Context-Aware Trustworthy Service Evaluation in Social Internet of Things

Maryam Khani(✉), Yan Wang(✉), Mehmet A. Orgun, and Feng Zhu

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
{maryam.khani,feng.zhu3}@hdr.mq.edu.au
{yan.wang,mehmet.orgun}@mq.edu.au

Abstract. In Social Internet of Things (SIoT) environments, a large number of users and Internet of Things (IoT) based devices are connected to each other, so that they can share SIoT-based services. 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. Currently, the prevalent trust management mechanisms consider QoS-based trust and social-relation based trust mechanisms in evaluating 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 paper, we first propose three contexts of trust in SIoT environments including the status and environment (time and location) of devices, and the types of tasks. Then, we propose a novel Mutual Context-aware Trustworthy Service Evaluation (MCTSE) model. The experiments demonstrate that our proposed contextual trust evaluation model can effectively differentiate honest and dishonest devices and provide a high success rate in selecting the most trustworthy services and providing high resilience against different attacks from dishonest devices.

Keywords: Social Internet of Things · Contextual trust
Trustworthy service evaluation

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 [1,2,24]. Those *things* include personal devices (*e.g.*, smartphones, tablets), devices fitted with tags (*e.g.*, RFIDs) in our environment, sensors and actuators [24]. 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

C. Pahl et al. (Eds.): ICSOC 2018, LNCS 11236, pp. 129–145, 2018.
https://doi.org/10.1007/978-3-030-03596-9_9

autonomous manner by considering their owners' social networks [1,2]. 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) [1,2].

Recently, a broad range of Social Internet of Things (SIoT) based applications have emerged [1], such as smart traffic management [23], smart airport [26], and smart home [25]. To find the right source of information in such an SIoT environment, a user's devices can connect with other devices which are identified by means of co-location relations. However, devices can be either *honest*, providing good quality services, or *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) [3–5,9]. In order to mitigate against such attacks, the issue of trust evaluation in SIoT environments arises and becomes prominent. Firstly, 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. Secondly, the resources of a service-providing device could be maliciously exploited by some dishonest service-consuming devices [14]. Thirdly, 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.

1.1 Background and Problem

A variety of context-aware trust evaluation approaches have been proposed in Online Social Networks (OSNs) [12,22]. These approaches are mostly concerned with the 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 [16,17,24,28] 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 approaches have been proposed in SIoT environments [3–5,7,14,15,17,23]. To date, SIoT trust evaluation systems use direct evidence, such as QoS-based trust, and indirect experiences, such as social relation based trust, to evaluate the trust level of service-providing devices or 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.,* the status and environment of devices) and the types of tasks. Therefore, they cannot ultimately select the most trustworthy service-providing devices or trustworthy service-consuming devices. A motivating example is given below.

Example 1: 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]. Users want to share the provided services by their devices specially when a device cannot provide requested services from its user. Suppose that users A, B and C register their IoT-based devices (*e.g.*, smartphones, tablets, *etc.*) in the same SIoT-based communities. Then, suppose that the smartphone of user A, has low battery, and thus automatically searches the nearest devices to delegate the task of recording an on-line video from an important event. Suppose, user B is on the way to leave the place where user A is. B has a smartphone, with a low battery. User C is on the way to reach the place where user A is, and 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 (*i.e.*, time and location) of devices are taken into account. 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, and the environment of the devices, and the types of tasks [9]. In the literature, the existing studies on trust evaluation only consider a service-providing device's single context, such as a service context, but a multi-contextual model will be more accurate in evaluating the trustworthiness of devices and thus in demand.

1.2 Contributions

To overcome the above-mentioned drawbacks, this paper proposes a novel Mutual Context-aware Trustworthy Service Evaluation (MCTSE) model in SIoT environments for trust enhanced service evaluation. The characteristics and contributions of our proposed model are summarised as follows:

1. 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.
2. Then, we propose two new concepts Context-aware QoS Similarity based Trust (CQSST) and Context-aware Social Similarity based Trust (CSST), and propose novel models for evaluating them. Then, we apply these new concepts in the MCTSE model to evaluate the trustworthy of service-consuming and service-providing devices.
3. We conduct simulations with 600 randomly generated service-consuming devices and service-providing devices to evaluate the effectiveness of our model. The experimental results show that our model outperforms three

state-of-the-art models effectively in evaluating the trustworthiness of service-providing devices and service-consuming devices. It can also differentiate honest and dishonest devices with a high accuracy which perform tasks without attacks or with different types of attacks, respectively. Therefore, our model can select the most trustworthy services with high quality and with high resilience against different malicious attacks of dishonest devices.

