability as a context. For trust composition, QoS trust is considered as one of the trust metrics by using context information such as service type and device capability (e.g., energy status) to facilitate a service quality rating. Therefore, they only consider QoS trust as a single-trust property for trust formation. For trust update, propagation and aggregation, they consider event-driven, centralized and dynamic-weighted sum techniques respectively. However, they consider simple context without considering context similarity to generate the most proper recommendations. Therefore, their model is a single-context trust. Furthermore, Lin *et al.* [21] proposed a contextual trust management model in which the context consists of two components, task type and environment. They considered different types of environments, for example a hostile environment means that the external condition is unsuitable for the current task, and an amicable environment means that the external condition is suitable for performing the current task. For trust composition, QoS based trust (*e.g.*, bandwidth, packet lost, *etc.*) and social based trust (social relationships, such as friendship) is applied. However, they only consider the task type and the situation of the environment as context and they do not consider different contexts such as time, location, and the features of a device, to be multi-context. Moreover, they do not consider context similarity to generate the most proper recommendations.

Both non-contextual and single-contextual proposed trust management systems in SIoT environments can defend against BMA, BSA, and SPA attacks of dishonest devices. However, these existing trust management systems in SIoT environments can not defend against OOA of dishonest devices. To sum up, the existing trust management systems in SIoT environments have not investigated context-aware (*i.e.* multi-contextual) trust evaluation and recommendation yet. Moreover, context-aware trust models in OSNs cannot be directly applied in SIoT environments because the specific characteristic of trust in SIoT systems includes direct (*e.g.*, QoS-based trust), dynamic, *etc*, which should be considered. In addition, existing trust models in service-oriented applications and IoT environments do not consider the social relation among devices in SIoT environments. In Table 2.2, the MCTSM model is compared with some existing trust management systems in SIoT environments so as to highlight its characteristics and the contributions of our work from the perspective of trust evaluation and trust recommendation.

2.3 Technique-based Taxonomy of Context-Aware Trust Evaluation and Recommendation

2.3.1 Context-Aware Trust Evaluation Approaches

In a *Multi-Faceted Context-Aware* approach, proposed by Griffiths [62], the context trust is assessed through a *Multi-Dimensional Trust (MDT)* model. In this model the contextual trustworthiness of a specific task is calculated in several dimensions (e.g, quality and timeliness). For instance, a web service is evaluated in different QoS contexts, like response time, throughput, and execution time. RATEweb systems [25] apply the same multi-dimensional structure to evaluate the reputation of a seller or a service provider. However, these models overlook the changes of context in previous transactions. Therefore, it is difficult to predict the probability of a successful oncoming transaction. In a *Similarity-based* context-aware approach, the model context is computed, and then the trust value is calculated from one context to another based on their context similarity. As an example, Uddin *et al.* [63] proposed *Context-Aware Trust (CAT)* model that computes the similarity of different contexts by using key values. Moreover, Liu and Datta [64] applied a similarity-context-aware trust model in P2P backup storage systems by describing context in different dimensions to enhance the data availability. However, key values are not appropriate for sophisticated schemes with complex contextual information.

In a *Multi-context Heuristic-Based approach*, a practical model is defined that is easy to understand, while contextual information is considered in trust evaluation. Moreover, Heuristic-Based approaches are proper for systems with a large number of users [65]. Zhang *et al.* [66, 67] proposed the *ReputationPro* trust model which is an heuristic-Based multi-context model applied in large-scale e-commerce applications. Our proposed model in this thesis for context-aware trustworthy service evaluation is typically a multi-context heuristic-based trust evaluation model which outperforms the existing trust evaluation models in SIoT environments due to its mechanisms for dealing with different contexts at a time.

2.3.2 Context-Aware Trust Recommendation Techniques

In this section, we focus on the *Contextual Collaborative Filtering* approach, which is a popular context-aware recommender system [68–71] including independent modeling [72] and dependent modeling [70, 71, 73].

As independent models, in *Tensor Factorization* [74, 75], contexts are considered as additional dimensions in the multidimensional rating space which is not dependent on other dimensions like users. Karatzoglou *et al.* [72] proposed a *Multiverse Recommendation* model by applying Tensor Factorization in which different types of context are considered as additional dimensions which are independent of other dimensions in the representation of the data as a tensor. Zheng *et al.* [76] proposed a contextual modeling probabilistic tensor factorization which integrated ratings, social relations, and contexts to improve the quality of recommendation. However, independent contextual modeling is not usually better than the dependent modeling because of the existence of dependency among users, items, and contexts in the data.

As dependent models, in a *Context-aware Matrix Factorization (CMF)* model [77–79], contextual dependencies are modeled with other dimensions like user. Baltrunas *et al.* [70] improved the rating prediction accuracy by proposing a context-aware recommendation algorithm based on *Matrix Factorization (MF)*. In a *Contextual Sparse Liner (CSL)* method [71, 73], traditional item-based K-nearest-neighbour collaborative filtering [80] is improved by modeling contextual variables for top-N recommendations. Zheng *et al.* [81] proposed a similarity-learning model that is built by integrating a sparse linear recommendation model with context similarity. Generally, dependent models adapt to contextual preferences by modeling contextual information with different contextual modeling such as Multi-dimensional-Context Similarity-based (MCS) modeling. In MCS, a multidimensional space is applied in representing each context variable by a dimension and each context condition will be assigned to a real number value to be placed in a specific position. Zheng *et al.* [81] demonstrated that the CSL method using Multidimensional-Context Similarity (CSL_MCS), is the best performing dependent contextual modeling approach, with the highest precision in comparison with some other contextual recommendation methods. Our proposed model in this thesis for context-aware trustworthy service recommendation is a typical CSL_MCS model to exploit the dependency

TABLE 2.2: The comparison of existing trust management systems

Trust Management System	Design Components of Trust Management	Context-Aware Dependent	Resistant Against Attacks
2012 F. Bao *et al.* [51, 61]	TC: QoS + Social, TF: Multi-trust, TU: Event + Time-driven, TP: Distributed, TA: Static-weighted sum,	NC	SPA, BMA, BSA
2013 F. Bao *et al.* [52]	TC: QoS + Social, TF: Multi-trust, TU: Event + Time-driven, TP: Distributed, TA: Static-weighted sum	NC	SPA, BMA, BSA
2013 Y.B. Saied *et al.* [18]	TC: QoS , TF: Single-trust, TU: Event-driven, TP: Centralised, TA: Dynamic-weighted sum	SC	SPA, BMA, BSA
2014 M. Nitti *et al.* [43]	TC: QoS + Social, TF: Multi-trust, TU: Event-driven, TP: Distributed + Centralised, TA: Static-weighted sum	SC	SPA, BMA, BSA
2015 Z. Chen *et al.* [44]	TC: QoS + Social, TF: Multi-trust, TU: Event + Time-driven, TP: Distributed, TA: Static-weighted sum	NC	SPA, BMA, BSA
2016 I.R. Chen *et al.* [17]	TC: QoS + Social, TF: Single-trust, TU: Event + Time-driven, TP: Distributed, TA: Bayesian inference + Dynamic-weighted sum	NC	SPA, BMA, BSA
2017 Lin *et al.* [21]	TC: QoS + Social, TF: Multi-trust, TU: Event-driven, TP: Distributed, TA: Static-weighted sum	SC	No information
2018 MCTSM	TC: QoS + Social, TF: Multi-trust, TU: Event-driven, TP: Distributed, TA: Static-weighted sum	MC	SPA, BMA, BSA, OOA

Design Components of Trust Management	Context-Aware Dependent	Resistant Against Attacks
TC: **T**rust **C**omposition TF: **T**rust **F**ormation TP: **T**rust **P**ropagation TA: **T**rust **A**ggregation TU: **T**rust **U**pdate	NC: **No C**ontext model SC: **S**ingle-**C**ontext model MC: **M**ulti-**C**ontext model	SPA: **S**elf-**P**romoting **A**ttacks BMA: **B**ad-**M**outhing **A**ttacks BSA: **B**allot- **S**tuffing **A**ttacks OOA: **O**n-**O**ff **A**ttacks

among service-consuming devices or service-providing devices, recommenders and contexts of trust in SIoT environments.

2.4 Conclusion

In this chapter, we first introduced five design components of trust management as well as trust-related attacks in SIoT environments. Second, the typical trust evaluation models have been categorised and reviewed based on different application environments. Finally, we presented a review on context-aware trust evaluation and context-aware trust recommendation approaches for solving our target context-aware trust evaluation and recommendation problem in SIoT environments, and highlighted the contributions of this thesis.

3

Problem Statement and Metrics of Contextual Trust

In SIoT environments, before effectively evaluating and recommending trustworthy devices as service-providing devices or service-consuming devices, a fundamental task is to discover the contexts of trust between devices in SIoT environments. To the best of our knowledge, although a few studies have been proposed on single-context trust evaluation in SIoT environments [18, 21], no existing studies have investigated trustworthy service evaluation and service recommendation based on multiple contexts (multi-context). This chapter proposes multi-context of trust in SIoT environments. Then, based on proposed contexts of trust, we propose metrics of contextual trust which affect service evaluation and service recommendation. In contrast to single-contextual trust evaluation models, we point that the multi-contextual trust evaluation models can provide more accurate results and comprehensive trust information related to a target object. However, multi-contextual trust evaluation models are much more complex [66], and therefore, the contexts of trust should be selected precisely.

This chapter is organized as follows: Section 3.1 introduces the problem statement. Section 3.2 describes the relation between trust and contexts in SIoT environments. We explain how devices and their relations in SIoT environments are bound to contextual information (*e.g.*, status, environment such as location and time, and task type). In Section 3.3, based on the considered contexts of trust in SIoT environments, we propose several metrics of contextual trust including independent and dependent metrics of contextual trust. Finally, Section 3.4 summaries our work in this chapter.

3.1 Problem Statement

In our SIoT modeling, there are M devices which are represented by $D = \{d_1,\ldots, d_M\}$ and there are N users which are represented by $U = \{u_1,\ldots,u_N\}$. Let the social network between users be described by an undirected graph $G = \{U, E\}$, where $E \subseteq U \times U$, and $<u,v> \in E$ means there is a social relation between u and v. Moreover, there are I service-consuming devices and J service-providing devices with considering their owner social relations which are represented by $SC = \{SC_1,\ldots,SC_I\}$ and $SP = \{SP_1,\ldots,SP_J\}$ respectively. Let the vector of SP_i denote a combination of d_i (device i) and u_i (user i). Each SC_i or SP_j can be a service-recommender like R_K that recommends a service-consuming device or a service-providing device to other devices. In addition, each SC_i or SP_j is represented by a vector in a three dimensional space of contexts of trust in SIoT including status (C_S), environment (C_E), and task type (C_T) (see section 3.2) which are represented by $C = \{C_S, C_E, C_T\}$. Each of C_S, C_E, C_T has different values which are presented by $C_S = \{C_{S_1},\ldots,C_{S_h}\}$, $C_E = \{C_{E_1},\ldots,C_{E_h}\}$, and $C_T = \{C_{T_1},\ldots,C_{T_h}\}$ respectively. The vectors of $\overrightarrow{SC}_i$ and $\overrightarrow{SP}_j$ are denoted by Eq. (3.1) and Eq. (3.2) respectively. Each SC_i and SP_j has a list of owner's friends which is denote by $UFre_{SC_i}$ and $UFre_{SP_j}$ respectively and a list of owner's community of interests which is denote by $UCom_{SC_i}$ and $UCom_{SP_j}$ respectively. Also, let $S = \{s_1,\ldots,s_l\}$ denote the set of services which are provided or consumed by devices in different time $\tau = \{t_1,\ldots,t_p\}$, and locations $L = \{l_1,\ldots,l_q\}$. Moreover, each SC_i and SP_j has a user satisfaction level or ground truth [82] which is shown by GT_{SC_i} and GT_{SP_j} respectively. The aim of this thesis is to provide a list of the most trustworthy SP and SC for each SP_i and SC_j respectively in each transaction.

$$\overrightarrow{SC}_i = \begin{bmatrix} C_{S_i} \\ C_{E_i} \\ C_{T_i} \end{bmatrix} \quad (3.1) \qquad \overrightarrow{SP}_j = \begin{bmatrix} C_{S_j} \\ C_{E_j} \\ C_{T_j} \end{bmatrix} \quad (3.2)$$

3.2 The Contexts of Trust in SIoT Environments

In general, devices in IoT environments may trust each other based on different contextual factors including different statuses of devices such as energy, and capability of computing, which provide or request different services at different time and locations. In addition, the owners of devices in a contextual OSNs [34] may trust each other based on common social relations for different types of tasks. For example, suppose that there are two devices d_j and d_k, as service-providing devices, advertising the services requested by device d_i, as the service-consuming device, in an SIoT environment. In this scenario, the QoS based trust value evaluated by d_i for d_j and d_k varies at different time, locations and different statuses of d_j and d_k. These contexts are considered as the contexts of trust in IoT environments as depicted in Fig. 3.1. Moreover, the social relation based trust values evaluated by d_i by considering the common social relations between its owner (u_i) and the owner of d_j (u_j) and d_k (u_k) for different types of tasks. Therefore, the task type context is considered as the context of trust in OSNs which is shown in Fig. 3.2. By considering different contextual aspects between devices in IoT environments and their owners in OSNs, we classify the contexts of trust in SIoT environments in three categories including the status of devices, environment (time and location) of devices, and the types of tasks. Fig. 3.3 depicts the space of the contexts of trust in SIoT environments. In such a space, each device is considered as a service-providing device or a service-consuming device which is shown with a vector. The contexts of trust in SIoT environments are described as follows.

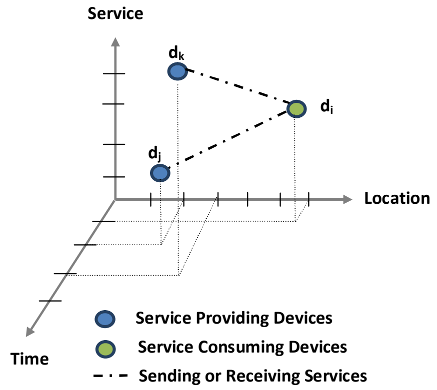


FIGURE 3.1: Contexts of Trust in IoT environments

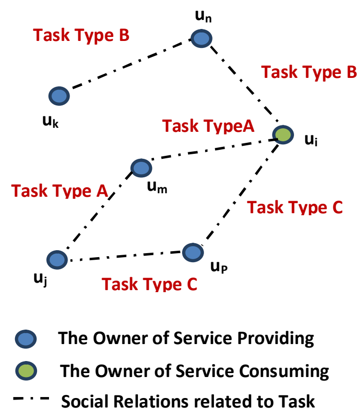


FIGURE 3.2: Contexts of Trust in OSNs environments

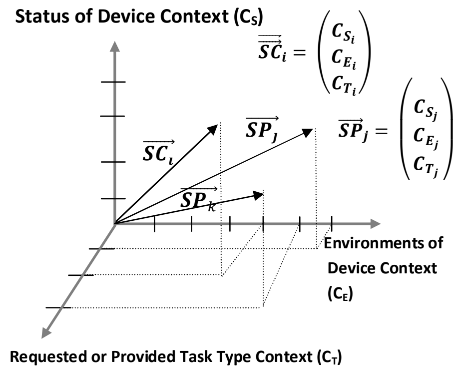


FIGURE 3.3: Contexts of Trust in SIoT environments

- **Status of a device (C_S):** The features of devices such as energy, and the capability of computing.

