symmetry

MDPI

Article

Conceptualizing Distrust Model with Balance Theory and Multi-Faceted Model for Mitigating False Reviews in Location-Based Services (LBS)

Manmeet Mahinderjit Singh [1,*], Lee Wern Shen [1] and Mohammed Anbar [2]

[1] School of Computer Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia
[2] National Advanced IPv6 Centre, Universiti Sains Malaysia, 11800 Penang, Malaysia
* Correspondence: manmeet@usm.my; Tel.: +604-6535346

Received: 15 July 2019; Accepted: 21 August 2019; Published: 4 September 2019

Abstract: Location-based services (LBS) use real-time geo-data from a smartphone to provide information, entertainment or surveillance information. However, the reputations of LBS application have raised some privacy and security issues such as location tracked by third parties and creation of fake reviews and events through Sybil attack. Fake events on LBS such as congestion, accidents or police activity affect routes users and fake reviews caused nuisances and decreases trust towards this technology. The current trust model in LBS is single faceted and not personalized. The concept of both trust and distrust are essential criteria of any trust management model to measure the reliability of LBS applications. This paper explores the relationship between trust models and the distrust concept in LBS. By deriving a representation of the multi-faceted model and balance theory conceptualized in a MiniLBS prototype, trust in this technology is quantified. By adopting matrix factorization and probability algorithms on the survey results, the relationship between distrust and trust is further examined and tested. The result obtained from the experiment was nearly zero, the smallest one was 3.0253×10^{-95}, and the largest value was only 4.967×10^{-43}. The results show that distrust is not a negation of trust. Another crucial finding suggests that balance theory within distrust in the LBS trust model can enhance the trust management model in LBS and indirectly cater issues rise from fake event problem.

Keywords: Internet of Things (IoT); trust; security; multi-faceted model; social network service (SNS)

1. Introduction

Location-based services (LBS) is an application that uses network-based services that integrate a mobile device's location or position with other information, to provide added value to the user [1]. LBS use real-time geo-data from a mobile device or smartphone to provide information, entertainment or security [2]. According to a recent report by Berg Insight at the end of 2013, about 40 percent of mobile subscribers in Europe were frequent users of at least one location-based service [3]. LBS applications such as Google Maps, Foursquare, Instagram, Facebook and Waze function perfectly on mobile devices via a mobile network [4]. LBS such as Waze provides turn-by-turn and best routes navigation; provide information to users on real-time incidents and allow simple social interactions between users [5].

Nonetheless, despite the benefits that LBS have provided, LBS applications such as mobile devices can collect the locations and identities of users and understand the usage patterns of a user [2] without any knowledge of a user. For example, recently Apple was alleged to regularly record the locations of iPhone and iPad users in a hidden file within their devices raising very serious security and privacy concerns [1]. In fact, location information can be useful for marketing and promotional purposes such as for location-based advertising [2]. Sybil attacks on LBS applications in which a multiple fake devices node in an interconnected network could impersonate a genuine device and trick users into sharing their personal details is another concern. Lately, Sybil attacks have been used by some organizations in reputable systems such as eBay, Google Page Rank and LBS, such as Waze, to obtain fake opinions [6]. The creation of fake events such as forging congestion to force automatic rerouting of trips is possible due to non-reliable authentication mechanism in place [7] for users reporting on any real-time updates on incidents. The spread of disinformation phenomena, intending to influence users' opinions or decisions, is an act aimed at deception [8]; fake reviews generated via technical-based attacks such as Sybil or non-technical act of malicious users adding fake event has become a non-trivial issue. Because the correlation between security and privacy threats with trust is interchangeable, high trustworthiness towards any technology simply means that users are comfortable in accepting the trade-off between the impacts of security and convenience that they will face while adopting a technology. Thus, in this research the domain of trust will be further elevated to provide a mitigation solution to mitigate the fake reviews/events problem in Internet of Things (IoT) applications such as LBS.

Trust management plays an important role in reliable data fusion and mining, qualified services with context-awareness, and enhanced user privacy and information security [9]. Trust management helps people to gain confidence while adopting LBS. What remains unknown is how the impacts of trust will affect a user's perceptions of trustworthiness. Trust involves people's interactions. For example, users in e-commerce are likely to gather information from their trusted user to make decisions. Trust is uncountable, dynamic, propagative, non-transitive, compostable, asymmetric and event-sensitive [10]. In theory, trust refers to the willingness of a party to engage in risk-taking and to reduce doubts about the lowest level [11]. Distrust plays a crucial role in understanding trust. Transitive, asymmetric, dynamic and subjective are examples of the properties of distrust [12]. Some studies [12,13] have found that distrust is a negation of trust and can help in improving trust management. Balance theory and status theory can help in incorporating distrust to improve trust [12,14].

The motivation for this research was to explore the trustworthiness concept needed for an LBS application to enhance user acceptance of the technology. The current management model is single faceted and not personalized [14]. Single facet trust is not suitable for an IoT application, which is distributed by nature. Thus, a multi-faceted trust management model [11,15] is worth being explored to tackle the IoT trustworthiness issue. Social theory adopted by [12] has investigated whether distrust has added value for trust and, thus, increases trust performance. In social theory, two mains theories in the study of trust are balance theory and status theory. In the research of distrust, the balance theory has been tested in checking the nature of its applicability, user acceptability towards this theory and how this theory can be used in current IoT applications. By adopting the matrix factorization technique, the theory is further tested. This paper acknowledges the integration of multi-facet trust and balance trust for IoT applications. Specifically, this paper makes the following contributions:

1.1. Integration of Multi-Facet Trust and Balance Theory in IoT

Most current IoT applications (e.g., social media, LBS) adopt single facet trust, and, with the current demand in securing IoT applications, the need to enhance the current trust model with a multi-faceted model is a must. Based on [12] findings on the weightage of trust attributes in an Online Social Network (OSN), a similar weightage can be adopted for an IoT application. The concept of balance theory has been adopted widely in distributed computing environments such as OSN. The adoption of this theory in the domain of sensor-enabled applications has not been tested and proved. This current work applies multi-facet adoption into the existing balance theory concept to enhance the trustworthiness of an IoT application such as LBS. In addition, due to failures in terms of lack of authentications in current LBS applications between users and the service providers, challenges have increased, such as fake reviews. In this work; by scoring trust values and adopting balance theory, a new approach in reducing fake reviews among users will be proposed.

1.2. Testing the Relationship Between Trust and Distrust for IoT Application

Low trust is equivalent to high distrust and vice versa [13], and it has a negative impact on a human relationship. However, because trust and distrust can co-exist, distrust can be incorporated in trust to improve the trust model [14]. Tang, Hu and Liu (2014) [12] proved that distrust is not the negation of trust for the domain of the social network, but has a positive impact in enhancing the trustworthiness of social media. In this research, the relationship between trust and distrust in IoT applications will be tested. The outline of the paper is organized as follows: Section 2 is the literature review of existing LBS applications and trust models. Section 3 is the detailed design of the proof of concept application, MiniLBS. Section 4 includes the evaluation and discussion of MiniLBS. Finally, the conclusion and the future work of the current study will be presented.

2. Literature Review

The literature review is divided into several sections including one on Location-Based Services (LBS) and a review of existing LBS applications. After that, trust and distrust, social theory as well as trust management model, will be studied.