2 Literature Review

In this section, we first review the most relevant the contextual trust evaluation techniques applied in OSNs. We then review the trust management techniques proposed in IoT, and SIoT studies that are related to our work. We categorize the proposed techniques into single-context (one or two simple contexts are applied to trust evaluation) and multi-context (more complicated contexts are applied to trust evaluation).

2.1 Trust Models in Online Social Networks (OSNs)

In the studies of trust evaluation in OSNs, some qualitative approaches have been proposed. As an example of a single-context trust evaluation, Kuter *et al.* [12] 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 an example of multi-context trust evaluation, Liu *et al.* [8] 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. They considered social information including social position, social relation, and preferences of participants to select trustworthy trust paths. Zhan *et al.* [22], in online multimedia social networks, used credible feedback of digital contents, a feedback weighting factor, and user share similarity to evaluate a direct trust between users.

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 Trust Models in Internet of Things (IoT)

In IoT environments, there have been a few studies on trust management models. 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.* [24] proposed different architectures of the IoT, and identified the relevant research challenges in communication problems and information gathering problems. However, they did not propose any solution for security and privacy problems. Zheng *et al.* [17] 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.* [16] reported that trust management systems could be defined as deterministic trust (including policy-based mechanism and certificates systems) and non-deterministic trust (including recommendation-based, reputation-based systems, prediction-based, and social network based systems). Recently, Chen *et al.* [28] 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.

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

2.3 Trust Models in Social Internet of Things (SIoT)

In SIoT environments, the existing trust management systems can be broadly categorised into non-contextual and single contextual methods.

In a non-context-aware trust management model proposed in [6], Bao *et al.* 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. However, the proposed factors for computing cooperativeness based on the percentage of common friends are very simple. Chen *et al.* [7] 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 based on certain social similarities. However, Chen *et al.* did not consider some trust properties such as contextual and dynamic characteristics of trust. Chen *et al.* [5] proposed an adaptive and scalable trustworthy service composition in SOA-based IoT systems. They only apply a single QoS trust to rate a service provider. However, the social relations between devices are not considered.

As a single-context trust management model, Nitti *et al.* [15] proposed a trust computation method which considers both direct and indirect trust. For trust composition, QoS based trust (including transaction service quality and computational capability) and social relation based trust (including centrality, relation factor) are applied. In this model, trust is context-dependent but only factors such as the number of transactions in a QoS based trust is considered as a context. Therefore, their model is a single-context trust. Furthermore, Lin *et al.* [14] proposed a contextual trust management model in which a 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. For trust composition, QoS based trust (*e.g.*, bandwidth, packet loss, *etc.*) and social based trust (social relationships, such as friendship) is applied. However, they only consider the type of task and the situation of the environment as contexts, and they do not consider other contexts such as time, location, and the features of a device, to be multi-context.

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 characteristics of trust in SIoT systems include direct (*e.g.*, QoS-based trust), dynamic, *etc*, which should be considered. In addition, existing trust models in IoT environments do not consider the social relation among devices in SIoT environments.

3 Problem Statement and Metrics of Contextual Trust

3.1 Problem Statement

In our SIoT model, there are M devices which are denoted by $D = \{d_1, ..., d_M\}$ and there are N users which are denoted by $U = \{u_1, ..., u_N\}$. Let the social network between users be represented 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 by considering the social relations o their owner which are represented by $SC = \{SC_1, ..., SC_I\}$ and $SP = \{SP_1, ..., SP_J\}$ respectively. In addition, each of SC_i or SP_j is represented by a vector in a three dimensional space of the contexts in SIoT including status (C_S), environment (C_E), and task type (C_T), which are represented by $C = \{C_S, C_E, C_T\}$. Each of C_S, C_E, C_T has different values presented by $C_S = \{C_{S_1}, ..., C_{S_h}\}$, $C_E = \{C_{E_1}, ..., C_{E_{\acute{h}}}\}$, and $C_T = \{C_{T_1}, ..., C_{T_{\acute{\acute{h}}}}\}$, respectively. The vectors of $\overrightarrow{SC}_i$ and $\overrightarrow{SP}_j$ are represented by Eqs. (1) and (2), respectively. Each of SC_i and SP_j has a list of the owner's friends which is denoted by $UFre_{SC_i}$ and $UFre_{SP_j}$, respectively, and a list of owner's community of interests which is denoted by $UCom_{SC_i}$ and $UCom_{SP_j}$, respectively. Also, let S $= \{s_1, ..., s_l\}$ denote the set of services which are provided or consumed by devices in different time $\tau = \{t_1, ..., t_p\}$, and locations $L = \{l_1, ..., l_q\}$. Moreover, each of SC_i and SP_j has a user satisfaction level or ground truth [19] which is shown by GT_{SC_i} and GT_{SP_j}, respectively. The aim of this paper is to provide a list of trustworthy SPs and SCs for each of SP_i and SC_j in each transaction.