- **Environment of a device (C_E):** Service-consuming devices and service-providing devices may be located in different locations and may be available in different time (*e.g.*, next 1 hour, next 2 hour, next 3 hour, and *etc.*).

- **Task type (C_T):** For example, a service-consuming device could trust a service-providing device for task type A not for task type B. A task type context which is requested by a service-consuming device could be made by a combination of some services. Here, only two services are considered. For example, the task type of A is a combination of services including S_1 and S_2.

3.3 The Metrics of Contextual Trust Evaluation

Based on the classified contexts of trust in SIoT environments, we propose the following metrics of contextual trust with significant effects on trust evaluation and trust recommendation.

3.3.1 Independent Metrics

Independent metrics of a service-consuming device and a service-providing device in SIoT environments refer to the individual preferences of the service-consuming device and individual capabilities of the service-providing device that has direct influence on contextual QoS based trust evaluation. Moreover, QoS refers to a level of service that is satisfactory to some user requirements including bandwidth, latency (or delay), error rate, availability. The independent metrics include expected QoS and advertised QoS. Each of these parameters is shown with a vector in the two-dimensional space of the status and environment contexts of trust.

- Let $\overrightarrow{\boldsymbol{ExQoS}}^{C_S,C_E}_{SCi}$ denote the *Expected Quality of Service (ExQoS)* that is requested by a service-consuming device i (SC_i) at a specific status and environment contexts (C_S, S_E)

- Let $\overrightarrow{\boldsymbol{AdQoS}}^{C_S,C_E}_{SP_j}$ denote the *Advertised Quality of Service (AdQoS)* that is provided by service-providing device j (SP_j) at a specific status and environment contexts (C_S, S_E). These parameters are depicted by Eq. (3.3) and Eq. (3.4) respectively.

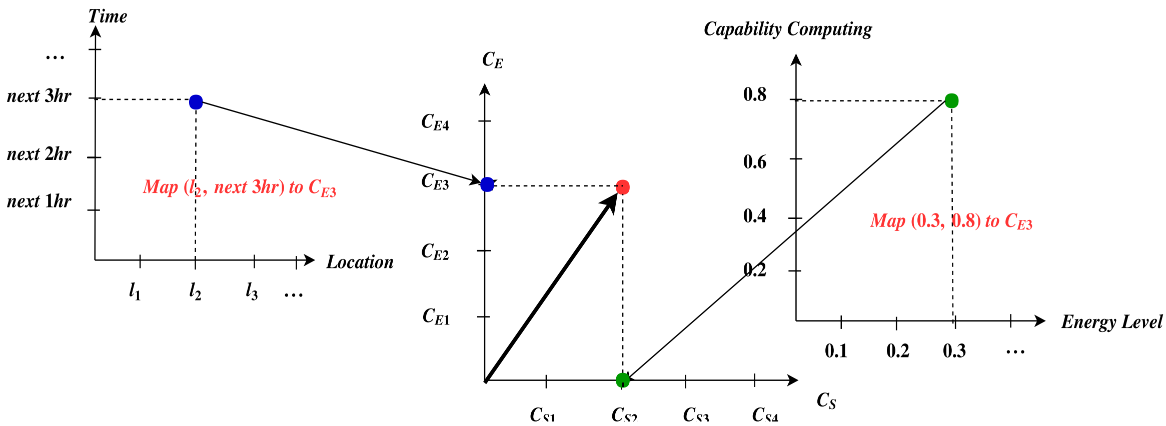


FIGURE 3.4: Example of computing $\overrightarrow{ExQoS}^{C_S,C_E}_{SCi}$ or $\overrightarrow{AdQoS}^{C_S,C_E}_{SP_j}$ in space of status and environment (time and location) contexts of device

$$\overrightarrow{ExQoS}^{C_S,C_E}_{SCi} = \begin{bmatrix} C_{S_j} \\ C_{E_j} \end{bmatrix} \tag{3.3}$$

$$\overrightarrow{AdQoS}^{C_S,C_E}_{SP_j} = \begin{bmatrix} C_{S_i} \\ C_{E_i} \end{bmatrix} \tag{3.4}$$

Example: Fig. (3.4) depicts an example of computing $\overrightarrow{ExQoS}^{C_S,C_E}_{SCi}$ or $\overrightarrow{AdQoS}^{C_S,C_E}_{SP_j}$ in space of status and environment (time and location) contexts of device. There are different context of device including status context such as energy level and capability computing and environment context such as time and location. Moreover, we categorized devices into different capability computing levels. The value of devices like *laptop* and *smart phone* is equal 0.8, *smart gateway* is equal 0.6, *smart camera* is equal 0.4, *sensor* is equal 0.2 [44]. As it shows in the Fig. (3.4), For example, SC_i expect a service that is provided next 3hr at location L_2 with energy 0.3 and capability computing 0.8. Therefore, the values of time and location from the space of environment are mapped to the point C_{E3} as context environment and the values of energy level and compability computing from the space of status to the point C_{S2} as context status. Moreover, QoS advertised by SP_j is computed in the same way in the space of status and environment contexts.

3.3.2 Dependent Metrics

The dependent metrics illustrate the contextual social based trust value between a service-providing device and a service-consuming device, which include social similarity friendship, social similarity community, social similarity relations, and contextual feedback of trust in the task type of context. We consider the fact that the idea of friends has an important effect on the decision of someone. Therefore, the more interests one has with another in a specific task type context the more likely they trust each other in that task type context [34].

- Let $\boldsymbol{SSimFre^{C_T}_{SC_i,SP_j}}$ denote the *Social Similarity Friendship (SSimFre)* and $\boldsymbol{SSimCom^{C_T}_{SC_i,SP_j}}$ denote the *Social Similarity Community (SSimCom)* that provide the degree of the common social friends and the common communities between the user of a service-consuming device i and the user of a service-providing device j respectively which are evaluated by the service-consuming device i based on its direct observations at the task type context. Moreover, We consider the task type in calculating the degree of these social similarity metrics. For example, users A and B are registered in the same Cloud Service community, therefore, they have at least one common community in task type like finding storage place. After two service-providing and service-consuming devices exchange the friend list of their owners [2], $UFre_{SC_i}$ and $UFre_{SP_j}$, they can compute two binary list including $LFre^{C_T}_{SC_i}$ and $LFre^{C_T}_{SP_j}$ where the size of each list is equal with $S_{Fre} = |UFre_{SC_i} \cup UFre_{SP_j}|$. Each element in these lists will be 1 if the corresponding user is in $UFre_{SC_i}$ or ($UFre_{SP_j}$) and has relationship in the specific task type context C_T with SC_i or (SP_j), otherwise 0. If a service-providing device is able to provide two task types, its user will have two separate lists of friends for each task type. Moreover, two service-providing and service-consuming devices exchange the list of community interest of their owners [2], $UCom_{SC_i}$ and $UCom_{SP_j}$. Then, they compute two binary list including $LCom^{C_T}_{SC_i}$ and $LCom^{C_T}_{SP_j}$ where the size of each list is equal with $S_{Com} = |UCom_{SC_i} \cup UCom_{SP_j}|$. Each element in these lists will be 1 if the corresponding community interest is in $UCome_{SC_i}$ or ($UCome_{SP_j}$) and is related to the specific task type context C_T, otherwise 0. The metrics of $SSimFre^{C_T}_{SC_i,SP_j}$ and $SSimCom^{C_T}_{SC_i,SP_j}$ are calculated by Eq. (3.5) and Eq. (3.6) respectively.

$$SSimFre^{C_T}_{SC_i,SP_j} = \frac{LFre^{C_T}_{SC_i}.LFre^{C_T}_{SP_j}}{S_{Fre}} = \frac{\sum_{\acute{h}=1}^{h} LFre^{C_T}_{SC_i}[\acute{h}].LFre^{C_T}_{SP_j}[\acute{h}]}{S_{Fre}} \tag{3.5}$$

$$SSimCom^{C_T}_{SC_i,SP_j} = \frac{LCom^{C_T}_{SC_i}.LCom^{C_T}_{SP_j}}{S_{Com}} = \frac{\sum_{\acute{q}=1}^{q} LCom^{C_T}_{SC_i}[\acute{q}].LCom^{C_T}_{SP_j}[\acute{q}]}{S_{Com}} \tag{3.6}$$

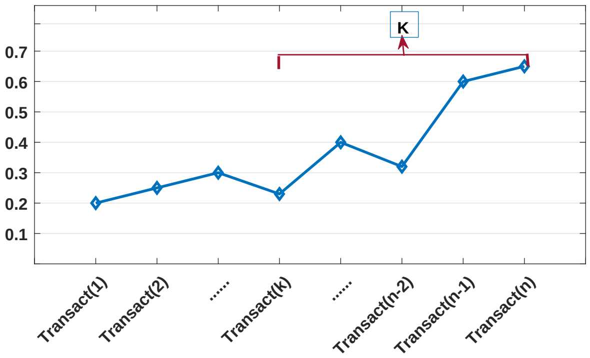
- Let $\boldsymbol{SSimR^{C_T}_{SC_i,SP_j}}$ denote the *Social Similarity Relation (SSimR)* that indicates the degree of common social relations (*e.g.* ownership, co-work, co-location, parental) [1–3, 6–8] between a service-providing device j with a service-consuming device i at task type type context. We consider different weighted values for each device relation form which are listed in Table 3.1. For example, if two devices have the same owner while they provide or request the same type of tasks, the weighted value is equal to 1. If they have the same owner but they provide or request different types of tasks, the weighted value is equal

TABLE 3.1: Social Similarity Relations (SSimR)

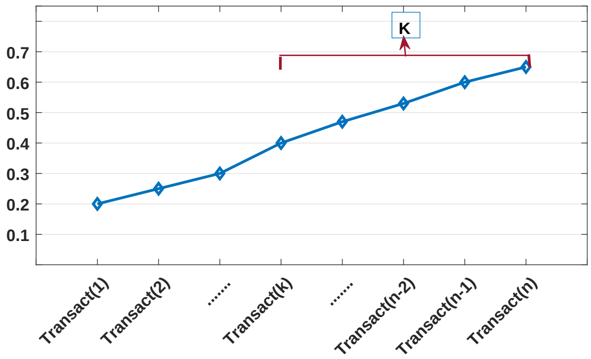
Relationship	Value with C_T	Value without C_T	Description
Ownership	1	0.9	between devices that belong to the same owner
Co-work	0.8	0.7	between devices that collaborative to provide common service
Co-location	0.6	0.5	between devices that are in the same area
Social	0.4	0.3	between devices that continuously interact with each other
Parental	0.2	0.1	between devices that belong to the same production batch

to 0.9. Moreover, if there are different social relations between two devices, only the highest weight is considered.

- Let $\boldsymbol{CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}(n-1)}$ and $\boldsymbol{CFT^{C_S,C_E,C_T}_{SC_i \to SP_j}(n-1)}$ denote the *Contextual Feedback of Trust (CFT)* in the view of SC_i and in the view of SP_j respectively, where n indicates the number of transactions between SC_i and SP_j at status and environment contexts of device and the task type context. $CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}(n-1)$ indicates the previous direct feedback of a service-providing device j toward a service-consuming device i at status and environment contexts of device and the task type context and $CFT^{C_S,C_E,C_T}_{SC_i \to SP_j}(n-1)$ indicates the previous direct feedback of service-consuming device i toward service-providing device j at status and environment contexts of device and the task type context, if there is any direct feedback. Moreover, let $\boldsymbol{Variance^{C_S,C_E,C_T}_{SC_i \to SP_j}(K)}$ indicate the *Variance* of $CFT^{C_S,C_E,C_T}_{SC_i \to SP_j}(n-1)$ in its K latest transactions and let $\boldsymbol{Variance^{C_S,C_E,C_T}_{SP_j \to SC_i}(K)}$ indicate the *Variance* of $CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}(n-1)$ in its K latest transactions. For example, Fig. 3.5 depicts the differentiation of the variance of trust feedback of a dishonest device and an honest device in their previous transactions at a specific status and environment contexts of device and the task type context. In fact, the trend of trust feedback of a dishonest device has more variance in comparison with a honest device. The metrics of $Variance^{C_S,C_E,C_T}_{SC_i \to SP_j}(K)$ and $Variance^{C_S,C_E,C_T}_{SP_j \to SC_i}(K)$ are calculated by Eq. (3.7), Eq. (3.8), Eq. (3.9), and Eq. (3.10). Then, the metrics of $e^{Variance^{C_S,C_E,C_T}_{SC_i \to SP_j}(K)}$ and $e^{Variance^{C_S,C_E,C_T}_{SP_j \to SC_i}(K)}$ have been considered as a coefficient applied to the previous direct feedback of service-providing device in our MCTSM model. Therefore, If there is more variance in K latest transactions of device, means that it was a dishonest device, therefore, its dishonest behaviour is memorized and it decrease the importance of its previous direct feedback. We apply the e^{-x} function where x is equal with the $Variance$ because the more variance in the previous feedbacks, the less the trust value between them. Moreover, the e^{-x} function keeps the value of $Variance$



(a) Trend trust feedback of a dishonest device



(b) Trend trust feedback of an honest device

FIGURE 3.5: Differentiation of the variance of trust feedback of a dishonest device and an honest device in their previous transactions at status and environment contexts of device and the task type context.

between 0 and 1.

$$Variance^{C_S,C_E,C_T}_{SC_i \to SP_j}(K) = \frac{\sum_{x=n-k}^{n} (CFT^{C_S,C_E,C_T}_{SC_i \to SP_j}(x) - \overline{\mathrm{CFT}}^{C_S,C_E,C_T}_{SC_i \to SP_j}(K))^2}{k-1} \tag{3.7}$$

$$Variance^{C_S,C_E,C_T}_{SP_j \to SC_i}(K) = \frac{\sum_{x=n-k}^{n} (CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}(x) - \overline{\mathrm{CFT}}^{C_S,C_E,C_T}_{SP_j \to SC_i}(K))^2}{k-1} \tag{3.8}$$

$$\overline{\mathrm{CFT}}^{C_S,C_E,C_T}_{SC_i \to SP_j}(K) = \frac{\sum_{x=n-k}^{n} CFT^{C_S,C_E,C_T}_{SC_i \to SP_j}(x)}{K} \tag{3.9}$$

$$\overline{\mathrm{CFT}}^{C_S,C_E,C_T}_{SP_j \to SC_i}(K) = \frac{\sum_{x=n-k}^{n} CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}(x)}{K} \tag{3.10}$$

3.4 Conclusion

In this chapter, we first described the relation between devices, their owners, and different contexts of trust to clarify the problem which is selecting the most trustworthy service-providing device and service-consuming device in SIoT environments. Second, we proposed the contexts of trust between devices in SIoT environments by considering different contextual aspects between devices in IoT environments and their owners in OSNs, including *Status of a device*, *Environment of a device*, and *Task Type*. Third, based on considered contexts of trust in SIoT environments, several metrics of contextual trust including the independent and dependent metrics have been proposed. Independent metrics refer to the individual preferences of service-consuming and capability of service-providing devices. Moreover, dependent metrics refer to the contextual social based trust value between a service-providing and service-consuming device. We apply the concepts of our model which described in this chapter for proposing our trust evaluation and trust recommendation models in the next chapter.