2.1. Location-Based Services

Location-based Services (LBS) have grown rapidly on the market since the invention of the smartphone. There were about 150 million users in the United States who adopted an LBS application in 2014 [16]. According to Statista (2015) [16], this number will increase continuously every year, reaching about 242 million users in 2018. LBS, as network-based services, integrate a mobile device's location or position with other information, to provide added value to a user [1]. Some people may doubt how useful location-based services are. Location-aware services collects and analyzed user experience data via opinion and feedback through the usage of geo positioning technologies. Real-Time Locating Systems (RTLS) are widely used to track the location of people or objects within a specific area [17]. Examples of LBS applications are Google Maps, Waze and Foursquare. LBS applications can navigate routes and keep users connected with their friends and family.

However, several risks and issues need to be tackled while using location-based services. Although an LBS can be highly beneficial, it can also harm a user's privacy. Several common challenges must be addressed with respect to LBS such as the abuse of LBS, spam and hidden security threats. For instance, the location information might be shared with various third parties for understanding user usage patterns without the knowledge of the user [2]. As users do not know who these third parties are or why they need the location data, users are unable to identify whether they are disclosing their data to trustworthy parties who can provide the level of security protection these users require [18]. In addition, location data can also be sold to others for marketing and advertising. LBS can track a person's physical location through their mobile devices and send the information to various sources such as restaurants and other businesses.

Five popular applications are studied in the recommendation of X.800 [19]. Among the five applications, Waze is the navigation application with the most users worldwide. Yelp, Burpple, and Foursquare are applications to discover places to go to. Find My Friends is an iOS application that allows us to know the location of friends and family. Yelp has the longest history of these applications as it was founded 11 years ago. Most of the information in LBS services has value, especially with respect to sensitive information such as bank accounts and mobile numbers. Therefore, LBS applications should protect user information from being stolen by others. Among the five applications, Burpple has the worst setting in terms of security, because the location a user wishes to travel to is publicly known. In a reputation system or any LBS applications, users' reviews involving feedback or opinions on the usage of the application matters in ensuring the quality and increasing any business profit. However, lately the phenomena of spreading false reviews on reputations system or even LBS applications has increased dramatically. False reviews or opinions are grouped as disinformation [20] which aims to influence future decisions and to deceive users [8]. The motive behind this kind of deception [21,22] could be simply for fun: to compromise availability of services or to increase profit on less quality products and services by adding fake positive reviews.

In the case of LBS, fake reviews generated via technical-based attacks such as Sybil or non-technical acts of malicious users adding fake events has become a non-trivial issue. A Sybil attack is an attack in which many pseudonymous identities are created to gain influence. In IoT applications such as LBS, a Sybil attack is executed via devices that appear as 'virtual mobile devices'. Three main attacks caused by Sybil devices are (i) creation of fake events such as congestion and accidents; (ii) ghost riders in which multiple Sybil devices launch attack using a single emulator and (iii) to track individual movement by launching the ghost riders' devices [5]. The risk or damage caused by the Sybil devices on reputation services is compromising the availability of services and decreasing trust towards the technology. As possible defenses, [23] argued that number/Ip verification or location authentication with cellular towers have their downsides. Similarly, the lack of authentication between users and apps providers leads to making the tackling of the malicious act of adding false reviews [7] a challenge.

Overall, the relationship between system security and trustworthiness can be represented through the relative equation of how well a user fares using any system and their feelings of confidence towards that system. In addition, since the degree of trust is correlated directly to the sense of feeling safe in adopting a system, the need to ensure LBS reviews are genuine can also be enforced through the domain of trust. By tapping on the trust model which involve in authenticating and evaluating user trust related attributed; the degree of trusting one's review will increase as well. Hence, the need to understand trust theories and models is essential in this research.

2.2. Trust and Distrust Perspectives

Trust is also defined as an individual's confidence in another person's intentions and motives, and the sincerity of that person's word [24]. Trust is a complex subject relating to belief in the honesty, truthfulness, competence, and reliability of a trusted person or service [9]. In defining trust in computer science, trust is normally specified in terms of a relationship between a trustor (user) and a target entity known as the trustee (system) [10,25]. If a user feels safe and secure with respect to an application that user subsequently trusts that application when using it. For example, trust is based on feedback from past interactions for users of eBay and Amazon [10].

Compared with trust, a lack of research exists on distrust. Nonetheless, studying distrust is vital for understanding trust. Both trust and distrust help a decision-maker reduce uncertainty in decision-making. A lack of trust causes difficulties for people in decision-making. According to [24], distrust can be defined as confidence about a relationship partner's undesirable behavior, stemming from the knowledge of the individual's capabilities and intentions. Distrust theories have stated that low trust is equivalent to high distrust. Likewise, low distrust is equivalent to high trust [12]. Scholars understand distrust to be the expectation that others will not act in someone's best interests, even engaging in potentially injurious behavior and producing the expectation that capable and responsible behavior from specific individuals will not be forthcoming [25]. Some studies [13,25,26] have found that distrust is the negation or the opposite of trust.

However, [27] opined that distrust as merely a negation of trust does not make understanding the concept easier. Negation of trust can occur in several ways. For example, these may include a lack of expectation, an expectation of harmful behavior or the lack of expectation of harmful behavior (two negations in one sentence): each statement defining something very different [27]. The lack of expectation is categorized as ignorance instead of distrust. Low trust is equivalent to high distrust and vice versa [13]. Distrust has a bad reputation and has a negative impact on a human relationship. Trust and distrust are two separate concepts and can co-exist [25]. [12] believe that distrust can be incorporated in trust to improve the trust model. The characteristics of trust and distrust are shown in Table 1 below:

Table 1. The properties of trust and distrust.

Property	Trust	Distrust
Transitive	Trust is transitive, for example, if A trusts B and B trusts C. Tang and Liu (2014) [14] are of the opinion that A has high possibilities that he/she may trust C [12]. Some studies also say that trust is not transferred [10,11,14,28].	Distrust is not transitive. For example, if A distrusts B and B distrusts C, then A may find that he/she may trust C. It can be explained by the balance theory as 'the enemy of your enemy is your friend' [12].
Asymmetric	Trust is not identical. For example, A trusts B fully 100%. However, this does not imply that B will trust A completely. However, when both parties are trustworthy, they will converge in high mutual trust. [10,11,14,28].	Distrust is even more non-identical. For example, if A has a prejudice against B, then B will be forced to penalize back, and this will cause low mutual trust [10,12].
Dynamic	Trust degree can increase or decrease with different experiences and will decay with the passage of time [10,28].	The same goes for distrust.
Subjective	Trust degree is different towards different individuals. If A and B try a new restaurant and give different comments about the food, but C trusts A more, so C will think that A's review is useful [10].	The same goes for distrust.

2.3. Social Theory of Trust

The two fundamental theories of balance theory and status theory are often used in representing the social networks. The social psychologist Heider [29] formulated balance theory, which fundamentally revolves around how people tend to maintain consistency in patterns of their liking and disliking of each another and of impersonal objects. Balance theory focus on two types of triads: balanced triads and unbalanced triads (see Figures 1 and 2). These triads are formed by two types of relations, unit relation, and sentiment relation. The unit relationship is the relationship between two or three individuals while the sentiment relationship refers to social objects such as trust [30].