$$\overrightarrow{SC}_i = \begin{bmatrix} C_{S_i} \\ C_{E_i} \\ C_{T_i} \end{bmatrix} \tag{1}$$

$$\overrightarrow{SP}_j = \begin{bmatrix} C_{S_j} \\ C_{E_j} \\ C_{T_j} \end{bmatrix} \tag{2}$$

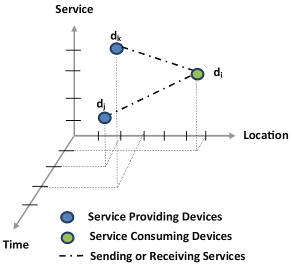

Service
d_k
d_i
d_j
Location
Time
Service Providing Devices
Service Consuming Devices
Sending or Receiving Services

Fig. 1. Contexts of Trust in IoT environments

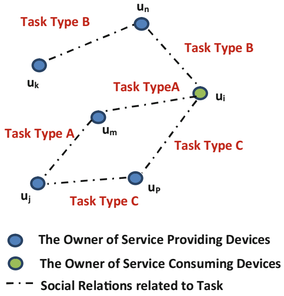

u_n
Task Type B
Task Type B
u_k
Task TypeA
u_i
Task Type A
u_m
Task Type C
u_j
u_p
Task Type C
The Owner of Service Providing Devices
The Owner of Service Consuming Devices
Social Relations related to Task

Fig. 2. Contexts of Trust in OSN

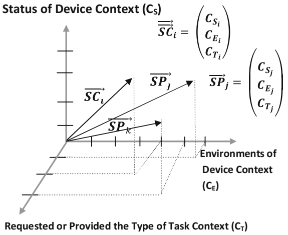

Status of Device Context (C_S)
$\overrightarrow{SC}_i = \begin{pmatrix} C_{S_i} \\ C_{E_i} \\ C_{T_i} \end{pmatrix}$
$\overrightarrow{SC_i}$
$\overrightarrow{SP_j}$
$\overrightarrow{SP}_j = \begin{pmatrix} C_{S_j} \\ C_{E_j} \\ C_{T_j} \end{pmatrix}$
$\overrightarrow{SP_k}$
Environments of Device Context (C_E)
Requested or Provided the Type of Task Context (C_T)

Fig. 3. Contexts of Trust in SIoT environments

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 OSN [27] 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. 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 u_i of d_j and the owner u_k of d_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. 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. Figure 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 in the three-dimensional space of contexts including the status of devices, environment (time and location) of devices, and the types of tasks. The contexts of trust in SIoT environments are described as follows.

- **The Status of a device (C_S):** The features of devices such as energy, and the capability of computing.
- **The 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 hours, next 3 hours, and *etc.*).

- **Task type (C_T):** For example, a service-consuming device could trust a service-providing device for task type A but 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.

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 performance, cost, availability, *etc.* The independent metrics include expected QoS and advertised QoS. Each of these parameters is shown in a vector in the two-dimensional space of the status and environment contexts of trust.

- Let $\overrightarrow{\boldsymbol{ExQoS}}_{\boldsymbol{SCi}}^{\boldsymbol{C_S,C_E}}$ 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 $\overrightarrow{\boldsymbol{AdQoS}}_{\boldsymbol{SP_j}}^{\boldsymbol{C_S,C_E}}$ 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 Eqs. (3) and (4) respectively.

$$\overrightarrow{ExQoS}_{SCi}^{C_S,C_E} = \begin{bmatrix} C_{S_j} \\ C_{E_j} \end{bmatrix} \tag{3}$$

$$\overrightarrow{AdQoS}_{SP_j}^{C_S,C_E} = \begin{bmatrix} C_{S_i} \\ C_{E_i} \end{bmatrix} \tag{4}$$

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 context of task type. 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.