4

Mutual Context-aware Trustworthy Service Management in SIoT Environments

Over the past few years, in SIoT environments, researchers have been building various trust evaluation models [9, 16–18, 21, 41, 43–47]. In brief, the basic idea of most existing trust evaluation models is to employ direct evidence(*e.g.*, QoS based trust) and indirect experience (*e.g.*, social relation based trust) to evaluate the trustworthiness of service providers. However, the existing trust management mechanisms in SIoT environments do not consider the different contexts of devices (status and environment) and the types of tasks. Therefore, honest service-consuming and service-providing devices are vulnerable to some attacks from dishonest SIoT devices [13–18]. Moreover, dishonest devices, based on their owners' social relations, can easily succeed in advertising low-quality services or exploiting maliciously provided services or resources for their benefit.

In contrast to the most existing trust management models that compute the trust values of service-providing devices without considering the contexts of trust (non-contextual model)

[17, 44, 51, 52] or with single-trust [18, 21, 43], in Chapter 3 we have proposed different contexts of trust, including the status and environment of the device and task type to compute the trust value of a device. Based on these contexts of trust, we proposed the metrics of contextual trust. This chapter describes a MCTSM model which is designed based on the proposed metrics of contextual trust to assess the trust between a service-consuming device and a service-providing device. The MCTSM model consists of MCTSE model and MCTSR model for trust enhanced service evaluation and recommendation, respectively. Then, we propose the MCTSE model and the MCTSR model from the perspective of a service-consuming device or a service-providing device.

This chapter is organised as follows. Section 4.1 introduces the design components of an MCTSM model to evaluate the trustworthiness of a service-consuming device or a service-providing device. Then, the different steps of trust assessment between service-consuming and service-providing devices in SIoT environments by the MCTSM model are described. Section 4.2 describes the MCTSE model that indicates the trust evaluation between a service-providing device and a service-consuming device. Section 4.3 describes the MCTSR model that indicates the trust recommendation received from the service recommender from the perspective of service-consuming and service-providing devices. Finally, Section 4.4 summaries our work in this chapter.

4.1 Overview of Mutual Context-aware Trustworthy Service Management (MCTSM) Model

4.1.1 Design Components of MCTSM Model

As illustrated in Section 2.1, like the existing trust management systems in SIoT environments [16–18, 21, 43, 51, 52], our proposed MCTSM model consists of five design components, namely Trust Composition (TC), Trust Formation (TF), Trust Update (TU), Trust Aggregation (TA) and Trust Propagation (TP). They are described in the following sections.

4.1.1.1 Trust Composition (TC)

In our proposed TC, we consider the concepts including *QoS Similarity based Trust*, *Social Similarity based Trust*, and *Context Similarity* in the computation of MCTSE and MCTSR, which are described below.

- **Context-aware QoS Similarity based Trust (CQoSSTrust):** Let $CQoSSTrust_{SC_i,SP_j}^{C_S,C_E}$ denote the *Context-aware QoS similarity based Trust* that indicates the degree of similarity between the expected quality of service (see the Expected QoS in subsection 3.3.1) which is requested by a service-consuming device i and the advertised quality of service (see the Advertised QoS in subsection 3.3.1) which is provided by a service-providing device j at status and environment context of the device. We apply the cosine similarity function to calculate the similarity between two vectors $\overrightarrow{ExQoS}_{SC_i}^{C_S,C_E}$ and $\overrightarrow{AdQoS}_{SP_j}^{C_S,C_E}$ (see subsection 3.3.1). Therefore, $CQoSSTrust_{SC_i,SP_j}^{C_S,C_E}$ is calculated by Eg. (4.1), which contains the dot product and magnitude of vectors $\overrightarrow{ExQoS}_{SC_i}^{C_S,C_E}$ and $\overrightarrow{AdQoS}_{SP_j}^{C_S,C_E}$ in a two-dimensional space of the status and environment (time and location) contexts. As the maximum QoS similarity based trust, $CQoSSTrust_{SC_i,SP_j}^{C_S,C_E} = 1$ indicates that the SP_j can provide the maximum expected QoSs of SC_i while $CQoSSTrust_{SC_i,SP_j}^{C_S,C_E} = 0$ indicates that there is no similarity between the expected QoSs of SC_i and the advertised QoSs of SP_j.

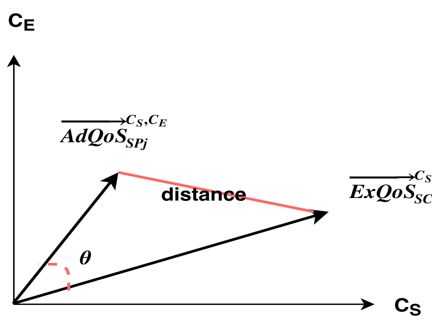


FIGURE 4.1: Computing of CQSST by cosine similarity function between $\overrightarrow{ExQoS}_{SC_i}^{C_S,C_E}$ and $\overrightarrow{AdQoS}_{SP_j}^{C_S,C_E}$

If $\overrightarrow{ExQoS}_{SC_i}^{C_S,C_E} = \text{A}$ and $\overrightarrow{AdQoS}_{SP_j}^{C_S,C_E} = B$ then:

$$CQoSSTrust_{SC_i,SP_j}^{C_S,C_E} = \cos(\theta) = |\overrightarrow{A} \times \overrightarrow{B}| = \frac{A.B}{\| A \|_2 \| B \|_2} = \frac{\sum_{\acute{h}=1}^{h} A_{\acute{h}}.B_{\acute{h}}}{\sqrt{\sum_{\acute{h}=1}^{h} A_{\acute{h}}^2}\sqrt{\sum_{\acute{h}=1}^{h} B_{\acute{h}}^2}} \tag{4.1}$$

- **Context-aware Social Similarity based Trust (CSSTrust):** Let $CSSTrust_{SC_i,SP_j}^{C_T}$ denote the *Context-aware Social Similarity based Trust* that indicates the overall degree of social similarity between SC_i and SP_j at the task type context. Eq. (4.2), Eq. (4.3), and Eq. (4.4) are applied to compute $CSSTrust_{SC_i,SP_j}^{C_T}$. First, $SSissimilarity^{C_T}$ is computed by Eq. (4.4) which denote *Social Similarity* between SC_i and SP_j at the task type context. It is computed by the sum of the degree of common social friends (see Social Similarity Friendship in subsection 3.3.2), common social communities (see Social Similarity Communities in subsection 3.3.2) and the common social relations (see Social Similarity Relations in subsection 3.3.2) between SC_i and SP_j while the variables w_1, w_2, w_3 are used as the normalised weight parameters. Then, $SDissimilarity^{C_T}$ is computed by Eq. (4.3) which denote *Social Dissimilarity* between SC_i and SP_j at the task type context. Finally, we apply the e^{-x} function in Eq. (4.2) where x is equal with $SDissimilarity^{C_T}$ because the more dissimilarity between a service-consuming device and a service-providing device, the less the trust value between them. Moreover, the e^{-x} function keeps the value of $CSSTrust^{C_T}_{SC_i,SP_j}$ between 0 and 1. $CSSTrust^{C_T}_{SC_i,SP_j}$ is applied as a weight for computing direct trust evaluation. If there is no social similarity between the owners of two devices in SIoT environments, $CSSTrust^{C_T}_{SC_i,SP_j} = e^{-SDissimilarity^{C_T}}$ means that there is less trust value between the owners of devices. Moreover, if a service-consuming device and a service-providing device don't have any common social similarity, the contextual social similarity based trust is equal to zero.

$$CSSTrust^{C_T}_{SC_i,SP_j} = e^{-SDissimilarity^{C_T}} \tag{4.2}$$

$$SDissimilarity^{C_T} = 1 - SSimilarity^{C_T} \tag{4.3}$$

$$SSimilarity^{C_T} = w_1 \times SSimFre^{C_T}_{SC_i,SP_j} + w_2 \times SSimCom^{C_T}_{SC_i,SP_j} + w_3 \times SSimR^{C_T}_{SC_i,SP_j} \tag{4.4}$$

- **Context Similarity (CSim):** Let $C^{S,E}_{SC_i \to SP_j}$ denote status and environment (time and location) contexts of device of a service-consuming device i (SC_i) and $C^{S,E}_{R_k \to SP_j}$ denote the status and environment (time and location) contexts of device of a service-recommender k (R_k) which are trusted to service-provider j (SP_j) in their previous transactions under these contexts of device. Moreover, let $CSim(C^{S,E}_{SC_i \to SP_j}, C^{S,E}_{R_k \to SP_j})$ denote the *Context Similarity* which indicates the degree of similarity between the status and environment (time and location) contexts of device of service-consuming device i ($C^{S,E}_{SC_i \to SP_j}$) and recommender k ($C^{S,E}_{R_k \to SP_j}$) towards service-providing device j which is computed by Eq. (4.5), Eq. (4.6), and Eq. (4.9). Let $C^{S,E}_{SP_j \to SC_i}$ denote status and environment (time and location) contexts of device of a service-providing device j (SP_j) and $C^{S,E}_{R_k \to SC_i}$ denote the status and environment (time and location) contexts of device of a service-recommender k (R_k) which are trusted to service-consuming device i (SC_i) in their previous transactions under these contexts of device. Moreover, let *CSim*($C^{S,E}_{SP_j \to SC_i}$, $C^{S,E}_{R_k \to SC_i}$) denote the *Context Similarity* which indicates the degree of context similarity between the status and environment (time and location) contexts of device of service-providing device j ($C^{S,E}_{SP_j \to SC_i}$) and recommender k ($C^{S,E}_{R_k \to SC_i}$) towards service-consuming device i which is computed by Eq. (4.7), Eq. (4.8), and Eq. (4.9).

The context similarity is useful for predicting how the feedback trust values of the service recommender and the service-consuming device (or the service-providing device) are related. Moreover, in a multidimensional context similarity, each contextual variable and each contextual condition is represented as an axis and as a point respectively in the space. Therefore, a contextual situation is mapped to a point in the space. The distance between two points is considered as the dissimilarity.

$$CSim(C^{S,E}_{SC_i \to SP_j}, C^{S,E}_{R_k \to SP_j}) = 1 - CDis \tag{4.5}$$

$$CDis = \frac{\sqrt{(C^{S}_{SC_i \to SP_j} - C^{S}_{R_k \to SP_j})^2 + (C^{E}_{SC_i \to SP_j} - C^{E}_{R_k \to SP_j})^2}}{Max_{dis}} \tag{4.6}$$

$$CSim(C^{S,E}_{SP_j \to SC_i}, C^{S,E}_{R_k \to SC_i}) = 1 - CDis \tag{4.7}$$

$$CDis = \frac{\sqrt{(C^{S}_{SP_j \to SC_i} - C^{S}_{R_k \to SC_i})^2 + (C^{E}_{SP_j \to SC_i} - C^{E}_{R_k \to SC_i})^2}}{Max_{dis}} \tag{4.8}$$

$$Max_{dis} = \sqrt{(C_{S_{max}} - C_{S_{min}})^2 + (C_{E_{max}} - C_{E_{min}})^2} \tag{4.9}$$

From the perspective of a service-consuming device, a combination of CQoSSTrust and CSSTrust is considered to be the trust composition (see Trust Composition in Section 2.1) for MCTSE. Moreover, a combination of CSSTrust and CSim is considered to be the trust composition for MCTSR. From the perspective of a service-providing device, CQoSSTrust is considered to be the trust composition for MCTSE. Moreover, CSim is considered to be the trust composition for MCTSR.

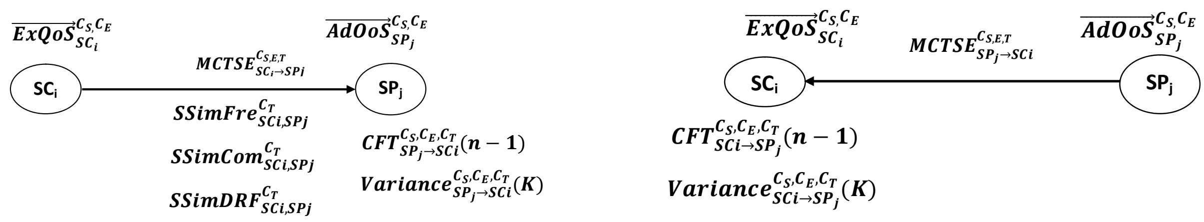
4.1.1.2 Trust Formation (TF)

In our proposed TF, we consider multi-trust properties (see *Trust Formation* in Section 2.1) including QoS trust properties, social trust properties and the property of context-dependence in trustworthy service evaluation and trustworthy service recommendation to form the overall trust. Each device's trustworthiness is evaluated on the basis of direct trust evaluation and indirect trust recommendation in the context of trust (including status, environment contexts of device and task type context). The trustworthiness of service-providing device j from the perspective of service-consuming device i in the context of trust is denoted by Eq. (4.10) and the trustworthiness of service-consuming device i from the perspective of service-providing device j in the context of trust (including status, environment contexts of device and task type context) is denoted by Eq. (4.11).