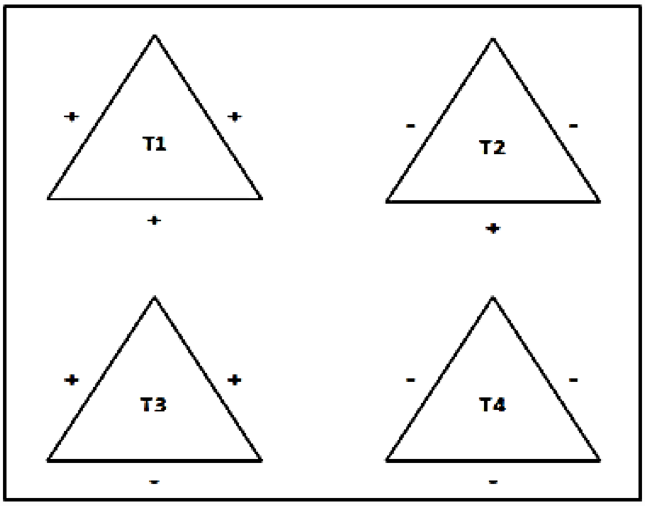

Figure 1. Theory Triads.

For the sentiment relationship, positive is trust or like and negative is distrust or dislike. In a triangular relationship, there are four possible sign combinations as shown in Figure 1: T1 (+,+,+), T2 (−,−,+), T3 (+,+,−) and T4 (−,−,−). A balance state is achieved when you like a person that you are associated with (positive relation) or dislike a person that you are not associated with (negative relation). An imbalance state exists when you dislike a person that you are associated with or like a person that you are not associated with. In the possible sign combinations, only T1 and T2 achieve a balanced state [30]. It seems clear that if user A trusts user B, and user B trusts user C, then user A will have a positive view of C based on this knowledge ('the friend of my friend is my friend'). However, such transitivity might not hold with respect to distrust [12,31]. Guha et al. [31] believe that distrust is not propagated like trust. If user A distrusts user B, who distrusts user C, then perhaps user A is expressing the view that user B's entire value is so misaligned with user A's value that anyone user B distrusts is more likely to be trusted by user A ('the enemy of your enemy is your friend').

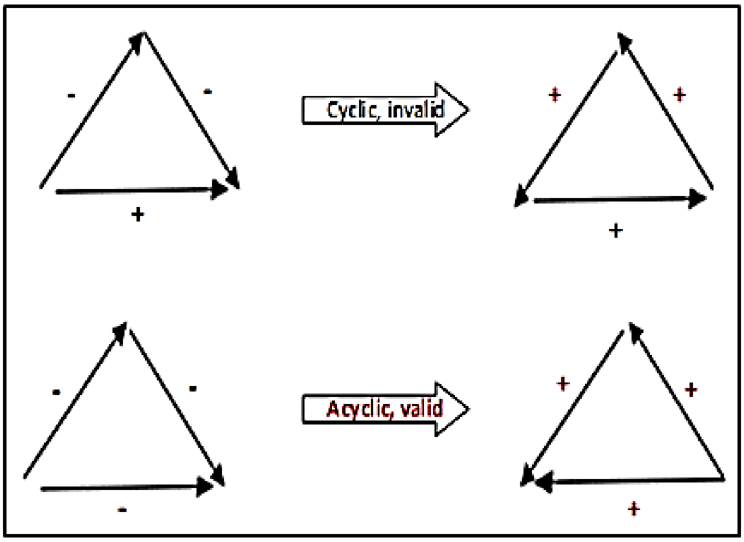

Figure 2. Cyclic and Acyclic Triads.

Status theory is also a popular theory from social psychology; it was implicit in the work of [31] and later developed further by [32,33]. Status is a theory of signed link formation based on the implicit ordering of the nodes. In this theory, a positive link from A to B indicates that A thinks that B has higher status than A. Similarly, a negative link from A to B means that A thinks that B has a lower status than A. For a particular triad, status theory suggests that if each negative relation is taken, its direction reversed and its sign flipped to positive, then the resulting triangle (with all positive edge signs) should be acyclic (non-cycle) [12]. As shown in Figure 2, the acyclic cycle generated from the condition is a valid status theory triad. The computational trust model proposed by [26] integrates three aspects of trust including basic trust, situational trust, and general trust. Basic trust is known as disposition trust, which is calculated from all the experiences accumulated by an individual. General trust is trust of another individual. Situation trust indicates the amount of trust that individual has in another taking into account a specific situation. The Marsh trust model is a computational model that focuses on trust dynamics. The trust values are calculated by using a formula or equation. These trust values are used to help individuals to identify whether another individual is trustable.

Tang and Liu (2014) [14] found that current Online Social Networks (OSN) are single faceted and not personalized and that the trust level cannot be calculated. They adopted the idea of a multi-faceted trust model from [34], in which a user-centric model in OSN is proposed. The relationship between individuals is multi-faceted [11,14]. Sometimes, people might want to disclose their information to a close friend but not to everyone else. Chieng et al. (2015) [35] and Liu (2014) [15] developed MiniOSN with trust rating features that include eight trust traits, which are: competency, confidence, credibility, reliability, reputation, faith, honesty and belief. The user can rate the trust attributes from 1 to 10. The greater the trust attribute value is, the greater the trustworthiness would be.

Tang, Hu, and Liu (2014) [12] and Tang and Liu (2014) [14] previously worked on finding the relationship between trust and distrust by applying two computational models. There are two tasks. The first task is to predict distrust from only trust to answer the question of 'is distrust the negation of trust?' whereas the second task is to predict trust with distrust for measuring the value of distrust. The prediction of distrust can be suggested for pairs of users with low trust scores in the same trust network. For trust prediction in task 2, both [12,14] found that trust and distrust metrics may be used in a model by extending negative values to the trust model to incorporate distrust into trust management. He further introduces balance theory and status theory to understand trust and distrust. The inspiration for developing this line of theory comes from [31] work in observing the Epinions. Epinions is a website at which people can review products, and web-of-trust is used to rate user trustworthiness based on their feedback consistency. Reference [31] adopted status theory in their study of the Epinions website, and their findings show that in Epinions, a signed link from A to B can have more than one interpretation. A positive link from A can mean either 'B is my friend' or 'I think B has a higher status than I do'. A negative link represents an enemy with lower status. For a triad, status theory suggests that if we take each negative relationship and reverse its direction, and flip its sign to positive, then the resulting triangle with all positive edge signs should be acyclic.

Based on further observations of previous studies and arguments from previous researchers, both distrust and trust have a positive impact when integrated with a trust management model. Our previous research work has explored the concept of a multi-faceted context within the greater content of media comprising a distributed manner network spread through a social media platform. Thus, this current study extends our research with respect to the adoption of a multi-facet model in an IoT application. So far, no previous study has examined the adoption of balance theory within the IoT Technology and location-based services (LBS). This has motivated the current study. Thus, the first hypothesis is:

Hypothesis 1 (H1): *The balance theory within distrust in trust can enhance the trust management model in location-based services (LBS).*

Because previous studies by [12,14,31] demonstrated a clear relationship between distrust and trust in an interconnected and distributed network such as social media, its essential to quantify the relationship in a location-based services application, which can be represented as centralized. Most of the LBS services adopt a centralized server in compiling final retrievable geo-data information before feeding a user query.

This stands as a catalyst to explore the second hypothesis, which is:

Hypothesis 2 (H2): *Distrust is the negation of trust in location-based services.*

By employing the balance theory and multi-faceted model, a need to exists to test H1 and to confirm whether H2 holds. Next, the research methodology of our work will be presented.