- Let $\boldsymbol{SSimFre^{C_T}_{SC_i,SP_j}}$ denote the *Social Similarity Friendship (SSimFre)* that captures the degree of the common social friends between the owner of a service-consuming device i and the owner 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. After two service-providing and service-consuming devices exchange the friend lists of their owners [2], *i.e.*, $UFre_{SC_i}$ and $UFre_{SP_j}$, they can compute two binary lists including $LFre^{C_T}_{SC_i}$ and $LFre^{C_T}_{SP_j}$ where the size of each list is equal to $S_{Fre} = |UFre_{SC_i} \cup UFre_{SP_j}|$. Each element in these lists will be 1 if the corresponding owner is in $UFre_{SC_i}$ or $(UFre_{SP_j})$ and has a relationship in the specific task type context C_T with SC_i or (SP_j), otherwise 0. The metric of $SSimFre^{C_T}_{SC_i,SP_j}$ is calculated by Eq. (5).

$$SSimFre^{C_T}_{SC_i,SP_j} = \frac{LFre^{C_T}_{SC_i}.LFre^{C_T}_{SP_j}}{S_{Fre}} = \frac{\sum_{\acute{h}=1}^{h} LFre^{C_T}_{SC_i}[\acute{h}].LFre^{C_T}_{SP_j}[\acute{h}]}{S_{Fre}} \qquad (5)$$

- Let $\boldsymbol{SSimCom^{C_T}_{SC_i,SP_j}}$ denote the *Social Similarity Community (SSimCom)* that captures the degree of the common communities between the owner of a service-consuming device i and the owner 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, the two service-providing and service-consuming devices exchange the lists of community interest of their owners [2], $UCom_{SC_i}$ and $UCom_{SP_j}$. Then, they compute two binary lists including $LCom^{C_T}_{SC_i}$ and $LCom^{C_T}_{SP_j}$ where the size of each list is equal to $S_{Com} = |UCom_{SC_i} \cup UCom_{SP_j}|$. 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 metric of $SSimFre^{C_T}_{SC_i,SP_j}$ is calculated by Eq. (6).

$$SSimCom^{C_T}_{SC_i,SP_j} = \frac{LCom^{C_T}_{SC_i}.LCom^{C_T}_{SP_j}}{S_{Com}} = \frac{\sum_{\acute{q}=1}^{q} LCom^{C_T}_{SC_i}[\acute{q}].LCom^{C_T}_{SP_j}[\acute{q}]}{S_{Com}} \qquad (6)$$

- Let $\boldsymbol{SSimR^{C_T}_{SC_i,SP_j}}$ denote the *Social Similarity Relation (SSimR)* that captures the degree of common social relations (*e.g.* ownership, co-work, co-location, parental) [1,2] between a service-providing device j with a service-consuming device i at the task type context. We consider different weighted values for each device social relations with other devices which are listed in Table 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 to 0.9. Moreover, if there are different social relations between two devices, only the highest weight is considered.

Table 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

- Let $\boldsymbol{CFT^{C_S,C_E,C_T}_{SP_j\rightarrow SC_i}(n-1)}$ and $\boldsymbol{CFT^{C_S,C_E,C_T}_{SC_i\rightarrow SP_j}(n-1)}$ denote the *Contextual Feedback of Trust (CFT)* in the view of SC_i and in the view of SP_j respectively, where n denotes the number of transactions between SC_i and SP_j in the status and environment contexts of devices and the task type context. $CFT^{C_S,C_E,C_T}_{SP_j\rightarrow SC_i}(n-1)$ denotes the previous direct feedback of a service-providing device j toward a service-consuming device i at status and environment contexts of devices and the task type context and $CFT^{C_S,C_E,C_T}_{SC_i\rightarrow SP_j}(n-1)$ denotes the previous direct feedback of the service-consuming device i toward service-providing device j in the status and environment contexts of device and the task type context, if there is any direct feedback. Moreover, let $\boldsymbol{Variance^{C_S,C_E,C_T}_{SC_i\rightarrow SP_j}(K)}$ denote the *Variance* of $CFT^{C_S,C_E,C_T}_{SC_i\rightarrow SP_j}(n-1)$ in its K latest transactions and let $\boldsymbol{Variance^{C_S,C_E,C_T}_{SP_j\rightarrow SC_i}(K)}$ denote the *Variance* of $CFT^{C_S,C_E,C_T}_{SP_j\rightarrow SC_i}(n-1)$ in its K latest transactions. The metrics of $Variance^{C_S,C_E,C_T}_{SC_i\rightarrow SP_j}(K)$ and $Variance^{C_S,C_E,C_T}_{SP_j\rightarrow SC_i}(K)$ are calculated by Eqs. (7), (8), (9) and (10) respectively. Then, the metrics of $e^{Variance^{C_S,C_E,C_T}_{SC_i\rightarrow SP_j}(K)}$ and $e^{Variance^{C_S,C_E,C_T}_{SP_j\rightarrow SC_i}(K)}$ have been considered as coefficients applied to the previous direct feedback of service-providing device in our MCTSE model. Therefore, if there is more variance in K latest transactions of a device, it means that it was a dishonest device. Therefore, its dishonest behaviour is memorized and it decreases the importance of its previous direct feedback. We apply the e^{-x} function where x is equal to 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 $Variance$ between 0 and 1.