The acronyms ***MCTSE*** and ***MCTSR*** denote *Mutual Context-aware Trustworthy Service Evaluation* and *Mutual Context-aware Trustworthy Service Recommendation* respectively which are described in the following sections. Let $MCTSE^{C_S,C_E,C_T}_{SC_i \to SP_j}$ and $MCTSR^{C_S,C_E,C_T}_{SC_i \to SP_j}$ denote MCTSE and MCTSR respectively which are computed by SC_i toward SP_j at status, environment (time and location) contexts of device and task type context. Moreover, let $MCTSE^{C_S,C_E,C_T}_{SP_j \to SC_i}$ and $MCTSR^{C_S,C_T}_{SP_j \to SC_i}$ denote MCTSE and MCTSR respectively which are computed by SP_j toward SC_i at status, environment (time and location) contexts of device and task type context. Here, σ is a weight parameter ($0 \leq \sigma \leq 1$) to balance the importance of MCTSE and MCTSR. Let $T^{C_S,C_E,C_T}_{SC_i \to SP_j}$ and $T^{C_S,C_E,C_T}_{SP_j \to SC_i}$ denote overall trust values which are computed by SC_i toward SP_j and SP_j toward SC_i respectively. Fig. 4.2 depicts independent metrics (including expected QoS and advertised QoS) and dependent metrics (including social similarity friendship, social similarity community, social similarity relations, contextual feedback of trust and its variance) of contextual trust evaluation (see Metrics of Contextual Trust Evaluation in Section 3.3). These metrics are applied in the computation of MCTSE in the view of service-consuming device i and service-providing device j respectively. In addition, Fig. 4.3 depicts metrics of context-aware trustworthy service recommendation including context-aware social similarity based trust and context similarity between a service consuming i and each service recommender, and overall trust values are computed from service recommenders to service provider j (see Section 4.1.1.1). These metrics are applied in the computation of MCTSR in the view of service-consuming device i and service-providing device j respectively.

$$T^{C_S,C_E,C_T}_{SC_i \to SP_j} = \sigma \times MCTSE^{C_S,C_E,C_T}_{SC_i \to SP_j} + (1-\sigma) \times MCTSR^{C_S,C_E,C_T}_{SC_i \to SP_j} \tag{4.10}$$

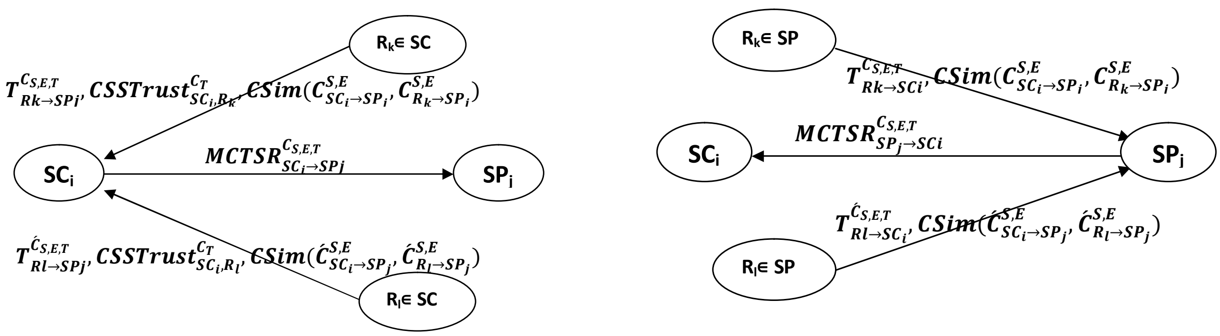
$$T^{C_S,C_E,C_T}_{SP_j \to SC_i} = \sigma \times MCTSE^{C_S,C_T}_{SP_j \to SC_i} + (1-\sigma) \times MCTSR^{C_S,C_E,C_T}_{SP_j \to SC_i} \tag{4.11}$$



(a) MCTSE model from the perspective of service-consuming device i

(b) MCTSE model from the perspective of service-providing device j

FIGURE 4.2: Mutual Context-aware Trustworthy Service Evaluation (MCTSE) model which includes independent and dependent metrics of contextual trust evaluation from the perspective of service-consuming device i and service-providing device j



(a) MCTSR model from the perspective of service-consuming device i

(b) MCTSR model from the perspective of service-providing device j

FIGURE 4.3: Mutual Context-aware Trustworthy Service Recommendation (MCTSR) model which includes the metrics of context-aware trustworthy service recommendation from the perspective of service-consuming device i and service-providing device j

4.1.1.3 Trust Update (TU)

In our proposed TU, we consider an event-driven scheme (see *Trust Update* in Section 2.1). After finishing the transaction between a service-consuming device and a service-providing device, the direct trust feedback for each service-consuming device and service-providing device is updated dynamically by Eq. (4.12) and Eq. (4.13) respectively. We consider the effect of ground truth (see section 3.1) in evaluating of feedback. Therefore, if a device is a dishonest device, its behaviour has a direct impact on its feedback.

$$CFT_{SC_i \to SP_j}^{C_S,C_E,C_T}(n) = GT_{SP_j} \times T_{SC_i \to SP_j}^{C_S,C_E,C_T} \tag{4.12}$$

$$CFT_{SP_j \to SC_i}^{C_S,C_E,C_T}(n) = GT_{SC_i} \times T_{SP_j \to SC_i}^{C_S,C_E,C_T} \tag{4.13}$$

4.1.1.4 Trust Aggregation (TA)

In the literature, different trust aggregation techniques have been investigated to aggregate direct trust values and indirect trust values from other devices [17, 39, 43, 52] (see *Trust Aggregation* in Section 2.1). However, the weighted sum is a popular and simple technique. For the MCTSE model, we use the static-weighted-sum technique to aggregate the direct trust evidence including *Context-aware QoS Similarity based Trust (CQoSSTrust)*, *Context-aware Social Similarity based Trust (CSSTrust)* (see the *CQoSSTrust and CSSTrust* in subsection 4.1.1.1), and *Contextual Feedback of Trust (CFT)* (see *CFT* in the subsection 3.3.2). Moreover, for MCTSR, we use *Context Similarity (CSim)* and *Context-aware Social Similarity based Trust (CSSTrust)* (see *CSim and CSSTrust* in subsection 4.1.1.1) as a static weight associated with the recommendation provided by a recommender as indirect trust aggregation. Therefore, raters with a higher context and social similarity have a higher weight.

4.1.1.5 Trust Propagation(TP)

In our proposed TP, we apply distributed trust propagation models. From a service-consuming device perspective, each service-consuming device acts autonomously to collect evidence and also serves as a recommender upon request. The service-consuming device stores in its local storage the feedback from service-providing devices after each transaction. Moreover, it propagates its trust observations to other service-consuming devices upon receiving a request. From a service-providing device perspective, we apply a dispute arbitration protocol [83] to propagate the feedback from service-consuming devices after each transaction to other service-providing devices.

4.1.2 Assessing trust in SIoT environments by MCTSM model

In SIoT environments, MCTSM assesses the trust for each transaction between a service-consuming device and a service-providing device. The details of assessing trust by MCTSM model are as follows, and Fig. 4.4 shows the inner connections between these steps by an activity diagram. Moreover, the inner connections between components of MCTSM are shown by Fig. 4.5. **Step 1:** A service-consuming device selects a list of service-providing device that can provide requested task (contains some services) or some services of tasks. Then, it evaluates the trustworthiness of each selected service-providing device by direct evidences (trust evaluation) and indirect observations (trust recommendation). As direct observation, *CQSSTrust* (including independent metrics) and *CSSTrust* (including dependent metrics) between service-consuming and service-providing devices are computed by *Trust Composition* (see the subsection 4.1.1.1). Then, these parameters with the latest CFT are aggregated by *Trust Aggregation* (see subsection 4.1.1.4) to compute MCTSE. The pseudo-code of MCTSE from service-consuming device *i* to service-providing device *j* is shown in **Algorithm** 1. As indirect evidence, CSSTrust (including independent metrics) and CSim between service-consuming and recommender are computed by *Trust Composition* (see subsection 4.1.1.1). Then, these parameters with the latest CFT are aggregated by *Trust Aggregation* to compute MCTSR (see subsection 4.1.1.4). The pseudo-code of MCTSR from service-consuming device *i* to service-providing device *j* is shown in **Algorithm** 3. Thereafter, the combination of MCTSE and MCTSR is computed by *Trust Formation* to compute the overall trust value of the service-providing device. Fig. 4.5(a) depicts the details of computing the overall trust value of a service-providing device by a service-consuming device.

Step 2: After each service-providing device is evaluated by a service-consuming device, a list of potential service-providing devices based on integrated trust values are created. In addition, these integrated trust values can be used to distinguish honest and dishonest service-providing devices. Then, the service-consuming device selects one or more service-providing devices with the most trustworthiness value(s) and sends its requests to them.

Step 3: When a service-providing device receives many requests from different service-consuming devices, it attempts to distinguish between honest and dishonest service-consuming devices. Therefore, it evaluates the trustworthiness of

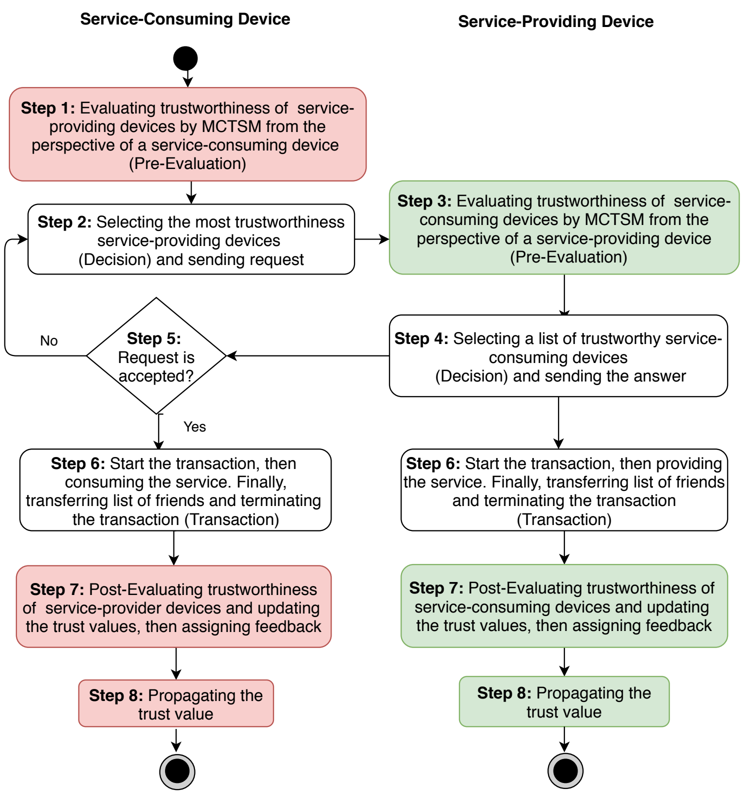


Figure 4.4: Activity diagram of assessing the trust value between a service-consuming device and a service-providing device

each service-consuming device. As direct evidence, CQSSTrust (including independent metrics) between service-consuming and service-providing devices is computed by *Trust Composition* (see subsection 4.1.1.1). Then, these parameters with the latest CFT are aggregated by Trust Aggregation (see subsection 4.1.1.4) to compute MCTSE. The pseudo-code for MCTSE from service-providing device j to service-consuming device i is shown in **Algorithm** 2. As indirect observation, CSim between service-consuming and recommender are computed by Trust Composition (see subsection 4.1.1.1). Then, these parameters with latest CFT are aggregated by Trust Aggregation (see subsection 4.1.1.4) to compute MCTSR. The pseudo-code for MCTSR from service-providing device j to service-consuming device i is shown in **Algorithm** 4. Thereafter, the combination of MCTSE and MCTSR is computed by *Trust Formation* to compute the overall trust value of the service-consuming device. Fig. 4.5(b) depicts the details of computing the overall trust value of a service-consuming device by a service-providing device.

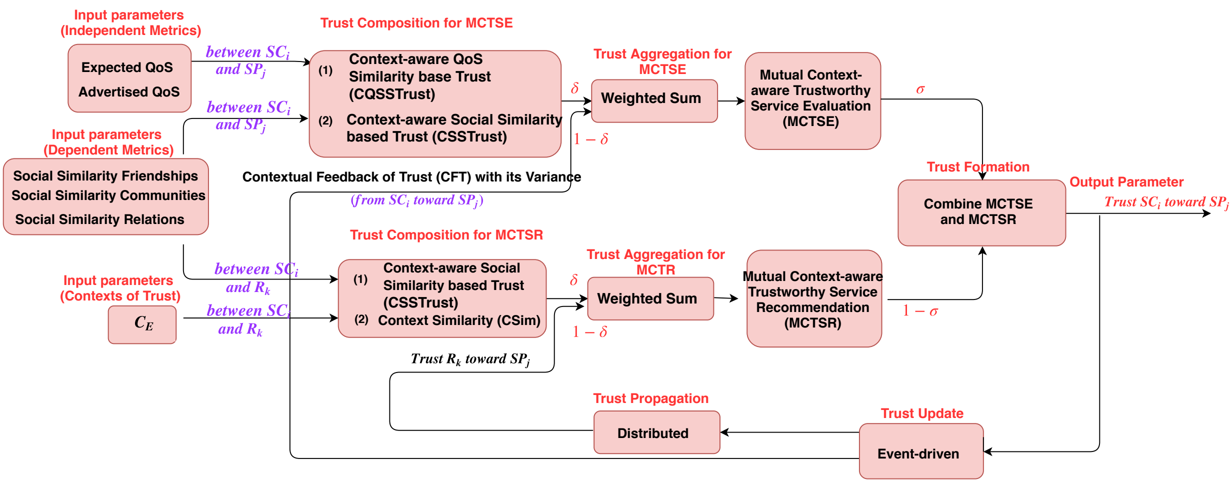
Step 4: Service-providing devices make a list of trustworthy service-consuming devices based on the integrated trust values and their available resources and send the answer to each service-consuming device.

Step 5: Each service-consuming device receives its answer from the the selected service-provider. If its request is accepted, then the transaction is started. If its request is not accepted, the service-consuming device selects the next trustworthy service-providing device and sends its request.

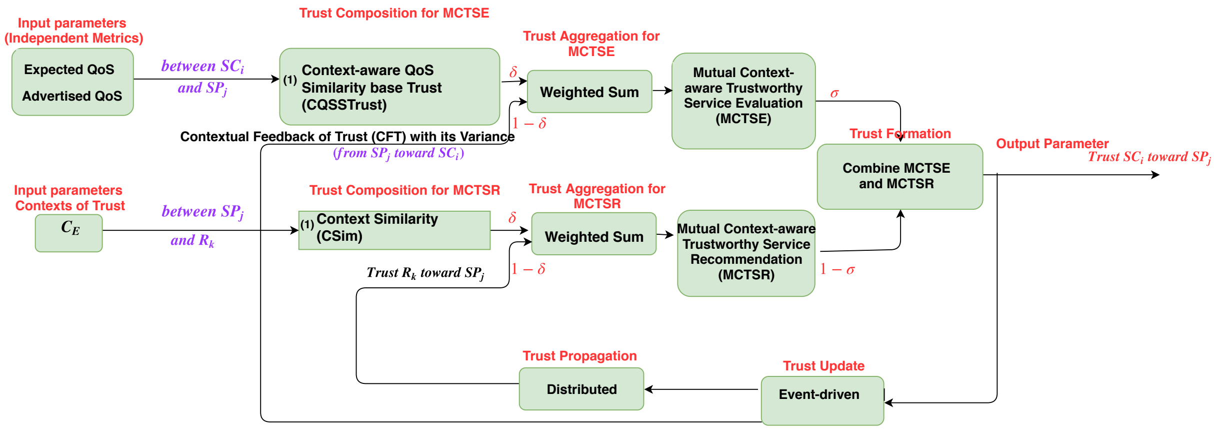
Step 6: Service-consuming devices and service-providing devices transact with each other. Moreover, service-consuming and service-providing devices transfer their friend lists.

Step 7: After terminating each transaction, each service-consuming device updates the trust value of each service-providing device, and then assigns feedback to each service-providing device. This feedback is based on the quality of the received service and the specific context it belongs to (see *Trust Update* component in the The Fig. 4.5(a)). Moreover, the service-providing device assigns a feedback to each service-consuming device based on the expected behaviour of each service-consuming device (see *Trust Update* component in Fig. 4.5(b)).

Step 8: Finally, each service-consuming device stores the feedback of service-providing devices and propagates its trust observations to other service-consuming devices upon receiving the request (see *Trust Aggregation* component in Fig. 4.5(a)). Moreover, each service-providing device propagates the feedback of service-consuming devices to other service-providing devices (see *Trust Aggregation* component in the The Fig. 4.5(b)). To preserve privacy of information



(a) From the perspective of a service-consuming device



(b) From the perspective of a service-providing device

FIGURE 4.5: MCTSM including design components, MCTSE model and MCTSR model for SIoT environments from the perspective of a service-consuming device and a service-providing device

in assessing of trust, we consider that the owners of devices who want to use SIoT services need to let to share their information related to the status and the environment. Moreover, owners can exchange their information related to their social relationship after interaction by using a hash function.