3. Research Methodology

The research methodology is divided into five phases. In phase 1, the problems existing in the current LBSs such as privacy and security challenges, and incomplete trust management in LBS are examined. After that, the related works regarding the Internet of Things, location-based services and its privacy and security concerns as well as existing trust management technique will be identified. A literature review is important before implementing the proof of concepts application because this review can help us to discover potential problems inherent in a holistic solution. After studying the related works in current location-based service security and privacy issues, case studies on current LBS applications that are available in application stores will be carried out. The privacy setting on each of the applications will be discussed as well.

In phase 2, a prototype of an LBS application was created to accomplish the second research objective. The prototype is used to study the relationship of trust and distrust by implementing balance theory and a multi-faceted model. Different scenarios of how balance theory can be proven must be conducted. The multi-faceted model is implemented in the prototype by the rate that each user identified with the eight trust attributes of belief, faith, honesty, competency, confidence, creditability, reliability, and reputation. The balance theory is calculated by randomly selecting the comments of two users. A user can select whether he/she trusts a comment or not, and the balance theory result will be calculated and use in analyzing the data. To prove the concept of prototype, a survey will be used in phase 3. It is very crucial to know the acceptance of users of the selected trust models. This study used interviews with a small group of users to test the proof of concept for the prototype. The step is necessary because balance theory is related to an undirected signed triad relationship. A prototype was designed by grouping users into groups of three to test the proof of concept prototype and balance theory. The results related to the hypothesis are collected at this stage.

In phase 4, results collected from all the questionnaire surveys will be evaluated by running an analysis through statistical tools. Proof of concept was examined by considering user feedback and then analyzing the performance and effectiveness of the proposed trust management technique. In this stage, a discussion and then the benchmarking of results will be done in support of Hypothesis 1. To answer Hypothesis 2, a suitable trust prediction algorithm was incorporated. In this case, the assumption was that if distrust is the negation of trust, then low trust can be used to predict distrust. By running the trust predictor algorithm, results can be obtained, and the hypothesis can be explicated.

3.1. Experiment Design for H1

Based on the literature review, along with influences from Tang and Liu (2014) [14] and Heider's (1946) [29] balance theory concept, a prototype was designed. Thus, MiniLBS, a location-based service application with a trust rating feature and the balance theory concept, was implemented. MiniLBS is an Android application that has functionalities of a basic LBS application. This location-based social networking adopts the concept of a social networking site including the interactions of the user.

3.2. Adoption of Multi-Faceted Model

MiniOSN is an online social network web page with a trust rating feature implemented. Both of their ideas were influenced by [34] trust model. In MiniOSN, users can restrict their posts and photos to selected people based on the rating feature. This model can help a user to express his/her subjective views on trust. In MiniLBS, this study slightly modified the ideas. Because MiniLBS is a location-based application, a restriction on posts is unnecessary because the posting is mainly commenting on a route. However, the study did adopt a trust rating feature for friends. Unlike MiniOSN, which needs approval of a friend's request, MiniLBS only needs to follow a friend, like with Instagram. Before following someone successfully, a user needs to evaluate him by rating him based on the eight trust attributes. These eight trust attributes are: belief, confidence, credibility, competency, faith, honesty, reliability and reputation. One objective of this prototype is to determine the possibility of improving the trust model by incorporating distrust in trust. Therefore, by knowing the trust value of a friend, their relationship to each other can be predicted by the trust level itself. The higher the trust value, the higher the trust level. MiniLBS provides a function that allows a user to add friends by following them. The definitions of the eight trust attributes are shown in Table 2.

The rating for OSN friends will be calculated based on the eight trust attributes and recorded in a web-based application. Three level of friendship are categorized according to the trust rating. Table 3 below illustrates the concept of how the value of the range of trust determines the trust level of a friend.

As the value of the trust is indicated from 1 to 10, a borderline of 7.5 was chosen to classify 'best friend'; an 'average friendship' will fall between 0 and 7.5, and a stranger will not be rated. For example, if Z is the account owner, Z will evaluate friends by adding them, Z adds a friend, namely Y. If the rating is higher than 7.5, the name of Y will change to green. This is because, in MiniLBS, a user can comment on the route. Therefore, the name can classify the relationship of the account owner and friends among the list of users that commented on the route. The trust score is calculated by using the Algorithm 1.

Table 2. The list of trust attributes.

Trust Attribute	Meaning
Belief	One's attitude towards the likelihood or truth of a person not immediately susceptible to rigorous proof. An acceptance that a statement is true or that something exists.
Confidence	State of one being certain that a chosen course of action is the best or most effective. Sure of oneself; having no uncertainty about one's own abilities, correctness, successfulness, etc.; self-confident; bold.
Credibility	The quality of being trusted and believed in.
Competency	One has the ability to do what another person needs to have done. The ability to do something successfully or efficiently.
Faith	The belief that is not based on proof. Applicable for a person or thing.
Honesty	Tells the truth and fulfils any promise made.
Reliability	The ability to be relied on or depended on, as for accuracy, honesty, or achievement.
Reputation	The ability to be relied on or depend on, as for accuracy, honesty, or achievement. A favorable and publicly recognized name or standing for merit, achievement, reliability, etc.

Table 3. Rating value and its color respectively.

Types of Friendship	Rating	Color
Best Friend	$7.5 \leq x \leq 10.0$	Green
Average Friend	$0 \leq x < 7.5$	Blue
Stranger	No rating	Black

Note: Where x = trust value.

Algorithm 1: Calculate Trust Score
(Reputation, Confidence, Belief, Faith, Honesty, Credibility, Competency, Reliability)

Input: reputation *(Vrep)*, confidence *(Vcon)*, belief *(Vbel)*, faith *(Vfai)*, honesty *(Vhon)*, credibility *(Vcre)*, competency *(Vcom)*, reliability *(Vrel)*

Output: Best Friend or Average Friend

```
Erat = $\frac{\mathrm{Vrep+Vcon+Vbel+Vfai+Vhon+Vcre+Vcom+Vrel}}{8.0}$
If Erat $\geq 7.5$
Return Best Friend
Else Erat
Return Average Friend
```

3.3. *Adoption of Balance Theory*

Balance theory is adopted in MiniLBS. Balance theory explains that attitudes towards persons or objects can influence each other. Heider's idea [29] was that we want to maintain psychological stability, and we form relationships that balance our trust and distrust. He developed the P-O-X triangle to examine relationships among three parties. In MiniLBS, the design of triangle P-O-X is a user or route comment as shown in Figure 3. For example, when a user logs in to MiniLBS, he or she will be denoted as P, which is the account owner in MiniLBS. O and X are the users from MiniLBS. Their relationships with P can be either best friend, average friend or stranger to each other. While the relationship between O and X depends on the type of route's comment. The type of the route comment can be positive, neutral or negative. In this research, it is assumed that only positive and negative comments are taken into consideration.