$$Variance^{C_S,C_E,C_T}_{SC_i\rightarrow SP_j}(K) = \frac{\sum_{x=n-k}^{n}(CFT^{C_S,C_E,C_T}_{SC_i\rightarrow SP_j}(x) - \overline{\text{CFT}}^{C_S,C_E,C_T}_{SC_i\rightarrow SP_j}(K))^2}{k-1} \tag{7}$$

$$Variance^{C_S,C_E,C_T}_{SP_j\rightarrow SC_i}(K) = \frac{\sum_{x=n-k}^{n}(CFT^{C_S,C_E,C_T}_{SP_j\rightarrow SC_i}(x) - \overline{\text{CFT}}^{C_S,C_E,C_T}_{SP_j\rightarrow SC_i}(K))^2}{k-1} \tag{8}$$

$$\overline{\text{CFT}}^{C_S,C_E,C_T}_{SC_i\rightarrow SP_j}(K) = \frac{\sum_{x=n-k}^{n}CFT^{C_S,C_E,C_T}_{SC_i\rightarrow SP_j}(x)}{K} \tag{9}$$

$$\overline{\text{CFT}}^{C_S,C_E,C_T}_{SP_j\rightarrow SC_i}(K) = \frac{\sum_{x=n-k}^{n}CFT^{C_S,C_E,C_T}_{SP_j\rightarrow SC_i}(x)}{K} \tag{10}$$

4 Mutual Context-Aware Trustworthy Service Evaluation (MCTSE) Model

4.1 Overview of the MCTSE Model

In our proposed MCTSE Model, we consider two concepts, including *Context-aware QoS Similarity based Trust*, *Context-aware Social Similarity based Trust*, in the computation of MCTSE, which are described below.

- **Context-aware QoS Similarity based Trust (CQoSSTrust):** Let $CQoSSTrust^{C_S,C_E}_{SC_i,SP_j}$ denote the *Context-aware QoS similarity based Trust* that captures the degree of similarity between the expected Quality of Service which is requested by a service-consuming device i and the advertised quality of service 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 $\overrightarrow{ExQoS}^{C_S,C_E}_{SC_i}$ and $\overrightarrow{AdQoS}^{C_S,C_E}_{SP_j}$. Therefore, $CQoSSTrust^{C_S,C_E}_{SC_i,SP_j}$ is calculated by Eg. (11). As the maximum QoS similarity based trust, $CQoSSTrust^{C_S,C_E}_{SC_i,SP_j}= 1$ captures that the SP_j can provide the maximum expected QoSs of SC_i while $CQoSSTrust^{C_S,C_E}_{SC_i,SP_j}=$ 0 indicates that there is no similarity between the expected QoSs of SC_i and the advertised QoSs of SP_j. If $\overrightarrow{ExQoS}^{C_S,C_E}_{SC_i}$ = A and $\overrightarrow{AdQoS}^{C_S,C_E}_{SP_j} = B$ then:

$$CQoSSTrust^{C_S,C_E}_{SC_i,SP_j} = \cos(\theta) = |\overrightarrow{A} \times \overrightarrow{B}| = \frac{A.B}{\parallel A \parallel_2 \parallel B \parallel_2} = \frac{\sum_{\acute{h}=1}^{h} A_{\acute{h}}.B_{\acute{h}}}{\sqrt{\sum_{\acute{h}=1}^{h} A^2_{\acute{h}}}\sqrt{\sum_{\acute{h}=1}^{h} B^2_{\acute{h}}}} \tag{11}$$

- **Context-aware Social Similarity based Trust (CSSTrust):** Let $CSSTrust^{C_T}_{SC_i,SP_j}$ denote the *Context-aware Social Similarity based Trust* that indicates the overall degree of social similarity between service consumer SC_i and service provider SP_j at the task type context. Equations (12), (13), and (14) are applied to compute $CSSTrust^{C_T}_{SC_i,SP_j}$. We apply the e^{-x} function in Eq. (12) where x is equal to $SDissimilarity^{C_T}$ (it denotes *Social Dissimilarity* between SC_i and SP_j in the task type context) because the more the 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. 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 a less trust value between the owners of devices. The social factors including social similarity friendship, social similarity community, social similarity relations may have different importance. Therefore, weight parameters w_i are applied to adjust the importance of these three social similarity factors.