4.2 Mutual Context-aware Trustworthy Service Evaluation (MCTSE) Model

Mutual Context-aware Trustworthy Service Evaluation (MCTSE) indicates the trust evaluation between a service-providing device and a service-consuming device while both of them evaluate each other and consider the contextual information. Below, we describe two parts of the mutual context-aware trustworthy service evaluation including *Trustworthy Service Evaluation from Service-Consuming Device i to Service-Providing Device j* and *Trustworthy Service Evaluation from*

Algorithm 1: Trust Evaluation by MCTSE Model, from SC_i to SP_j

Input: SC_i, SP_j, n, σ

Output: $MCTSE^{C_S,C_E,C_T}_{SC_i \to SP_j}$

begin

- Calculate $\overrightarrow{AdQoS}^{C_S,C_E}_{SP_j}$ by Eq. (3.3) and $\overrightarrow{ExQoS}^{C_S,C_E}_{SCi}$ by Eq. (3.4);
- Determine $CQoSSTrust^{C_S,C_E}_{SC_i,SP_j}$ by Eq. (4.1);
- Calculate $SSimFre^{C_T}_{SC_i,SP_j}$ by Eq. (3.5) and $SSimCom^{C_T}_{SC_i,SP_j} by (3.6)$;
- Calculate $SSimR^{C_T}_{SC_i,SP_j}$ by Table 3.1;
- Determine $CSSTrust^{C_T}_{SC_i,SP_j}$ by Eq. (4.2), Eq. (4.3), and Eq. (4.4);
- **if** $CFT^{C_S,C_E,C_T}_{SC_i \to SP_j}$ **then**
  - $CFT^{C_S,C_E,C_T}_{SC_i \to SP_j}(n) \leftarrow 0$;
  - $Variance^{C_S,C_E,C_T}_{SC_i \to SP_j}(K) \leftarrow 0$;
- **else**
  - Calculate $Variance^{C_S,C_E,C_T}_{SC_i \to SP_j}(K)$ by Eq. (3.7) and Eq. (3.9);
  - $Select\ item\ n-1\ from\ CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}$;
- **end**
- Calculate $MCTSE^{C_S,C_E,C_T}_{SC_i \to SP_j}$ by Eq. (4.14);
- **return** $MCTSE^{C_S,C_E,C_T}_{SC_i \to SP_j}$

end

Algorithm 2: Trust Evaluation by MCTSE Model, from SP_j toward SC_i

Input: SC_i, SP_j, n, σ

Output: $MCTSE^{C_S,C_E,C_T}_{SP_j \to SC_i}$

begin

- Calculate $\overrightarrow{AdQoS}^{C_S,C_E}_{SP_j}$ by Eq. (3.3) and $\overrightarrow{ExQoS}^{C_S,C_E}_{SCi}$ by Eq. (3.4);
- Determine $CQoSSTrust^{C_S,C_E}_{SC_i,SP_j}$ by Eq. (4.1);
- **if** $CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}$ **then**
  - $CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}(n) \leftarrow 0$;
  - $Variance^{C_S,C_E,C_T}_{SP_j \to SC_i}(K) \leftarrow 0$;
- **else**
  - Calculate $Variance^{C_S,C_E,C_T}_{SP_j \to SC_i}(K)$ by Eq. (3.8) and Eq. (3.10);
  - $Select\ item\ n-1\ from\ CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}$;
- **end**
- Calculate $MCTSE^{C_S,C_E,C_T}_{SP_j \to SC_i}$ by Eq. (4.15);
- **return** $MCTSE^{C_S,C_E,C_T}_{SP_j \to SC_i}$

end

Service Providing Device j to Service-Consuming Device i. Moreover, the variance is applied to consider the trend of a service-providing device in its K previous transactions. In the following equations, we apply δ as a weight ($0 \leq \delta \leq 1$) to balance the importance of $CQoSSTrust^{C_S,C_E}_{SC_i,SP_j}$, $CSSTrust^{C_T}_{SC_i,SP_j}$, $CFT^{C_S,C_E,C_T}_{SC_i \to SP_j}$ and $CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}$ (see Section 3.3.2).

- **Trustworthy Service Evaluation from Service-Consuming Device *i* to Service-Providing Device *j*:** the MCTSE from service-consuming device i to service-providing device j ($MCTSE^{C_S,C_E,C_T}_{SC_i \to SP_j}$) is calculated by Eq.(4.14). It denotes the direct trust value from service-consuming device i to service-providing device j. Algorithm 1 presents pseudo-code for $MCTSE^{C_S,C_E,C_T}_{SC_i \to SP_j}$. Firstly, independent metrics including $\overrightarrow{ExQoS}^{C_S,C_E}_{SCi}$ and $\overrightarrow{AdQoS}^{C_S,C_E}_{SPj}$ (see Section 3.3.1) are calculated to determine $CQoSSTrust^{C_S,C_E}_{SC_i,SP_j}$ (see Section 4.1.1.1) and dependent metrics including $SSimFre^{C_T}_{SC_i,SP_j}$, $SSimCom^{C_T}_{SC_i,SP_j}$, and $SSimR^{C_T}_{SC_i,SP_j}$ (see Section 3.3.2) are calculated to determine $CSSTrust^{C_T}_{SC_i,SP_j}$ (see Section 4.1.1.1). Secondly, if SC_i has any CFT of SP_j, the last $CFT^{C_S,C_E,C_T}_{SC_i \to SP_j}$ and the variance of last the k feedback values ($Variance^{C_S,C_E,C_T}_{SC_i \to SP_j}(K)$) (see Section 3.3.2) are calculated. Finally, $MCTSE^{C_S,C_E,C_T}_{SC_i \to SP_j}$

is calculated by a combination of $CQoSSTrust^{C_S,C_E}_{SC_i,SP_j}$, $CSSTrust^{C_T}_{SC_i,SP_j}$, $CFT^{C_S,C_E,C_T}_{SC_i \to SP_j}$ and $Variance^{C_S,C_E,C_T}_{SC_i \to SP_j}(K)$.

$$\begin{aligned} MCTSE^{C_S,C_E,C_T}_{SC_i \to SP_j} &= \delta \times CQoSSTrust^{C_S,C_E}_{SC_i,SP_j} \times CSSTrust^{C_T}_{SC_i,SP_j} \\ &+ (1-\delta) \times e^{Variance^{C_S,C_E,C_T}_{SC_i \to SP_j}(K)} \times CFT^{C_S,C_E,C_T}_{SC_i \to SP_j}(n-1). \end{aligned} \tag{4.14}$$

- **Trustworthy Service Evaluation from Service-Providing Device *j* to Service-Consuming Device *i***: the MCTSE from service-providing device j to service-consuming device i ($MCTSE^{C_S,C_E,C_T}_{SP_j \to SC_i}$) is calculated by Eq.(4.15). It denotes the direct trust value from service-providing device j to service-consuming device i. Algorithm 2 presents pseudo-code for $MCTSE^{C_S,C_E,C_T}_{SP_j \to SC_i}$. Firstly, independent metrics including $\overrightarrow{ExQoS}^{C_S,C_E}_{SCi}$ and $\overrightarrow{AdQoS}^{C_S,C_E}_{SPj}$ (see Section 3.3.1) are calculated to determine $CQoSSTrust^{C_S,C_E}_{SC_i,SP_j}$ (see Section 4.1.1.1). Secondly, if SP_j has any CFT of SC_i, the last $CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}$ and the variance of last the k feedback values ($Variance^{C_S,C_E,C_T}_{SP_j \to SC_i}(K)$) (see Section 3.3.2) are calculated. Finally, $MCTSE^{C_S,C_E,C_T}_{SP_j \to SC_i}$ is calculated by a combination of $CQoSSTrust^{C_S,C_E}_{SC_i,SP_j}$, $CSSTrust^{C_T}_{SC_i,SP_j}$, $CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}$ and $Variance^{C_S,C_E,C_T}_{SP_j \to SC_i}(K)$.

$$\begin{aligned} MCTSE^{C_S,C_T}_{SP_j \to SC_i} &= \delta \times CQoSSTrust^{C_S}_{SC_i,SP_j} \\ +(1-\delta) \times e^{Variance^{C_S,C_E,C_T}_{SP_j \to SC_i}(K)} &\times CFT^{C_S,C_E,C_T}_{SP_j \to SC_i}(n-1). \end{aligned} \tag{4.15}$$

4.3 Mutual Context-aware Trustworthy Service Recommendation (MCTSR) Model

Mutual Context-aware Trust Recommendation (MCTSR) indicates the trust recommendation received from the service recommender. In the following, we describe two parts of the mutual context-aware trustworthy service recommendation including *Trustworthy Service Recommendation from Service-Consuming Device i to Service-Providing Device j* and *Trustworthy Service Recommendation from Service-Providing Device j to Service-Consuming Device i*. We apply the Contextual Sparse Liner method using Multidimensional Context Similarity (CSL_MCS) modeling (see Section 2.3.2) as a distributed collaborative filtering method to collect trust feedback from devices that have interacted with the given service-providing device or service in the past. Moreover, each recommender will send its latest trust value which is computed by a combination of its previous trust evaluation and trust recommendation (see section 4.1.1.2)

Algorithm 3: Trust Recommendation by MCTSR Model, from SC_i to SP_j

Input: SC_i, SP_j, SumCSim, SumCSSTrust, $list_R[]$, SumTrust, n
Output: $MCTSR^{C_S,C_E,C_T}_{SC_i \to SP_j}$

```
SumTrust ← 0;
begin
    foreach R_k ∈ list_R[] do
        Calculate SSimFre^{C_T}_{SC_i,R_k} by Eq. (3.5) and SSimCom^{C_T}_{SC_i,R_k} by(3.6);
        Calculate SSimR^{C_T}_{SC_i,R_k} by Table 3.1;
        Determine CSSTrust^{C_T}_{SC_i,R_k} by Eq. (4.2), Eq. (4.3), and Eq. (4.4);
        Calculate CSim(C^{S,E}_{SC_i→SP_j}, C^{S,E}_{R_k→SP_j}) by Eq. (4.5) and Eq. (4.9);
        SumTrust+ = CSSTrust^{C_T}_{SC_i,R_k}/SumCSSTrust × CSim(C^{S,E}_{SC_i→SP_j}, C^{S,E}_{R_k→SP_j})/SumCSim × T^{C_S,C_E,C_T}_{R_k→SP_j};
    end
    MCTSR^{C_S,C_E,C_T}_{SC_i→SP_j} ← SumTrust;
    return MCTSR^{C_S,C_E,C_T}_{SC_i→SP_j}
end
```

Algorithm 4: Trustworthy Service Recommendation by MCTSR Model, from SP_j to SC_i

Input: SC_i, SP_j, SumCSim, $list_R[]$, SumTrust, n
Output: $MCTSR^{C_S,C_E,C_T}_{SP_j \to SC_i}$

```
SumTrust ← 0;
begin
    foreach R_k ∈ list_R[] do
        Calculate SSimFre^{C_T}_{SP_j,R_k} by Eq. (3.5) and SSimCom^{C_T}_{SP_j,R_k} by(3.6);
        Calculate SSimR^{C_T}_{SP_j,R_k} by Table 3.1;
        Determine CSSTrust^{C_T}_{SP_j,R_k} by Eq. (4.2), Eq. (4.3), and Eq. (4.4);
        Calculate CSim(C^{S,E}_{SP_j→SC_i}, C^{S,E}_{R_k→SC_i}) by Eq. (4.5) and Eq. (4.9);
        SumTrust+ = CSSTrust^{C_T}_{SP_j,R_k}/SumCSSTrust × CSim(C^{S,E}_{SP_j→SC_i}, C^{S,E}_{R_k→SC_i})/SumCSim × T^{C_S,C_E,C_T}_{R_k→SC_i};
    end
    MCTSR^{C_S,C_E,C_T}_{SP_j→SC_i} ← SumTrust;
    return MCTSR^{C_S,C_E,C_T}_{SP_j→SC_i}
end
```

which it includes the feedback of that device in N number of its previous transactions (see the section 3.3.2).

People can trust the others with whom they have close social relations [34]. Therefore, we select recommenders from the friends of the service-consuming device's owner or the service-providing device's owner.

- **Trustworthy Service Recommendation from Service-Consuming Device *i* to Service-Providing Device *j*:** Each service-consuming device receives the trust value calculated by service recommenders and then it computes *Context-aware Social Similarity based trust*, $CSSTrust^{C_T}_{SC_i,R_k}$, and *Context Similarity*, $CSim(C^{S,E}_{SC_i \to SP_j}, C^{S,E}_{R_k \to SP_j})$, (see Section 4.1.1.1) for each service recommender. We consider $CSSTrust^{C_T}_{SC_i,R_k}$ as a coefficient in the CSL_MCS method (see Section 2.3.2) and the *Trust Value* which is computed from service recommender k to service-providing device j, $T^{C_S,C_E,C_T}_{R_k \to SP_j}$, (see subsection 4.1.1.2) as rating of service recommenders [73]. Moreover, we consider the status and environment (time and location) contexts of device to compute the context similarity between the service-consuming device and service recommenders or the service-providing device and service recommenders. Then, the service-consuming device applies the Contextual Sparse Liner method using Multi-dimensional-Context Similarity (CSL_MCS) to compute the trust recommendations and collect them for each service-providing device. $MCTSR^{C_S,C_E,C_T}_{SC_i \to SP_j}$ is calculated by Eq. (4.16). Algorithm 3 presents pseudo-code for $MCTSR^{C_S,C_E,C_T}_{SC_i \to SP_j}$.

$$MCTSR^{C_S,C_E,C_T}_{SC_i \to SP_j} = \sum_{R_k \in SC} \frac{CSSTrust^{C_T}_{SC_i,R_k}}{\sum_{R_k \in SC} CSSTrust^{C_T}_{SC_i,R_k}} \times \frac{CSim(C^{S,E}_{SC_i \to SP_j}, C^{S,E}_{R_k \to SP_j})}{\sum_{R_k \in SC} CSim(C^{S,E}_{SC_i \to SP_j}, C^{S,E}_{R_k \to SP_j})} \times T^{C_S,C_E,C_T}_{R_k \to SP_j} \tag{4.16}$$

- **Trust Recommendation from Service-Providing Device *j* to Service-Consuming Device *i***: Each service-providing device receives the trust value, $T^{C_S,C_E,C_T}_{R_k \to SC_i}$, calculated by the service recommender and then it computes the *Context Similarity*, $CSim(C^{S,E}_{SP_j \to SC_i}, C^{S,E}_{R_k \to SC_i})$, (see Section 4.1.1.1) for each service recommender. We consider the *Trust Value* which is computed from service recommender k to service-consuming device i, $T^{C_S,C_E,C_T}_{R_k \to SC_i}$, (see subsection 4.1.1.2) as rating of service recommenders in the CSL_MCS method [73]. Moreover, we consider the context status and environment (time and location) of device to compute the context similarity between service-consuming devices and the service recommender or service-providing devices and the service recommender. Then, the service-consuming device applies the Contextual Sparse Liner method using Multi-dimensional-Context Similarity (CSL_MCS) to compute the trust recommendations and collect them for each service-providing device. $MCTSR^{C_S,C_E,C_T}_{SP_j \to SC_i}$ is calculated by Eq. (4.17). Algorithm 4 presents pseudo-code for $MCTSR^{C_S,C_E,C_T}_{SP_j \to SC_i}$.

$$MCTSR^{C_S,C_E,C_T}_{SP_j \to SC_i} = \sum_{R_k \in SP} \left(\frac{CSim(C^{S,E}_{SP_j \to SC_i}, C^{S,E}_{R_k \to SC_i})}{\sum_{R_k \in SP} CSim(C^{S,E}_{SP_j \to SC_i}, C^{S,E}_{R_k \to SC_i})} \right) \times T^{C_S,C_E,C_T}_{R_k \to SC_i} \tag{4.17}$$

4.4 Conclusion

In this chapter, we first introduced an overview of MCTSM that described the design components of our MCTSM model including trust composition (TC), trust formation (TF), trust update (TU), trust aggregation (TA) and trust propagation (TP). Then, we described different steps of assessing trust between a service-consuming device and a service-providing device by the proposed MCTSM model. Finally we described two parts of MCTSE and MCTSR from service-consuming device to service-providing device or vice versa. In the next chapter, we will describe and discuss our experimental results.