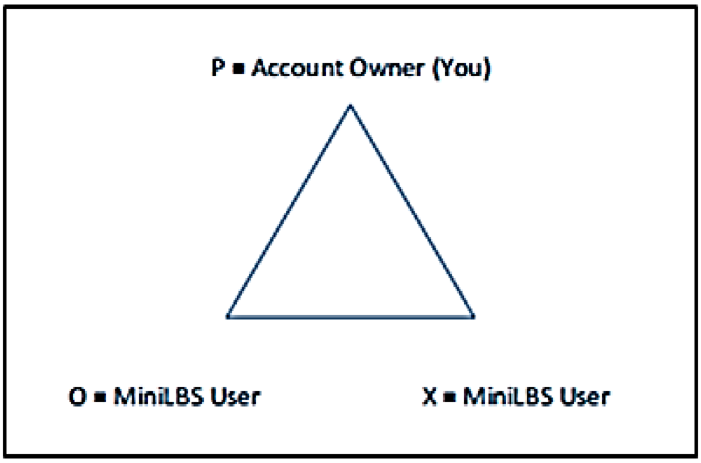

Figure 3. illustrated in MiniLBS.

The Algorithm 2 below illustrates how balance theory functions on MiniLBS. There are two main functions in this algorithm: the first one is to calculate the balance theory between user and commenter. The second function is to obtain the user-commenter relationship by computing the trust value from eight trust traits.

Algorithm 2: Calculate Balance Theory Action in MiniLBS
(User Id, Comment Id1, First Action, Comment Id2, Second Action)

```
Input: userId, commentId1, firstAction, commentId2, secondAction
Output: Balance Theory between three users (userId, user of comment 1 and comment 2)
Retrieve comment information from database where id = commentId1
Calculate Commenter Relationship for comment 1

Retrieve comment information from database where id = commentId2
Calculate Commenter Relationship for comment 2
If firstAction == 'Like'
    User agree comment 1. (+)
Else
    User disagree comment 1. (−)
If secondAction == 'Like'
    User agree comment 2. (+)
Else
    User disagree comment 2. (−)

Save the relationship of the user with commenter 1 and commenter 2 and the action (like or dislike) of the user to comment 1 and 2 information as a Balance Theory Group.
If user like either one of comment 1 or comment 2 and dislike another comment
    Return Negative (−)
Else If user like both comment
    Return Positive (+)
Else If user dislike both comments
    Return Positive (+)
```

3.4. MiniLBS Application Usability Tasks

MiniLBS is an application that incorporates the multi-faceted model and the balance theory concept. In this section, the survey findings, as well as the survey discussions, are presented. Several steps are needed for participants to evaluate the prototype, MiniLBS. These are to:

Understand the LBS and eight trust attributes;
Register an account in minilabs;
Select three friends and rate them (multi-faceted model);
Calculate a trust score and classify friends;
Comment on one of the routes;
Run balance theory and calculate the result; and
Complete the user acceptance survey.

MiniLBS is designed to provide a function for offering geo-location services. It is capable of providing the route to a selected location by employing the GPS sensors. For experimental purposes, the selected location was simulated. Once the location is chosen, two environments are simulated: (1) a clear route (no traffic or other disturbance) and (2) a busy route (traffic or with some construction). The steps of using MiniLBS are the following:

The user will register an account and log in. After that, the user will select three friends to evaluate by giving out a trust score based on eight trust attributes. The rating scale for each trust attribute ranges from 1–10. The lowest is 1, and highest is 10. The system will calculate the trust score by adding the trust score for each attribute and dividing it by 8. A friend will be classified. A trust score more than 7.5 is a best friend with high trust, while less than 7.5 is a normal friend.

The user is required to select a route for each normal and disturbance condition. There are three routes provided. Because the collection of comments the balance theory concept is necessary, the user, therefore, needs to comment on the selected route based on the impression of the route.

After that, the user needs to run the balance theory. Two random comments from other users will be selected. The user will add either trust or distrust to the comment. The balance theory result will be calculated. Lastly, the participants are required to complete a user acceptance survey.

The period for conducting in the study was a two-month span lasting from June to August 2017. During these two months, 71 participants were invited to take part in the prototype evaluation. The participants comprised users both with and without IT backgrounds. Of the 71 participants, the ages of 60 participants ranged from 20 to 25 and the ages of 11 participants ranged from 25 to 30. Two types of routes were present in MiniLBS, smooth and disturbance, a participant needed to make a selection from both types of conditions. The distance and time taken to reach a destination were different in these routes. Table 4 below shows the selection of each route for both of the two different conditions.

Table 4. Selection of route.

Route	Smooth	Disturbance
Route 1	35	22
Route 2	22	41
Route 3	14	8

The triads generated and users are selected randomly. The trial experiments are done three times and the average result is taken in account. The selection of the route depended on the distance under normal conditions; 35 users selected route 1 as it was the shortest path to reach a selected location X. Only 14 users selected route 3 because it took a longer time and had a longer distance to reach the destination. For the disturbance's route, route 1 had route construction, route 2 was normal route, while an accident was happening in route 3. As expected, route 2 was the most selected route. The route selection reflected the behavior of a user in response to changes if something was happening. Thus, he/she would try to avoid a route if the route was in trouble. Among the 71 users, 142 balance theory triads were formed in total for both the normal and disturbance condition on the routes. These included 71 triads from the normal route and another 71 triads from the disturbance route.

Table 5 shows that after three trials, an average of 105 of the users or 74% of the users achieved a balance state in the balance theory while the rest did not. One hypothesis tested whether the balance theory could be used in LBS, and, from the results obtained, the nature of the users showed that the balance theory was supported in LBS applications. Of 105 or 74% of the valid balance triads, 63 formed a positive triad, which means the balance state had three positives for each of the edges. Only 42 of them had a negative triad result, which means the combination of two negative edges and one positive edge to form the triad. The ratio was about 6:4 based on the positive and negative triads. Since the test is done within the setting of blind test; the variance of the ratio was because most comments provided on each route were positive comments. Therefore, the chances of getting two positive comments were higher. When a user trusts the first comment, he/she will tend to trust the second positive comment as well.

Table 5. Average balance theory result.

Type of State	Number of Participants
Balanced State	105
Non-balanced State	37

The balance theory generates the comments randomly by selecting any two comments from different users that commented on the route, and a few possible chances exist for a combination. The first one is that both users are friends of the current user. The second one is that only one of the two users is a friend. The third combination is that both of them are strangers. Each user is required to evaluate three friends during the initial stage of data collection, and the chance of generating a friend's comments are high. They will tend to trust their friend's comments rather than the comments of a stranger. As the number of the participants increases, the chances of generating friend's comment are less due to a huge number of comments.

3.5. Results and Findings in Balance Theory

The balance theory concept applied in MiniLBS focuses on the relationships among observer, person, and object. The relationships among these elements may be either positive or negative. In MiniLBS, the system will generate two random comments after the user has selected the route. The user will need to select whether to either trust or distrust the random comment. After that, the result will be calculated by using the matrix factorization algorithm. Table 6 below shows the summary of the results for balance theory concept.

Table 6. Summary of the results of balance theory.

Question	Yes	No
Agreement on the balance theory statement	51	20
Acceptance on the random comment from stranger	30	28
Acceptance of balance theory concept in LBS	39	17

First, a user was asked about whether they agreed with the ancient proverb of 'my friend of my friend is my friend, the enemy of my enemy is my friend'. Accordingly, 72% of them agreed with this phrase because they thought that two opposing parties should work together against a common enemy. Because the respondents were mostly from the Y Generation, they are affected by drama and movies in their lives; this ancient proverb is widely used in many films. Only 20 of them answered 'No', and this might have been because they thought that it was not applicable to their life.