$$CSSTrust^{C_T}_{SC_i,SP_j} = e^{-SDissimilarity^{C_T}} \tag{12}$$

$$SDissimilarity^{C_T} = 1 - SSimilarity^{C_T} \tag{13}$$

$$SSimilarity^{C_T} = w_1 \times SSimFre^{C_T}_{SC_i,SP_j} + w_2 \times SSimCom^{C_T}_{SC_i,SP_j} + w_3 \times SSimR^{C_T}_{SC_i,SP_j} \tag{14}$$

4.2 Assessing Trust in SIoT Environments by 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: (1) *Trustworthy Service Evaluation from Service-Consuming Device i to Service-Providing Device j* ($MCTSE^{C_S,C_E,C_T}_{SC_i \rightarrow SP_j}$). It is calculated by Eq.(15). It denotes the direct trust value from service-consuming device j to service-providing device i. (2) *Trustworthy Service Evaluation from Service Providing Device j to Service-Consuming Device i* ($MCTSE^{C_S,C_E,C_T}_{SP_j \rightarrow SC_i}$). It is calculated by Eq.(16). It denotes the direct trust value from 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 $CQoSSTrust^{C_S,C_E}_{SC_i,SP_j}$, $CSSTrust^{C_T}_{SC_i,SP_j}$, $CFT^{C_S,C_E,C_T}_{SC_i \rightarrow SP_j}$ and $CFT^{C_S,C_E,C_T}_{SP_j \rightarrow SC_i}$.

$$\begin{aligned} MCTSE^{C_S,C_E,C_T}_{SC_i \rightarrow SP_j} &= \delta \times CQoSSTrust^{C_S,C_E}_{SC_i,SP_j} \times CSSTrust^{C_T}_{SC_i,SP_j} \\ &+ (1-\delta) \times e^{Variance^{C_S,C_E,C_T}_{SC_i \rightarrow SP_j}(K)} \times CFT^{C_S,C_E,C_T}_{SC_i \rightarrow SP_j}(n-1). \end{aligned} \tag{15}$$

$$\begin{aligned} MCTSE^{C_S,C_T}_{SP_j \rightarrow SC_i} &= \delta \times CQoSSTrust^{C_S}_{SC_i,SP_j} \\ +(1-\delta) \times e^{Variance^{C_S,C_E,C_T}_{SP_j \rightarrow SC_i}(K)} &\times CFT^{C_S,C_E,C_T}_{SP_j \rightarrow SC_i}(n-1). \end{aligned} \tag{16}$$

5 Experiments

In this section, we introduce two experiments of our proposed MCTSE model in a simulation where 300 service-consuming devices need to select the most trustworthy service-providing devices from 300 service-providing devices.

5.1 Simulation Settings and Performance Comparison in SIoT Environments

To simulate an SIoT environment, because there is a lack of a 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 the synthetic dataset of the online social network Facebook obtained from the synthetic Stanford Large Network Dataset Collection [13]. We assume that each user owns two devices on average. Each device has a role as either 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 respectively. The percentage of dishonest devices is set to 0% and 50% respectively. The dishonest devices perform trust related attacks including BMA, BSA, SPA, and OOA. 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"*. We compute the trust values of all honest or dishonest devices using our proposed model and compare with the *"ground truth"* to assess the accuracy of our model. For each honest device, a random value in the range of [0.80, 0.85] is assigned to its ground truth (it shows that an honest device provides high-quality service), and for each a 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 the 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. In this paper, we select three state-of-the-art trust management models in this field as the baseline models. They are (1) SOA [5], as a non-context trust management model, (2) SubM [15] and (3) ObjM [15], as two single-context trust management models, which are subjective and objective models respectively. Each of these models is implemented using C# programming. Then, trust-related attacks are modeled by applying their descriptions [3–5,9].

5.2 Experiment 1: Effectiveness of Trustworthy Service Evaluation

Results & Analysis: Figure 4 shows the success rates of the MCTSE, SOA, SubM, and ObjM models when there are different percentages of dishonest devices (0% and 50%). When there are 50 % dishonest devices, we consider three cases of different attacks, *i.e*, with BMA-BSA, with SPA, and with OOA, respectively. From Fig. 4, we can see that MCTSE always has the best success rate in all the cases. On average, MCTSE is 2%, 13.8%, 7.4%, 10.6%, and 10.2% higher in success rate than the average of the three baseline models when there are 0% and 50% dishonest devices who provide or consume services "without attacks" and "with attacks" including BMA-MSA, SPA, and OOA respectively.