5

Simulation and Experiment

In this section, we validate our proposed MCTSM in a simulation scenario where 300 service-consuming devices need to select the most trustworthy service-providing devices from 300 service-providing devices. This chapter is organised as follows. Section 5.1 introduces the details of our simulation. Section 5.2 describes the experiment results by analysing and discussing them. In this section, we investigate the effectiveness of MCTSM in trustworthy service evaluation (subsection 5.2.1), and in trustworthy service recommendation (subsection 5.2.2) where there are 0% and 50% of dishonest devices respectively which provide or consume services with and without attacks including BMA, BSA, SPA, and OOA (see Table 2.1). Then, we investigate the performance of MCTSM (5.2.3) by examining trust convergence, accuracy and resiliency to show how MCTSM works with different attacks. Finally, Section 5.3 summaries our work in this chapter.

5.1 Simulation Settings

To simulate an SIoT environment, because there is a lack of real dataset in the literature, we create a synthetic dataset with 600 randomly generated devices with different statuses, in which there are 300 service-providing devices and 300 service-consuming devices. These devices are randomly assigned to 200 users who are selected from synthetic dataset of the online social network Facebook obtained from the Stanford Large Network Dataset Collection [84]. We assume that each user owns two devices on average. Each device has a role as either a service provider or a service consumer. We assume that the roles of randomly selected 20% of devices will change after each round because each device can be a service provider or a service consumer. In addition, we assume that after a direct interaction between the devices of two users, they exchange their friend lists and profiles.

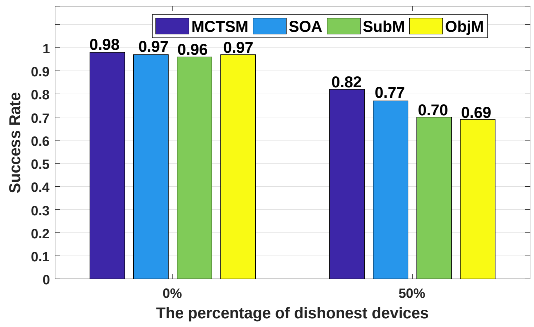
In our simulation, we classify the devices into two groups of honest and dishonest devices who provide high quality services and poor quality services. The percentage of dishonest devices set to 0% and 50%. The dishonest devices perform trust related attacks including BMA, BSA, SPA, and OOA (Table 2.1) which the pseudo-code of trust-related attacks are shown in Algorithm 5 and Algorithm 6 (see Appendix A). To assess the performance of our proposed trust model, the user satisfaction levels of service selections (or real service qualities of devices) are considered as the *"ground truth"* (see section 3.1). We compare the trust value of each honest or dishonest device which is computed by our proposed model with the *"ground truth"* of them to assess the accuracy of our model. For each honest device, a random number in the range of [0.80 , 0.85] is assigned to its ground truth (it shows that honest device provides high quality service), and for each dishonest device a random value in the range of [0.55, 0.60] is assigned to its ground truth (it shows that dishonest device provides poor quality services). Moreover, we consider optimal parameters in our models obtained by trial and test: σ=0.8, δ=0.5, w_1=0.33, w_2=0.33, and w_3=0.33. To assess *Social Similarity Relation (SSimR)* metric between any pair of devices (see subsection 3.3.2 and Table 3.1), we consider the owners of devices, who carry their devices, moving in an operational region including 10×10 cells according to the SWIM mobility model [85] which reflects human social behaviour. Moreover, we consider some devices such as sensors whose location are fixed. A device within a given cell is able to communicate with all devices within the same cell.

5.2 Performance Comparison in SIoT Environments

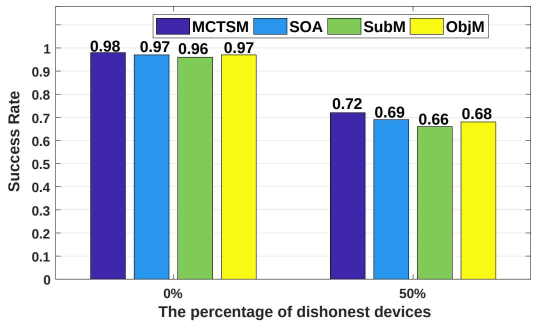
In this thesis, we focus on trust evaluation and trust recommendation in SIoT environments. So, we select three state-of-the-art trust management models in this field as the baseline models. They are SOA [17], as a non-context trust management model, and an adaptive and scalable trust management model, SubM [43] and ObjM [43], as two single-context trust management models, which are subjective and objective models respectively. Each of these models is implemented using C# programming. The experimental results plotted in the figures below are the average results of 20 iterations. Furthermore, we use two metrics, *i.e.*, the *success rate* and the *mean absolute error (MAE)*, to evaluate the performance of these models. The *success rate* is computed as the ratio of the real service quality value obtained by a service-consuming device to the optimal value of all candidates. It demonstrates the ability of a model to select the best quality services. *MAE* (Minimum Absolute Error) is computed as the average of the distance between the trust value and the ground truth. It shows the recommendation accuracy of a model (the lower, the better). For evaluating the effect of multi-contexts of trust on the *success rate* and *MAE*, we compare our MCTSM, which considers multi-contexts of trust, with MCTSM variants only considering single contexts of trust including $MCTSM^{C_S}$ (context status of device), $MCTSM^{C_E}$ (context environment of device), and $MCTSM^{C_T}$ (context task type). In addition, for evaluating the effect of the contextual feedback of trust and its variance (see subsection 3.3.2) on the *success rate* and *MAE*, we compare our MCTSM, which considers contextual feedback of trust and its variance, with $MCTSM^{SFT}$, where considers the Simple Feedback of Trust (SFT). In the SFT, we do not apply any context status and environment of device, context task type and variance of feedback in computing direct trust feedback. Furthermore, for evaluating the performance of our MCTSM to show how it works with different types of attacks, the metric of *trust value*, which depicts the trust convergence, accuracy and resiliency properties, is applied.

5.2.1 Experiment 1: Effectiveness in Trustworthy Service Evaluation

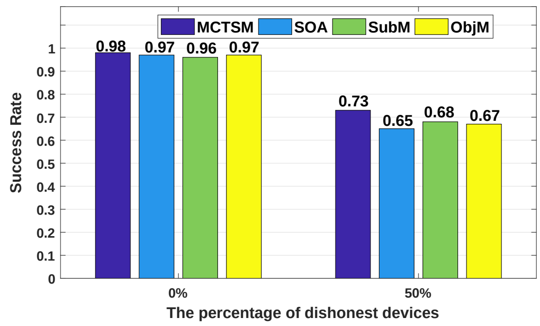
Results: Figs 5.1(a) to 5.1(d) depict the success rates of the MCTSM, SOA, SubM, and ObjM models when there are different percentages of dishonest devices (0% and 50%), to provide or consume services without attack and with attacks. From these figures, we can see that MCTSM always has the best success rate in all the cases. On average, MCTSM is 2% higher in the success



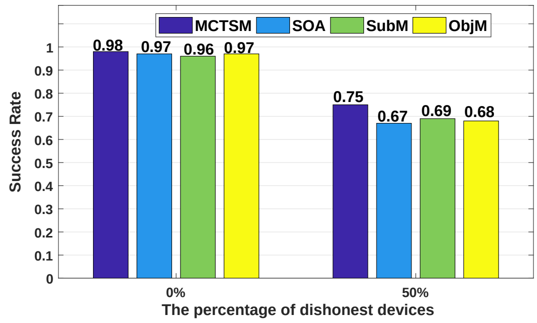
(a) Without attack



(b) Bad-Mouthing and Ballot-Stuffing Attacks



(c) Self-Promoting Attack



(d) On-Off Attack

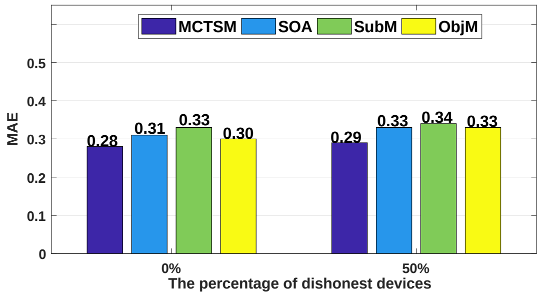
FIGURE 5.1: Comparison of the success rate of an honest device (iterations = 20) by increasing the number of dishonest devices without attack and with different types of attack

rate than the average of the three baseline models when the percentage of dishonest devices is 0% (without dishonest devices). There is no significant difference in this case because there is no dishonest device. Moreover, On average, MCTSM is 13.8%, 7.4%, 10.6%, and 10.2% higher in the success rate than the average of the three baseline models when there is 50% dishonest devices who provide or consume services without attack and with attacks including BMA-MSA, SPA, and OOA respectively.

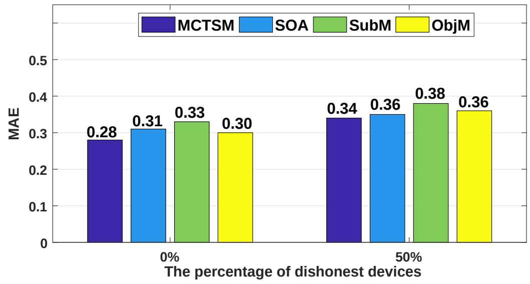
Analysis: The experimental results illustrate that: (1) the baseline models can not select the trustworthy devices with the optimal service quality value when there are dishonest devices as they do not consider devices' trustworthiness in multi-contexts of trust; and (2) the MCTSM model can select the most trustworthy devices with the best quality service when compared with the other three models. This is because the MCTSM considers multi-contexts of trust to be able to distinguish dishonest devices more accurately.

5.2.2 Experiment 2: Effectiveness in Trustworthy Service Recommendation

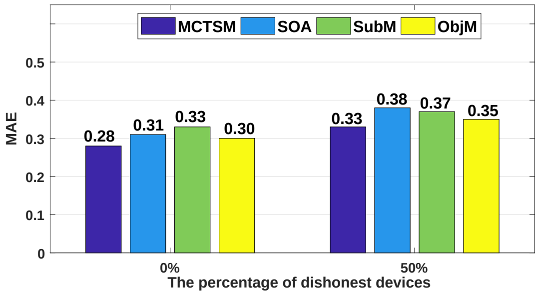
Results: Figs. 5.2(a) to 5.2(d) plot the MAE values of the MCTSM, SOA, SubM, and ObjM models, when there are different percentages of dishonest devices (0% and 50%), to estimate



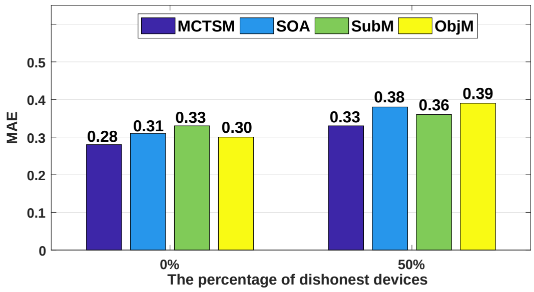
(a) Without attack



(b) Bad-Mouthing and Ballot-Stuffing Attacks



(c) Self-Promoting Attack



(d) On-Off Attack

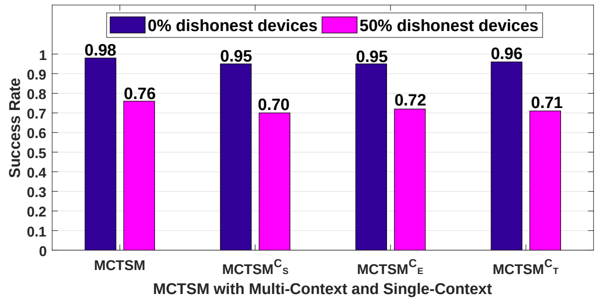
FIGURE 5.2: Comparison of the MAE of an honest device (iterations = 20) by increasing the number of dishonest devices without attack and with different types of attack

their ability to provide or consume services without attacks and with attacks. From these figures, we can see that MCTSM always has the least MAE in all the cases. On average, MCTSM is 9.6% less in MAE than the average of the three baseline models when the percentage of dishonest devices is 0% (without dishonest devices). Moreover, On average, MCTSM outperforms the three baseline models by 12%, 5.5%, 8.3%, and 10.8% less in MAE than the average of the three baseline models when there is 50% dishonest devices who provide or consume services without attacks or with attacks including BMA-MSA, SPA, and OOA.

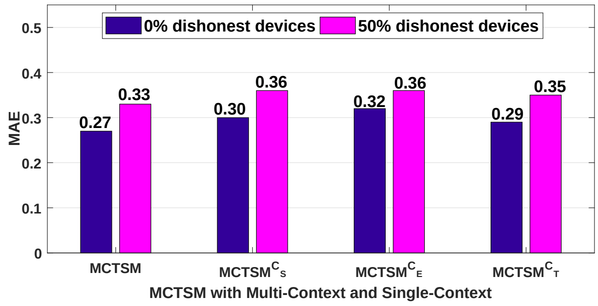
Analysis: The experimental results illustrate that: (1) the baseline models can not recommend the most trustworthy devices with accuracy as they do not consider the degree of similarity between the contexts of trust of a service-consuming device and a service recommender towards a service-providing device (see context similarity subsection 4.1.1.1); (2) the MCTSM model can significantly improve the recommendation accuracy when compared with the other three models. This is because our MTCM can differentiate honest and dishonest devices more accurately and recommend high-quality services to service-consuming devices by considering context similarity in trustworthy service recommendation.