More than half of the users thought that balance theory concept was suitable for use in LBS applications. One reason was because they had achieved a balance state with other users when trying out the prototype. The experiment set up in the prototype was easy for them to use. Moreover, the adoption of balance theory did not complicate their usage in a LBS application. Only 17 respondents did not agree that balance theory was suitable for use a LBS application, and this was because they could read all the comments on the route together, and it was pointless to select only two comments from among all the comments.

In the adoption of balance theory concept, many people remain positive about the presence of the balance theory concept in LBS applications. Hypothesis one of this research was proven by getting the result of 74% of the balance state triangle. The balance theory concept comprises sentiment relations or unit relations. The balance theory triad is the relationship between you, another person and an object. Therefore, the balance theory is widely used in product placement in televisions shows and consumer-brand relationships. If a person likes a celebrity and a celebrity likes a product, that person will tend to like the product more to achieve psychological balance. However, if a person already dislikes the product being endorsed by the celebrity, he/she may begin disliking the celebrity, again to achieve psychological balance. In fact, in an LBS application, no consumer-brand relationships exist.

Fake reviews or opinions from users using LBS application could be tackled by adopting multi-facet model as well. Due to the fact, most fake reviews occur as a result of no authentication mechanism between device users and the LBS service provider; this new model will force users to not only identify the users using the model but also to evaluate the other users. Evaluation of other connected users within one LBS network will ensure that only trusted opinion are taken into account. With the adoption of balance theory to further support the evaluations made and correctly designing a triad of three users within one's LBS connection; the tasks of classifying trustworthy and non-trustworthy users become much more concrete.

In conclusion, more than half of the participants supported both the multi-faceted model and the balance theory implementation. This demonstrated that the model could be used as a solution to enhance trust of LBS technology and mitigate certain security risk such as fake reviews.

3.6. Experiment Design for H2

Figure 4 represents some steps taken to test and further prove Hypothesis 2. To prove the second hypothesis, a framework was developed by using the result collected from the prototype in Section 5. Another experiment was developed by using trust propagation [31] as discussed in Section 2 earlier. The following sets were used for this experiment.

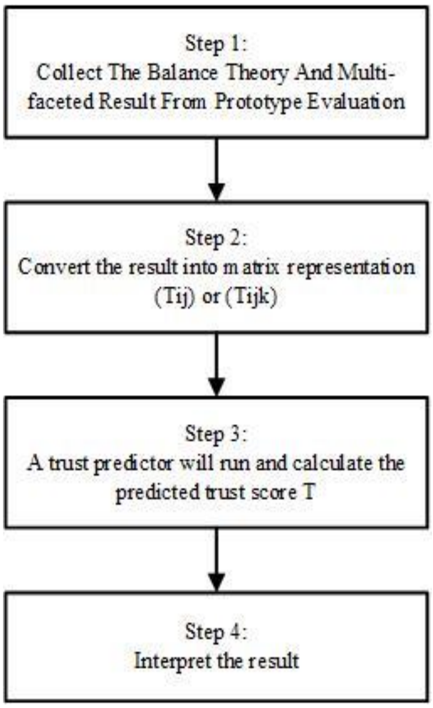
Step 1:
Collect The Balance Theory And Multi-faceted Result From Prototype Evaluation
Step 2:
Convert the result into matrix representation (Tij) or (Tijk)
Step 3:
A trust predictor will run and calculate the predicted trust score T
Step 4:
Interpret the result

Figure 4. Steps in proving H2.

The result has two parts, the balance theory result involving three users and the multi-faceted result between user and user. A 3*3 matrix that represents a triangle of the balance theory will be formed. A 2*2 matrix that indicates the relationship between user and user was also formed. It is a one to one directed relationship because user A trust user B does not mean that user B will trust user A in the same way. However, the value is more precise compared with the balance theory concept. The relationship between stranger and stranger is denoted as 0.5 instead of 0, which indicated low trust. The trust predictor that will be adopted is the trust propagation algorithm [31]. The trust propagation Algorithm 3 as below.

```
Algorithm 3: Trust Propagation Algorithm
Input: Belief Matrix, B
Output: Propagated Trust Matrix, P
1. Define the belief matrix, B
2. Case 1: Trust Only
3. Case 2: One-Step Distrust
4. Case 3: Propagated Distrust
5. Calculate the atomic propagation, C by using B
6. $C = aB + bB^TB + cB^T + dBB^T$
7. Assume Ck be the matrix for trust propagation from user A to user B
8. The final matrix representation, F is calculated.
9. $F = \sum_{k=1}^{k} V^kP^k$
```

After the result from step 3 is obtained, the result will be interpreted by categorizing it as either trust or distrust based on the value.

4. Framework of Trust Propagation Algorithm

In this section, a trust propagation framework [12,31] will be discussed. We define an n x n trust matrix, T and distrust matrix, D. The value of Tij is assumed to lie between 0 and 1. As shown in Table 7, matrix B represent the set of beliefs, Bij might be i trust j (trust alone, T) or a combination of i's trust and distrust of j (T—D).

Table 7. Matrix names used.

Name	Meaning
T	Trust Matrix: Tij is i's trust of j
D	Distrust Matrix: Dij is i;s distrust of j
B	Belief Matrix: B is either T or T—D
C	Combined atomic propagation matrix
P(k)	k-step propagation matrix
F	Final Belief: Fij is i's trust of j

4.1. Atomic Propagation

Atomic Propagation is a basic propagation technique, called 'atoms'. There are four basic atoms, namely, direct propagation, co-citation, transpose trust and trust coupling. The atomic propagation is summarized in Table 8.

For example, if Bij = 1 indicating that i trusts j and Bjk = 1 indicates that j trusts k, the direct propagation in atomic propagation will yield a result of i trusts k (Bik = 1). The matrix B will be used for chaining the four-atomic propagation. Take a note that BT is the transformation of matrix B. The result single combined matrix of all four-atomic propagation is denoted as:

$$C = aB + bB^T B + cB^T + dBB^T$$

The constants, a, b, c, and d are a vector representing weights for combining the four-atomic propagation schemes. These values of the constant will be discussed later.

Table 8. Four basic atomic propagation.

Atomic Propagation	Operator	Description
Direct Propagation	B	If i trusts j, and j trusts k. Direct propagation allows us to infer that i trusts k.
Co-citation	B^TB	i should trust j and k, and l will trust k
Transpose Trust	B^T	i's trust of j causes j to develop some level of trust towards i
Trust Coupling	BB^T	i and j trust k, so if k trusts i, k should imply trusting j.

4.2. The Propagation of Trust and Distrust

Our end goal is to produce a final matrix, F, from which we can read off the computed trust and distrust of any two users. In Table 9, there are three cases to define B (The belief matrix) and P(k) for the propagation of trust and distrust after k-steps, given an initial trust and distrust matrix.

$$F = \sum_{k=1}^{k} V^k P^k.$$

Table 9. Three cases to define B and P.

Case	Description	Defining Matrices
Trust Only	In this case, distrust is ignored completely and simply propagate trust score.	B = T, P(k) = C^k
One-step Distrust	Assume that when a user distrusts somebody, he/she also discounts all judgments made by that person. Therefore, distrust is only propagated in one-step while trust may propagate in multiple steps.	B = T, P(k) = C^k * (T—D)
Propagated Distrust	Assume that trust and distrust both propagate together and that they can be treated as two ends of a continuum.	B = T—D, P (k) = C^k

After getting P(k) by considering different cases, we substitute P(k) into to F. F is defined as the final matrix representation that concludes that the user's view of another user.