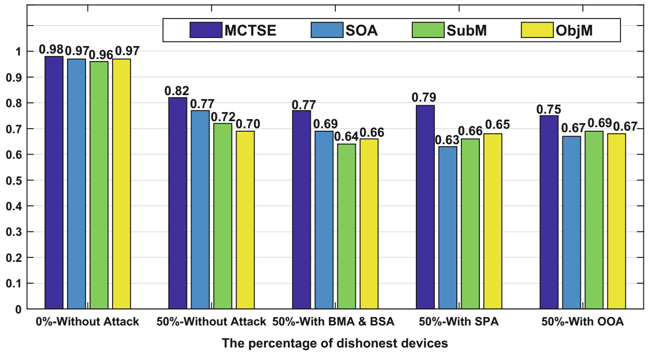
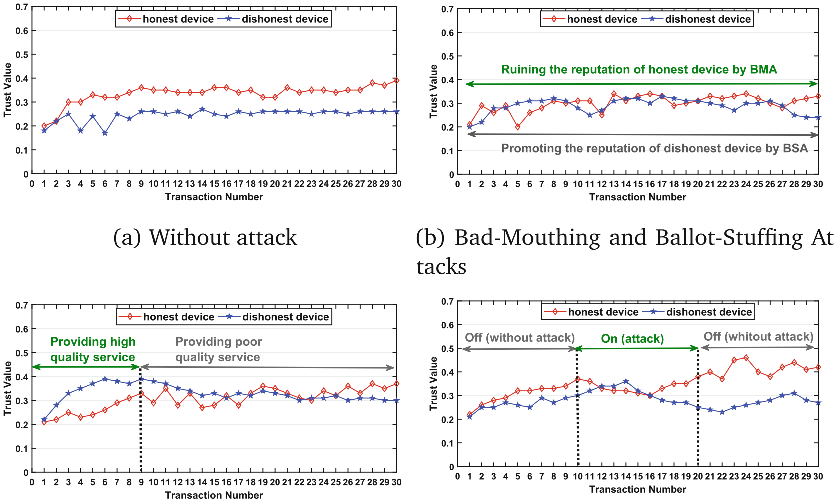


Fig. 4. Comparison of the success rate of an honest device (iterations = 20) by increasing the percentage of dishonest devices from 0% to 50%, which are also categorized into the cases of "without attack" and "with different types of attacks"

The experimental results illustrate that the MCTSE model can select the most trustworthy devices with the best quality service when compared with the other three baseline models. This is because the MCTSE considers multiple contexts of trust and thus is able to distinguish dishonest devices more accurately.

5.3 Experiment 2: Effectiveness in Resiliency Against Attacks

Results & Analysis: Figure 5a to d depict the trust results of a service-consuming device toward the honest and the dishonest devices, who provide or consume services without attacks, and with attacks including BMA-MSA, SPA, and OOA. From Fig. 5b, 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. From Fig. 5c, we can see that the dishonest device boosts its importance when the transaction number changes from 1 to 9, to be selected as a service provider, but then from transaction 10 onwards it starts to provide poor-quality services. Our model decreases the trust value of the dishonest device when it starts to provide poor-quality services by applying the variance of feedback. From Fig. 5d, we can see that when dishonest devices perform OOA, they behave alternatively well and badly. The MCTSE model with the consideration of the contextual feedback of trust and its variance can detect this attack. The experimental results illustrate that: (1) when an honest device provides high-quality services and acts cooperatively, MCTSE increases its trust value; and (2) when a dishonest device provides poor-quality services and acts maliciously, performing different types of attack, MCTSE decreases the trust value of the dishonest device.



(a) Without attack

(b) Bad-Mouthing and Ballot-Stuffing Attacks

(c) Self-Promoting Attack

(d) On-Off Attack

Fig. 5. The effect of feedback and context on the trust value of a dishonest device and an honest device

6 Conclusion

In SIoT environments, trust evaluation has been taken as an important task [3–5,7,14,15,17,23]. In this paper, we have proposed three contexts of trust, including the status, the environment (time and location) of devices and the task type. Then, we have proposed a Mutual Context-aware Trustworthy Service Evaluation (MCTSE) model. The experimental results on a synthetic dataset have demonstrated that the MCTE model can effectively identify honest and dishonest devices. In our future work, we plan to propose a Mutual Context-aware Trustworthy Service Recommendation model (MCTSR) and validate our model on larger datasets.