5.2.3 Experiment 3: Performance of MCTSM

This experiment is to investigate the performance of our MCTSM as follows: (1) evaluating the effect of feedback and contexts on the success rate and MAE, and (2) examining the trust

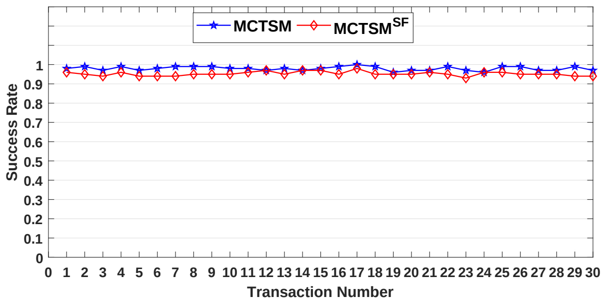


(a) The success rate

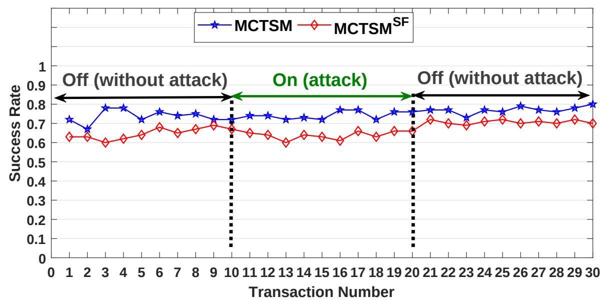


(b) MAE

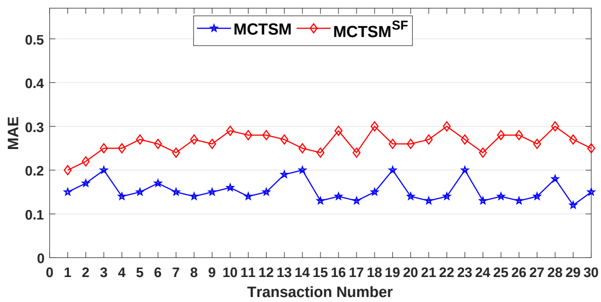
FIGURE 5.3: The effect of context in the success and MAE by increasing the number of dishonest devices with on-off attack



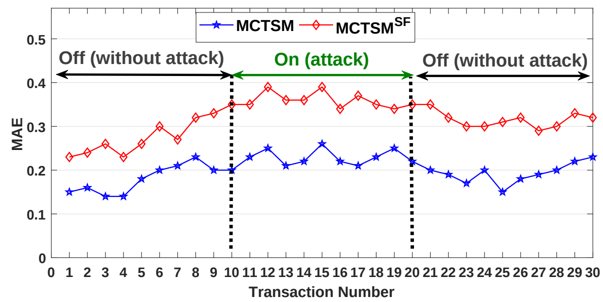
(a) 0% of dishonest devices



(b) 50% of dishonest devices with on-off attack



(c) 0% of dishonest devices



(d) 50% of dishonest devices with on-off attack

FIGURE 5.4: The effect of feedback on the success rate and MAE by increasing the number of dishonest devices with on-off attack.

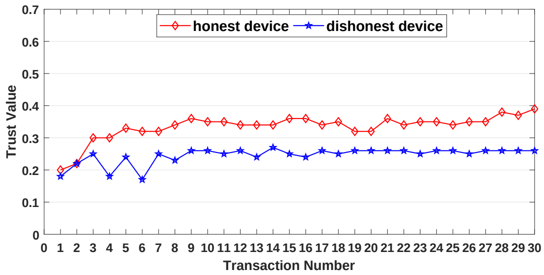
convergence, accuracy and resiliency properties to show how our MCTSM work with attacks.

A. The Effect of the Feedback and Context on the Success Rate and MAE Results: Figs. 5.3(a) and 5.3(b) depict the success rate and MAE of MCTSM, $MCTSM^{C_S}$, $MCTSM^{C_E}$, and $MCTSM^{C_T}$, where there are 0 and 50 percentage of dishonest devices, to provide or consume services without attacks and with OOA respectively. From these figures, we can see that MCTSM has the best success rate and the least MAE on all the cases. On average, MCTSM is 4.92% higher and 9.14% less in the success rate and MAE respectively than the average of MCTSM with a single-context of trust. Fig. 5.4(a) and 5.4(b) depict the success rate and Fig. 5.4(c) and 5.4(d) depict the MAE of the MCTSM and the $MCTSM^{SF}$ where there are 0 and 50 percent of dishonest devices without attack and with OOA in 30 transactions between service-providing devices and service-consuming-devices. From these figures, we can see that: (1) during these transactions, the success rate and MAE of MCTSM are more steady than for $MCTSM^{SF}$; and (2) MCTSM with consideration of contextual feedback and variance always has the best success rate and the least MAE.

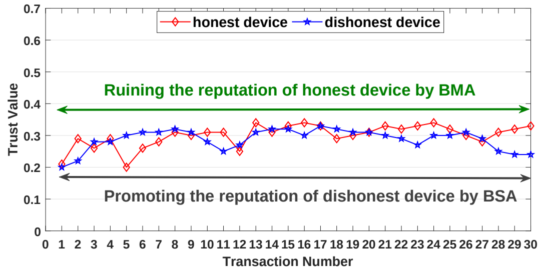
Analysis: The experimental results illustrate that: (1) MCTSM, which considers the context similarity of trust in a recommendation, can recommend the most trustworthy devices with accuracy when compared with MCTSM with a single context. This is because considering the context similarity of trust makes our model be able to recommend a device with more accuracy; (2) when dishonest devices perform OOA, they behave alternatively well and badly, therefore, they can compensate for their bad past behaviour by behaving well for a period of time. MCTSM with consideration of the contextual feedback of trust and the variance of the feedback received by the recommender can recommend the most trustworthy service-providing device to service-consuming devices even if subject to OOA.

B. The Effect of the Feedback and Context in Resiliency Against Attacks:

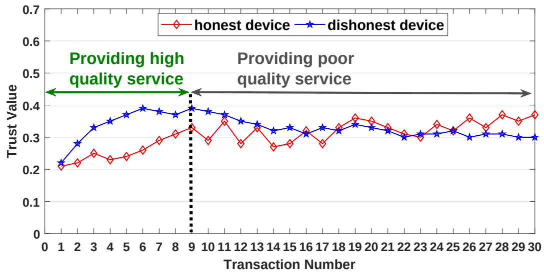
Results: Figs. 5.5(a) to 5.5(b) depict the trust results of a service-consuming device toward the honest and the dishonest devices, who provide or consume services without attack and with attacks including BMA-MSA, SPA, and OOA. From these figures, we can see that the trust value of the honest device always has increased in all the cases while the trust value of the dishonest device decreases, which shows the trust convergence, and accuracy properties. From Fig. 5.5(b), we can see that, although the trust value of the dishonest device has been promoted by good recommendation of other dishonest devices, its trust value decreases quickly after it provides poor quality services. Moreover, although the trust value of the honest device was ruined by wrong recommendations, its trust value increases after providing good service. Because, MCTSM can reduce the impact of the wrong recommendations by applying the context-aware QoS similarity base trust (see *CQoSSTrust*, subsection 4.1) in the MCRSE model, which shows the real ability of a device in providing services, and by applying the context-aware social similarity based trust (see *CSSTrust*, subsection 4.1) in the MCTSR model, which considers the trustworthy of recommender. From Fig. 5.5(c), we can see that the dishonest device boosts its importance (by providing a good recommendation for itself) from transaction numbers 1 to 9, to be selected as a service provider, but then from transaction 10 it provides poor quality services. Our model decreases the trust value of the dishonest device when it starts to provide



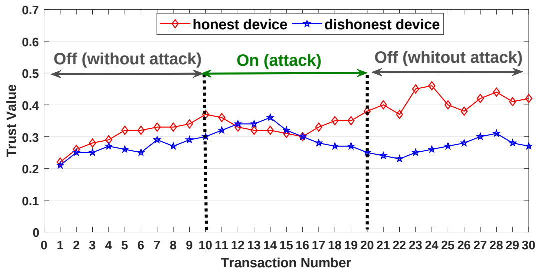
(a) Without attack



(b) Bad-Mouthing and Ballot-Stuffing Attacks



(c) Self-Promoting Attack



(d) On-Off Attack

FIGURE 5.5: The effect of feedback and context on the trust value of a dishonest and an honest devices

poor quality services by applying the variance of feedback. From Fig. 5.5(d), we can see that when dishonest devices perform OOA, they behave alternatively well and badly. The MCTSM with consideration of the contextual feedback of trust and its variance can detect this attack.

Analysis: The experimental results illustrate that: (1) when an honest device provides high quality services and acts cooperatively, MCTSM increases the trust value of an honest device; (2) when a dishonest device provides poor quality services and acts maliciously, performing different types of attack, MCTSM decreases the trust value of the dishonest device. Thus, MCTSM is able to distinguish honest and dishonest devices more accurately.

5.3 Conclusion

The above experimental results have demonstrated that our proposed model considers the multi-contexts of the trust and thus is more accurate in selecting services with a high service quality and in recommending the best services in comparison with the baseline models. Moreover, our model, by having convergence, accuracy and resiliency properties in computing the trust value of devices, is able to distinguish honest and dishonest devices more accurately.

6 Conclusion

6.1 Conclusion

In SIoT environments, trust management has been taken as an important task [16–18, 21, 41, 43, 44]. In this thesis, we have proposed contexts of trust between devices in SIoT environments by considering different contextual aspects between devices in IoT environments and their owners in OSNs. Therefore, we have identified three important contexts of trust in SIoT environments including *Status* of a device, *Environment* of a device (time and location), and *Task type*. Then, we have proposed several metrics of contextual trust which affect service evaluation and service recommendation, including independent and dependent metrics of contextual trust. Independent metrics refer to contextual QoS based trust evaluation and dependent metrics refer to contextual social based trust between a service-providing and service-consuming device. Finally, based on the proposed contextual metrics, we have proposed a Mutual Context-aware Trustworthy Service Management (MCTSM) model, which consists of a Mutual Context-aware Trustworthy Service Evaluation (MCTSE) model and a Mutual Context-aware Trustworthy

Service Recommendation (MCTSR) model in SIoT environments for trust enhanced service evaluation and recommendation. Moreover, in MCTSM, the service-consuming device and the service-providing device perform mutual evaluation of the trustworthiness. The experimental results on a synthetic dataset have demonstrated that the MCTSM model can outperform three state-of-the-art models effectively in evaluating the trustworthiness of service-providing devices and service-consuming devices. Then, it can effectively identify honest and dishonest devices. Moreover, our model can select the most trustworthy services which provide the requested services with high quality and recommend them to service-consuming devices with high accuracy. We have demonstrated that MCTSM provides resiliency against some malicious attacks of dishonest devices including SPA, BMA, BSA, and OOA. However, our approach maybe is vulnerable to attacks when there are malicious devices that may provide malicious services with other attacks like *Whitewashing Attacks (WA)* (where dishonest devices can disappear to dismantle their bad reputation), *Discriminatory Attacks (DA)* (where dishonest devices can launch a discriminatory attack on devices whose owners do not have strong social ties because of the human propensity towards friends in SIoT environments), and *Opportunistic Service Attacks (OSA)* (a dishonest device can provide high quality service to opportunistically get a high reputation, especially when it detects that its reputation is falling because of providing poor quality service) [14, 15]. Our proposed approach maybe is vulnerable to these types of attacks because we do not consider solution for them as well as we do not test these types of attacks yet.

6.2 Future Work

In our future work, we plan to extend our proposed trust management model to detect such attacks, and to add an adaptive MCTSM to dynamically adjust trust parameter settings to minimise trust estimation bias and maximise application performance. Moreover, we plan to propose a *Context-aware Trustworthy Service Composition* for SIoT environments to satisfy the indicated functionality requirement of service-consuming devices; it is essential to successfully compose different services as a service composition. In addition, We are going to improve our MCTSM model by considering the importance of the parameters such as time and resources due to the limited processing power of IoT devices.

A

Appendix

Algorithms Applied in Chapter 5

Algorithm 5: Trust-related attacks **(SPA-OOA)** by dishonest devices in SIoT environment ($Alg_{SPA,OOA}$)

Input: d_i, attack, $Current_{transactNum}$, $Fix_{transactNum}$

Output: ground truth of d_i

/* d_i denote a dishonest device, $Current_{transactNum}$ denote current transaction number, and $Fix_{transactNum}$ denote the transaction number that d_i will start to perform SPA */

begin
- **switch** *attack* **do**
  - **case** *SPA* **do**
    - **if** $Current_{transactNum} > Fix_{transactNum}$ **then**
      - $ground\ truth\ of\ d_i \leftarrow 0.55$;
      - /* d_i starts to provide poor quality services */
    - **else**
      - $ground\ truth\ of\ d_i \leftarrow 0.85$;
      - /* d_i starts to provide high quality services to collect good recommendation for itself */
    - **end**
  - **case** *OOA* **do**
    - $ground\ truth\ of\ d_i \leftarrow a\ random\ number$;
    - /* select a random number between 0.5 and 0.85 */
    - **if** *ground truth of* d_i *is less than 0.5* **then**
      - d_i starts to perform BMA and BSA attacks for other devices ;
      - /* call $Alg_{BMA,BSA}$ when d_i asked to send recommendation for d_j. Also, d_i provides poor quality services */
    - **else**
      - d_i starts to provide services without performing attack;
    - **end**
- **end**
- **return** ground truth of d_i

end

Algorithm 6: Trust-related attacks **(BMA-BSA)** by dishonest devices in SIoT environment ($Alg_{BMA,BSA}$)

Input: d_i, d_j, attack, transactNum

Output: $MCTR^{C_S,C_E,C_T}_{d_i \to d_j}$

/* d_i denote a dishonest device, d_j denote a dishonest or an honest device, $Current_{transactNum}$ denote current transaction number */

begin
- **switch** *attack* **do**
  - **case** *BMA* **do**
    - **if** d_j *is honest device* **then**
      - $MCTR^{C_S,C_E,C_T}_{d_i \to d_j} \leftarrow 0.55$;
      - /* d_i provide bad recommendation for an honest device */
    - **else**
      - d_i starts to provide services without performing attack;
    - **end**
  - **case** *BSA* **do**
    - **if** d_j *is dishonest device* **then**
      - $MCTR^{C_S,C_E,C_T}_{d_i \to d_j} \leftarrow 0.85$;
      - /* d_i provide good recommendation for a dishonest device */
    - **else**
      - d_i starts to provide services without performing attack;
    - **end**
- **end**
- **return** $MCTR^{C_S,C_E,C_T}_{d_i \to d_j}$

end

References

[1] L. Atzori, A. Iera, G. Morabito, and M. Nitti. *The social internet of things (siot) – when social networks meet the internet of things: Concept, architecture and network characterization*. Computer Networks **56**(16), 3594 (2012). 1, 2, 3, 22

[2] L. Atzori, A. Iera, and G. Morabito. *Siot: Giving a social structure to the internet of things*. IEEE Communications Letters **15**(11), 1193 (2011). 1, 3, 22

[3] L. Atzori, A. Iera, and G. Morabito. *From "smart objects" to "social objects": The next evolutionary step of the internet of things*. IEEE Communications Magazine **52**(1), 97 (2014). 1, 22

[4] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke. *Middleware for internet of things: A survey*. IEEE Internet of Things Journal **3**(1), 70 (2016). 1

[5] H. Z. Asl, A. Iera, L. Atzori, and G. Morabito. *How often social objects meet each other? analysis of the properties of a social network of iot devices based on real data*. 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA pp. 2804–2809 (2013). 1

[6] E. Borgia. *The internet of things vision: Key features, applications and open issues*. Computer Communications **54**, 1 (2014). 1, 22

[7] R. Girau, M. Nitti, and L. Atzori. *Implementation of an experimental platform for the social internet of things*. 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing pp. 500–505 (2013).