The value, k is an integer. We need to consider another constant value, V as a discount factor to penalize the lengthy propagation steps.

4.3. Evaluation of H2

The aim of this experiment is to predict distrust from only trust and answer whether distrust is a negation of trust. [12] conducted this experiment to evaluate the user-user trust and distrust relationships in trust recommender systems such as Epinions and eBay. This result will be evaluated after running the trust predictor. In this experiment, a user with a trust relationship is denoted as AT while a user without a trust relationship is denoted as AD. We assume that x% of users will establish a trust relationship, while x% of users will establish a distrust relationship, while x% of users is the predicted distrust relationship. The performance is computed by:

$$H = \frac{A_D^x \cap A_D^P}{A_D^x}$$

The H is computed as a conditional probability. This is because the aim of this experiment is to determine the performance of distrust by running it in a distrust trust propagation algorithm (dTP) as trust predictor to predict trust. In this experiment, x is varied as 50–100 as indicated in Table 10, and it is denoted as % of users. We want to see if the value of x will affect trust performance.

Table 10. Performance of Distrust-Trust Propagation Predictor, dTP.

x (%)	Balance Theory	Multi-Faceted Model
50	4.967×10^{-43}	1.3765×10^{-49}
60	2.8650×10^{-51}	1.0166×10^{-58}
70	1.5071×10^{-59}	2.0135×10^{-68}
80	9.5269×10^{-68}	5.5458×10^{-77}
90	5.0114×10^{-76}	4.0965×10^{-86}
100	3.1681×10^{-84}	3.0253×10^{-95}

In the balance theory concept, the input for representing matrix T is a triad that is combined with three positive sign (+,+,+) indicates that the friend of my friend is my friend, and the matrix D is combined with one positive sign and two negative signs (−,−,+). The matrix representation is a 3 x 3 matrix. In the multi-faceted model for the input we have chosen for representing matrix T as a trust matrix. We have taken one sample from the user evaluation result and the pairs of the user that are a best friend to each other (rating >7.5). We chose a constant 0.5 that indicates the value of the distrust relationship between two strangers. In both cases, C is computed by defining a constant of a, b, c and d. We follow [31] research by choosing a = 0.4, b = 0.4, c = 0.1, d = 0.1 that achieved a better result in the propagation of trust and distrust. After that, we chose 0.5 as a constant of V as 0.5 is suited better than fewer steps of propagation. However, for A_D^x, we will use the result of one step distrust propagation (refer to Table 9) that denoted the relationship of distrust as what [12] has done. The propagated distrust indicated in Table 9 will be chosen as A_D^P to predict the distrust relationship. We have written a program to test the result. The result will be discussed and compared in the next section.

5. Results and Findings

Based on the testing process for the above scenarios, two different results were obtained. Because the result was in matrix form that result was rounding by finding the average. The results are tabulated in the table below:

The result obtained from the experiment was nearly zero, the smallest one was 3.0253×10^{-95}, and the largest value was only 4.967×10^{-43}. The results show that distrust is not a negation of trust. This was because if distrust is the negation of trust, a low trust score should accurately indicate distrust. Performance is worsened if the percentage of users is increasing. These results are relatively small and suggest that a low trust score cannot be used to predict distrust. A low trust score and distrust are two different cases. Hence, distrust is not the negation of trust.

5.1. Findings and Discussions

Social scientists, who support distrust as a new dimension of trust, argue that pairs of users with distrust have a very low trust score [13,26] phenomenon is especially true with social media data because the users of social media are distributed worldwide, and many pairs of users in the trust network do not know each other. In the context of location-based services, a similar result may occur too. However, in this research, the adoption of a multi-faceted trust framework together with balance theory enhances the overall trust score. The reason is that prior evaluation in scoring the user based on certain attributes contributes to a better adoption of balance theory.

Hypothesis 1 (H1): *The balance theory within distrust in trust can enhance trust management model in location-based services (LBS).*

However, the performance of balance theory is better than the multi-faceted model; this is because the value we used in balance theory is imprecise. We used 0 or 1 to represent trust and distrust. The balance theory without an actual trust value is not accurate compared with the multi-faceted model that has the real trust score rated by users. The bigger the value, the more precise the result is. When compared with the result in [12] who adopted the algorithm in SNS, [12] achieved a better result because the dataset he used is bigger. The number of trust nodes and distrust nodes is greater. Therefore, by using a larger dataset, the result can be improved. Overall, both H1 and H2 were tested with the findings supporting Hypothesis 1 which is the balance theory within distrust in trust can enhance trust management model in LBS. In contrast, for Hypothesis 2, the findings suggest that distrust is not a negation of trust.

5.2. Theoretical and Practical Applications

The main findings of this work suggest that social theories used to prove distrust models can be applicable towards IoT applications such as messaging and location-based services. The adoption of balance theory on its own is incapable of enhancing any trustworthiness towards any application. However, when the theory is merged with a multi-faceted model, overall trust can be enhanced. This proved that the multi-facet trust model is applicable for usage with IoT applications, and theories such as balance theory have a positive impact on this kind of model. A multi-faceted model must be carefully modelled to fit IoT applications, and the significance of using eight attributes is applicable to IoT-based applications. However, this model is only tested on computers and smartphones without even considering the different architectures that both employ. However, on its own, balance theory employed in LBS does not have a positive impact. Overall, the findings of this study conclude that balance theory must be merged with a multi-facet model to achieve its full potential in terms of high trust ratings. Second, this study demonstrates that distrust is not a negation of trust in LBS applications. The result is consistent with [12] results. Thus, in an IoT-based application, trust and distrust must be tackled as separate representation.

In terms of practicality, a social theory such as balance theory which is used in a distrust model, focuses on social relationships such as a friendship/stranger linkage that has a positive impact on location-based applications. The acceptance of balance theory becomes stronger when a multi-faceted model is applied prior to any usage of an application. Thus, the relationship between trust model and balance theory enhances the trustworthiness of users in the adoption of applications, which are distributed and used in the different context of users. However, even though balance theory, combined with a multi-faceted model, enhanced trustworthiness towards any applications, the negation between trust and distrust is not achieved. In brief, if a user has low trust towards any LBS application/the users using this app or even feedback obtained from the apps' usage, the balance theory or multi-faceted adoption has no significant contribution in its distrust representation. Thus, trust is not a negation of distrust.

5.3. Limitations of the Study

There are some limitations that need to be considered with respect to this study. They are:

First, the dataset collected is much smaller in contrast to the work of [14,31]. Previous studies have used bigger datasets with 12,353 users, 322,044 trust relations and 41,253 distrust relations for evaluation. The size of data reflects the results obtained especially in the matrix factorization steps.

Second, the trust representation of the previous work is a huge interconnected and distributed network. However, in this study, the user and user relationship are represented in balance theory triads. Third, this study has two scenarios of matrix representation, balance theory and multi-faceted model, which might cause differences in the results.

6. Conclusions and Future Work

In this study, a multi-faceted model and the balance theory concept were implemented in the proof of concept of an LBS application to tackle security issues such as fake reviews and to increase the trustworthiness of a user towards LBS applications. In our proof of concept prototype, eight trust attributes were implemented in MiniLBS, so that users can classify their friends in a personalized way. From the result of testing, we proved that balance theory is workable in the proof of concept for the prototype. In future work, the incorporation of balance theory with other theories such as status theory should be done. In addition, the current performance of the balance theory concept can be implemented in real-life situations within any IoT application, specifically the LBS system thereof.