References

1. Atzori, L., Iera, A., Morabito, G., Nitti, M.: The Social Internet of Things (SIoT)-when social networks meet the internet of things: concept, architecture and network characterization. Comput. Netw. **56**(16), 3594–3608 (2012)
2. Atzori, L., Iera, A., Morabito, G.: SIoT: giving a social structure to the internet of things. IEEE Commun. Lett. **15**(11), 1193–1195 (2011)
3. Saied, Y.B., Olivereau, A., Zeghlache, D., Laurent, M.: Trust management system design for the internet of things: a context-aware and multi-service approach. Comput. Secur. **39**, 351–365 (2013)
4. Chen, I.R., Bao, F., Guo, J.: Trust-based service management for social internet of things systems, **13**(6), 684–696 (2016)

5. Chen, I.R., Guo, J., Bao, F.: Trust management for SOA-Based IoT and its application to service composition, **9**(3), 482–495 (2016)
6. Bao, F., Chen, R.: Trust management for the internet of things and its application to service composition, Mobile and Multimedia Networks (WoWMoM). In: IEEE International Symposium on a World of Wireless, pp. 1–6 (2012)
7. Chen, Z., Ling, R., Huang, C.M., Zhu, X.: A scheme of access service recommendation for the social internet of things. Int. J. Commun. Syst. **29**(4), 694–706 (2015)
8. Liu, G.: Trust Management in Online Social Networks. PhD thesis, Macquarie University (2013)
9. Guo, J., Chen, I.R.: A classification of trust computation models for service-oriented internet of things systems. In: IEEE International Conference on Services Computing, pp. 324–331 (2015)
10. Zhang, H: Context-Aware Transaction Trust Computation in E-Commerce Environments. PhD thesis, Macquarie University (2014)
11. Lei Li: Trust Evaluation in Service-Oriented Environments. PhD thesis, Macquarie University (2011)
12. Kuter, U., Golbeck, J.: Using probabilistic confidence models for trust inference in web-based social networks. ACM Trans. Internet Technol. **10**(2), 1–23 (2010)
13. Leskovec, J.: Stanford Large Network Dataset Collection. http://snap.stanford.edu/data/
14. Lin, Z., Dong, L.: Clarifying trust in social internet of things. IEEE Trans. Knowl. Data Eng. **30**(2), 234–248 (2018)
15. Nitti, M., Girau, R., Atzori, L.: Trustworthiness management in the social internet of things. IEEE Trans. Knowl. Data Eng. **26**(5), 1253–1266 (2014)
16. Sfar, A.R., Natalizio, E., Challal, Y., Chtourou, Z.: A roadmap for security challenges in the internet of things. Digit. Commun. Netw. **4**, 118–137 (2017)
17. Yan, Zheng, Zhang, Peng, Vasilakos, Athanasios V.: A survey on trust management for internet of things. J. Netw. Comput. Appl. **42**, 120–134 (2014)
18. Yang, G.: A health-IOT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. IEEE Trans. Industr. Inf. **10**(4), 2180–2191 (2014)
19. Zheng, Z., Zhang, Y., Lyu, M.R.: Investigating QoS of real-world web services. IEEE Trans. Serv. Comput. **7**(1), 32–39 (2014)
20. Zou, J., Wang, Y., Orgun, M.A.: A dispute arbitration protocol based on a peer-to-peer service contract management scheme. In: 2016 IEEE International Conference on Web Services (ICWS) (2016)
21. Zheng, Y., Mobasher, B., Burke, R.: Deviation-based contextual SLIM recommenders. In: Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management, pp. 271-280 (2014)
22. Zhang, Z., Wang, K: A trust model for multimedia social networks. Soc. Netw. Anal. Min. **3**(4), 969–979 (2013)
23. Truong, N.B., Lee, H., Askwith, B., Lee, G.M.: Toward a trust evaluation mechanism in the social internet of thing. Sensors **17**(6), 1346 (2017)
24. Razzaque, M.A., Milojevic-Jevric, M., Palade, A., Clarke, S.: Middleware for internet of things: a survey. IEEE Internet Things J. (2016)
25. Kim, J.E., Fan, X., Mosse, D.: Empowering end users for social internet of things. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, pp. 71-82 (2017)
26. Hussein, D., Han, S.N., Lee, G.M., Crespi, N., Bertin, E.: Towards a dynamic discovery of smart services in the social internet of things. Comput. Electr. Eng. **58**, 429–443 (2017)

27. Nitti, M., Girau, R., Atzori, L., Iera, A., Morabito, G.: A subjective model for trustworthiness evaluation in the social Internet of Things. In: IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC), pp. 18–23 (2012)
28. Chen, D., Chang, G., Sun, D., Li, J., Jia, J., Wang, X.: TRM-IoT: a trust management model based on fuzzy reputation for internet of things. ComSIS **8**(4), 1207–1228 (2011)