[8] R. Girau, S. Martis, and L. Atzori. *Lysis: A platform for iot distributed applications over socially connected objects*. IEEE Internet of Things Journal **4**(1), 40 (2017). 1, 22

[9] N. Truong, H. Lee, B. Askwith, and G. M. Lee. *Toward a trust evaluation mechanism in the social internet of things*. Sensors **17**, 1346 (2017). 2, 3, 25

[10] D. Hussein, S. N. Han, G. M. Lee, N. Crespi, and E. Bertin. *Towards a dynamic discovery of smart services in the social internet of things*. Comput. Electr. Eng. **58**, 429 (2017). 2

[11] A. Jayatilaka, Y. Su, and D. C. Ranasinghe. *Hotaal: Home of social things meet ambient assisted living*. 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops) pp. 1–3 (2016). 2

[12] J. E. Kim, X. Fan, and D. Mosse. *Empowering end users for social internet of things*. Proceedings of the Second International Conference on Internet-of-Things Design and Implementation pp. 71–82 (2017). 2

[13] J. Guo, I.-R. Chen, and J. J. Tsai. *A survey of trust computation models for service management in internet of things systems*. Computer Communications **97**, 1 (2017). 2, 3, 4, 7, 8, 9, 25

[14] J. Guo and I. R. Chen. *A classification of trust computation models for service-oriented internet of things systems*. 2015 IEEE International Conference on Services Computing pp. 324–331 (2015). 3, 4, 7, 8, 9, 50

[15] W. Abdelghani, C. A. Zayani, I. Amous, and F. Sèdes. *Trust management in social internet of things: A survey*. Social Media: The Good, the Bad, and the Ugly: 15th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society pp. 430–441 (2016). 8, 50

[16] I. R. Chen, F. Bao, and J. Guo. *Trust-based service management for social internet of things systems*. IEEE Transactions on Dependable and Secure Computing **13**(6), 684 (2016). 3, 8, 25, 26, 49

[17] I. R. Chen, J. Guo, and F. Bao. *Trust management for soa-based iot and its application to service composition*. IEEE Transactions on Services Computing **9**(3), 482 (2016). 8, 9, 12, 16, 26, 32, 43

[18] Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent. *Trust management system design for the internet of things: A context-aware and multi-service approach*. Computers and Security **39**, 351 (2013). 3, 8, 13, 16, 17, 25, 26, 49

[19] K. Hoffman, D. Zage, and C. Nita-Rotaru. *A survey of attack and defense techniques for reputation systems*. ACM Computing Surveys **42**(1), 1–31 (2009). 2, 9

[20] X. Xu, N. Bessis, and J. Cao. *An autonomic agent trust model for iot systems*. Procedia Computer Science **21**, 107 (2013). 2, 7

[21] Z. Lin and L. Dong. *Clarifying trust in social internet of things*. IEEE Transactions on Knowledge and Data Engineering **30**(2), 234 (2018). 2, 3, 7, 8, 13, 16, 17, 25, 26, 49

[22] Y. Lei, L. Chungui, and T. Sen. *Community medical network (cmn): Architecture and implementation*. Global Mobile Congress pp. 1–6 (2011). 2, 8

[23] L.-H. Vu, M. Hauswirth, and K. Aberer. *Qos-based service selection and ranking with trust and reputation management*. On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE pp. 466–483 (2005). 2, 7, 10

[24] A. Josang, R. Ismail, and C. A. Boyd. *A survey of trust and reputation systems for online service provision*. Decision Support Systems **43**(2), 618 (2007).

[25] Z. Malik and A. Bouguettaya. *Rateweb: Reputation assessment for trust establishment among web services*. The VLDB Journal **18**(4), 885 (2009). 10, 14

[26] X. Meng, T. Li, and Y. Deng. *prefertrust: An ordered preferences-based trust model in peer-to-peer networks*. Journal of Systems and Software **113**, 309 (2016). 10

[27] A. B. Can and B. Bhargava. *Sort: A self-organizing trust model for peer-to-peer systems*. IEEE Transactions on Dependable and Secure Computing **10**(1), 14 (2013). 10

[28] X. Fan, M. Li, J. Ma, Y. Ren, H. Zhao, and Z. Su. *Behavior-based reputation management in p2p file-sharing networks*. Journal of Computer and System Sciences **78**(6), 1737 (2012).

[29] L. Li. *Trust evaluation in service-oriented environments*. PhD thesis, Macquarie University (2011).

[30] Y. Wang, Y. Lu, I. Chen, J. Cho, and A. Swami. *Logittrust: A logit regression-based trust model for mobile ad hoc networks*. 6th ASE International Conference on Privacy, Security, Risk and Trust (2014). 2, 7

[31] U. Kuter and J. Golbeck. *Using probabilistic confidence models for trust inference in web-based social networks*. ACM Trans. Internet Technol. **10**(2), 1 (2010). 2, 7, 10

[32] G. Liu, Y. Wang, M. A. Orgun, and E. P. Lim. *A heuristic algorithm for trust-oriented service provider selection in complex social networks*. 2010 IEEE International Conference on Services Computing pp. 130–137 (2010).

[33] G. Liu, Y. Wang, M. A. Orgun, and E. P. Lim. *Finding the optimal social trust path for the selection of trustworthy service providers in complex social networks*. IEEE Transactions on Services Computing **6**(2), 152 (2013).

[34] Y. Wang, L. Li, and G. Liu. *Social context-aware trust inference for trust enhancement in social network based recommendations on service providers*. World Wide Web **18**(1), 159 (2015). 11, 19, 21, 38

[35] H. Ma, T. C. Zhou, M. R. Lyu, and I. King. *Improving recommender systems by incorporating social contextual information*. ACM Trans. Inf. Syst. **29**(2), 1 (2011). 11

[36] Z. Zhang and K. Wang. *A trust model for multimedia social networks*. Social Network Analysis and Mining **3**(4), 969 (2013). 11

[37] G. Guo, J. Zhang, and N. Yorke-Smith. *A novel recommendation model regularized with user trust and item ratings*. IEEE Transactions on Knowledge and Data Engineering **28**(7), 1607 (2016). 2, 7, 11

[38] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou. *A roadmap for security challenges in the internet of things*. Digital Communications and Networks (2017). 2, 7, 11

[39] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang. *Trm-iot: A trust management model based on fuzzy reputation for internet of things*. ComSIS **8**(4) (2011). 8, 9, 11, 32

[40] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini. *Security, privacy and trust in internet of things: The road ahead*. Computer Networks **76**, 146 (2015). 11

[41] Z. Yan, P. Zhang, and A. V. Vasilakos. *A survey on trust management for internet of things*. Journal of Network and Computer Applications **42**, 120 (2014). 3, 8, 11, 25, 49

[42] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke. *Middleware for internet of things: A survey*. IEEE Internet of Things Journal **3**(1), 70 (2016). 2, 7, 11

[43] M. Nitti, R. Girau, and L. Atzori. *Trustworthiness management in the social internet of things*. IEEE Transactions on Knowledge and Data Engineering **26**(5), 1253 (2014). 3, 8, 9, 13, 16, 25, 26, 32, 43, 49

[44] Z. Chen, R. Ling, C.-M. Huang, and X. Zhu. *A scheme of access service recommendation for the social internet of things*. International Journal of Communication Systems **29**(4), 694 (2015). 12, 16, 21, 26, 49

[45] H. Xiao, N. Sidhu, and B. Christianson. *Guarantor and reputation based trust model for social internet of things*. 2015 International Wireless Communications and Mobile Computing Conference (IWCMC) pp. 600–605 (2015).

[46] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito. *A subjective model for trustworthiness evaluation in the social internet of things*. 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC) pp. 18–23 (2012). 9, 13

[47] U. Jayasinghe, N. B. Truong, G. M. Lee, and T. W. Um. *Rpr: A trust computation model for social internet of things*. 2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress pp. 930–937 (2016). 3, 25

[48] S. Wang, L. Huang, C.-H. Hsu, and F. Yang. *Collaboration reputation for trustworthy web service selection in social networks*. Computer and System Sciences **82**, 130 (2016). 7

[49] A. M. Ortiz, D. Hussein, S. Park, S. N. Han, and N. Crespi. *The cluster between internet of things and social networks: Review and research challenges*. IEEE Internet of Things Journal **1**(3), 206 (2014). 7

[50] Z. Yan and S. Holtmanns. *Trust modeling and management: from social trust to digital trust*. Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions, IGI Global pp. 290–323 (2008). 8

[51] F. Bao and I.-R. Chen. *Dynamic trust management for internet of things applications*. Proceedings of the 2012 International Workshop on Self-aware Internet of Things pp. 1–6 (2012). 8, 9, 12, 16, 26

[52] F. Bao, I. R. Chen, and J. Guo. *Scalable, adaptive and survivable trust management for community of interest based internet of things systems*. 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS) pp. 1–7 (2013). 8, 9, 12, 16, 26, 32

[53] I. R. Chen and J. Guo. *Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection*. 2014 IEEE 28th International Conference on Advanced Information Networking and Applications pp. 49–56 (2014). 8

[54] I. R. Chen, F. Bao, M. Chang, and J. H. Cho. *Trust management for encounter-based routing in delay tolerant networks*. 2010 IEEE Global Telecommunications Conference GLOBECOM 2010 pp. 1–6 (2010). 9

[55] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. *The eigentrust algorithm for reputation management in p2p networks*. Proceedings of the 12th International Conference on World Wide Web pp. 640–651 (2003). 9

[56] L. Xiong and L. Liu. *Peertrust: supporting reputation-based trust for peer-to-peer electronic communities*. IEEE Transactions on Knowledge and Data Engineering **16**(7), 843 (2004). 10

[57] I. R. Chen, J. Guo, F. Bao, and J. H. Cho. *Integrated social and quality of service trust management of mobile groups in ad hoc networks*. 9th International Conference on Information, Communications Signal Processing pp. 1–5 (2013). 10

[58] Y. Wang, K.-J. Lin, D. Wong, and V. Varadharajan. *Trust management towards service-oriented applications*. Service Oriented Computing and Applications **3**, 129 (2009). 10

[59] P. Dewan and P. Dasgupta. *P2p reputation management using distributed identities and decentralized recommendation chains*. IEEE Transactions on Knowledge and Data Engineering **22**(7), 1000 (2010). 10

[60] G. Liu. *Trust management in online social networks*. PhD thesis, Macquarie University (2013). 10

[61] F. Bao and I.-R. Chen. *Trust management for the internet of things and its application to service composition*. 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM) pp. 1–6 (2012). 12, 16

[62] N. Griffiths. *Task delegation using experience-based multi-dimensional trust*. AAMAS (2005). 14

[63] M. Gias Uddin, M. Zulkernine, and S. Ahamed. *Cat: A context-aware trust model for open and dynamic systems*. Proceedings of the 2008 ACM Symposium on Applied Computing pp. 2024–2029 (2008). 14

[64] X. Liu and A. Datta. *Contextual trust aided enhancement of data availability in peer-to-peer backup storage systems*. Journal of Network and Systems Management **20**(2), 200 (2012). 14

[65] W. Sherchan, S. Nepal, and C. Paris. *A survey of trust in social networks*. ACM Comput. Surv. **45**(4), 47:1 (2013). 14

[66] H. Zhang. *Context-aware transaction trust computation in e-commerce environments*. PhD thesis, Macquarie University (2014). 14, 17

[67] H. Zhang, Y. Wang, X. Zhang, and E.-P. Lim. *Reputationpro: The efficient approaches to contextual transaction trust computation in e-commerce environments*. TWEB **9**, 2:1 (2015). 14

[68] A. Chen. *Context-aware collaborative filtering system: Predicting the user's preference in the ubiquitous computing environment*. Location- and Context-Awareness pp. 244–253 (2005). 15

[69] L. Liu, F. Lecue, N. Mehandjiev, and L. Xu. *Using context similarity for service recommendation*. IEEE Fourth International Conference on Semantic Computing pp. 277–284.

[70] L. Baltrunas, B. Ludwig, and F. Ricci. *Matrix factorization techniques for context aware recommendation*. RecSys (2011). 15

[71] Y. Zheng, B. Mobasher, and R. Burke. *Cslim: contextual slim recommendation algorithms*. RecSys 2014 - Proceedings of the 8th ACM Conference on Recommender Systems (2014). 15

[72] A. Karatzoglou, X. Amatriain, L. Baltrunas, and N. Oliver. *Multiverse recommendation: n-dimensional tensor factorization for context-aware collaborative filtering*. RecSys (2010). 15

[73] Y. Zheng, B. Mobasher, and R. Burke. *Deviation-based contextual slim recommenders*. Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management pp. 271–280 (2014). 15, 38, 39

[74] D. Lathauwer. *A survey of tensor methods*. EEE International Symposium on Circuits and Systems pp. 2773–2776 (2009). 15

[75] F. Evgeny and O. Ivan. *Tensor methods and recommender systems*. WIREs Data Mining Knowl Discov (2017). 15

[76] C. Zheng, H. E, M. Song, and J. Song. *Cmptf: Contextual modeling probabilistic tensor factorization for recommender systems*. Neurocomputing **205**, 141 (2016). 15

[77] B. L. Baltrunas, Linas Baltrunas and F. Ricci. *Matrix factorization techniques for context aware recommendation* . 15

[78] Y. Zheng, B. Mobasher, and R. Burke. *Correlation-based context-aware matrix factorization*. Proceedings of School of Computing Research Symposium (SOCRS) (2015).

[79] Y. Zheng, B. Mobasher, and R. Burke. *Incorporating context correlation into context-aware matrix factorization*. Proceedings of the 2015 International Conference on Constraints and Preferences for Configuration and Recommendation and Intelligent Techniques for Web Personalization **1440**, 21 (2015). 15

[80] X. Ning and G. Karypis. *Slim: Sparse linear methods for top-n recommender systems*. 2011 IEEE 11th International Conference on Data Mining pp. 497–506 (2011). 15

[81] Y. Zheng, B. Mobasher, and R. Burke. *Integrating context similarity with sparse linear recommendation model*. User Modeling, Adaptation and Personalization pp. 370–376 (2015). 15

[82] Z. Zheng, Y. Zhang, and M. R. Lyu. *Investigating qos of real-world web services*. IEEE Transactions on Services Computing **7**(1), 32 (2014). 18

[83] J. Zou, Y. Wang, and M. Orgun. *A dispute arbitration protocol based on a peer-to-peer service contract management scheme*. 2016 IEEE International Conference on Web Services (ICWS) pp. 41–48 (2016). 32

[84] J. Leskovec. *Stanford large network dataset collection [online].* Available: http://snap.stanford.edu/data/ . 42

[85] S. Kosta, A. Mei, and J. Stefa. *Small world in motion (swim): Modeling communities in ad-hoc mobile networking*. 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON) pp. 1–9 (2010). 42