Author Contributions: Conceptualization, M.M.S.; Formal analysis, W.S.L.; Funding acquisition, M.A.; Investigation, W.S.L.; Project administration, M.M.S. and M.A.; Software, W.S.L.; Supervision, M.M.S.; Writing – original draft, M.A.; Writing – review & editing, M.M.S.

Funding: This research received no external funding.

Acknowledgments: This research was supported by the Bridging Research Grant, Universiti Sains Malaysia (USM) No: 304/PNAV/631627

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yun, H.; Dongho, H.; Choong, C.L. Understanding the use of location-based service applications: Do privacy concerns matter? *J. Electron. Commer. Res.* **2013**, *14*, 215.
2. Beldad, A.; Margareta, C.K. Here's my location, for your information: The impact of trust, benefits, and social influence on location sharing application use among Indonesian university students. *Comput. Hum. Behav.* **2015**, *49*, 102–110. [CrossRef]
3. Malm, A. Mobile Location-Based Services. Available online: http://www.berginsight.com/ReportPDF/ProductSheet/bi-lbs9-ps.pdf (accessed on 2 August 2017).
4. Steiniger, S.; Neun, M.; Edwardes, A. Foundations of Location Based Services. 2006. Available online: http://www.e-cartouche.ch/ (accessed on 3 August 2017).
5. Wang, G.; Bolun Wang, T.W.; Ana Nika, H.Z.; Ben, Y.Z. Defending against sybil devices in crowdsourced mapping services. In Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services, Singapore, 25–30 June 2016.
6. Howard, A. What Is a Sybil Attack? 2018. Available online: https://www.toptenreviews.com/software/articles/what-is-a-sybil-attack (accessed on 14 October 2018).
7. Kumar, S.; Neil, S. False information on web and social media: A survey. *arXiv* **2018**, arXiv:preprint 1804.08559.
8. Pomerantsev, P.; Michael, W. *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*; Institute of Modern Russia: New York, NY, USA, 2014; Volume 14.
9. Yan, Z.; Peng, Z.; Athanasios, V.V. A survey on trust management for Internet of Things. *J. Netw. Comput. Appl.* **2014**, *42*, 120–134. [CrossRef]
10. Sherchan, W.; Surya, N.; Cecile, P. A survey of trust in social networks. *ACM Comput. Surv. (CSUR)* **2013**, *45*, 47. [CrossRef]
11. Teo, Y.C. *Multi-Faceted Model Computation Using Recommender & Enhanced Action-Based Trust for Online Social Network (OSN)*; University of Science Malaysia: Penang, Malaysia, 2015.
12. Tang, J.; Xia, H.; Huan, L. Is distrust the negation of trust? the value of distrust in social media. In Proceedings of the 25th ACM Conference on Hypertext and Social Media, Santiago, Chile, 1–4 September 2014.
13. Jøsang, A.; Elizabeth, G.; Michael, K. Analysing topologies of transitive trust. In Proceedings of the First International Workshop on Formal Aspects in Security & Trust (FAST2003), Pisa, Italy, September 2003.
14. Tang, J.; Huan, L. Trust in social computing. In Proceedings of the 23rd International Conference on World Wide Web, Seoul, Korea, 7–11 April 2014.
15. Liu, B.C. *User-Centric Personalized Multifacet Model Trust in Online Social Network*; FYP Project, School of Computer Sciences; University of Science Malaysia: Burdock, Penang, Malaysia, 2014.

16. Statista. Number of Location-Based Service Users in the United States from 2013 to 2018 (in Millions). 2015. Available online: http://www.statista.com/statistics/436071/location-based-service-users-usa/ (accessed on 15 October 2017).
17. Clarinox, T.P.L. Real Time Location Systems. Available online: http://www.clarinox.com/docs/whitepapers/RealTime_main.pdf (accessed on 23 August 2018).
18. Cooney, M. How do mobile location services threaten users? Available online: https://www.networkworld.com/article/2360206/how-do-mobile-location-services-threaten-users.html (accessed on 23 August 2018).
19. Rec, ITUT. *X. 800 Security Architecture for Open Systems Interconnection for Ccitt Applications*; ITU-T (CCITT) Recommendation: Geneva, Switzerland; Available online: https://www.itu.int/rec/T-REC-X.800-199103-I (accessed on 4 March 2018).
20. Thomas, J.E. Statements of Fact, Statements of Opinion, and the First Amendment. *Calif. Law Rev.* **1986**, *74*, 1001. [CrossRef]
21. Fallis, D. A Functional Analysis of Disinformation. iConference 2014 Proceedings. Available online: https://www.ideals.illinois.edu/handle/2142/47258 (accessed on 5 June 2018).
22. Skyrms, B. *Signals: Evolution, Learning, and Information*; Oxford University Press: Oxford, UK, 2010.
23. Sinai, M.B.; Nimrod Partush, S.Y.; Eran, Y. Exploiting social navigation. *arXiv* arXiv:preprint 1410.0151, 2014.
24. Lewicki, R.J.; Daniel, J.M.; Robert, J.B. Trust and distrust: New relationships and realities. *Acad. Manag. Rev.* **1998**, *23*, 438–458. [CrossRef]
25. Grandison, T.; Sloman, M. *Trust Management Tools for Internet Applications*; Nixon, P., Terzis, S., Eds.; Trust Management. iTrust 2003. Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2692.
26. Marsh, S.; Dibben, M.R. *Trust, Untrust, Distrust and Mistrust – An Exploration of the Dark(er) Side*; Herrmann, P., Issarny, V., Shiu, S., Eds.; Trust Management. iTrust 2005. Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3477.
27. Cofta, P. Distrust. In Proceedings of the 8th International conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet, Fredericton, New Brunswick, Canada, 13–16 August 2006.
28. Manoj, R.J.; Chandraseka, A. A Literature Review on Trust Management in Web Services Access Control. *Int. J. Web Serv. Comput.* **2013**, *4*, 1.
29. Heider, F. Attitudes and cognitive organization. *J. Psychol.* **1946**, *21*, 107–112. [CrossRef] [PubMed]
30. Cartwright, D.; Frank, H. Structural balance: A generalization of Heider's theory. *Psychol. Rev.* **1956**, *63*, 277–293. [CrossRef]
31. Guha, R.; Ravi Kumar, P.R.; Andrew, T. Propagation of trust and distrust. In Proceedings of the 13th international conference on World Wide Web, New York, NY, USA, 17–20 May 2004.
32. Leskovec, J.; Daniel, H.; Jon, K. Predicting Positive and Negative Links in Online Social Networks. In Proceedings of the 19th international conference on World wide web, Raleigh, North Carolina, USA, 26–30 April 2010.
33. Leskovec, J.; Daniel, H.; Jon, K. Signed networks in social media. In Proceedings of the SIGCHI conference on human factors in computing systems, Montréal, QC, Canada, 22–27 April 2010.
34. Quinn, K.; David, L.; O'Sullivan, D.; Vincent, P.W. An analysis of accuracy experiment carried out over of a multi-faceted model of trust. *Int. J. Inf. Secur.* **2009**, *8*, 103–119. [CrossRef]
35. Chieng, L.B.; Manmeet, M.S.; Zarul, F.Z.; Rohail, H. Multi-Facet Trust Model for Online Social Network Environment. *Int. J. Network Secur. Its Appl.* **2015**, *7*, 1. [CrossRef]