IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 21, 2017, accepted September 18, 2017, date of publication September 22, 2017,
date of current version February 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2755058

A Situational Awareness Trust Evolution Model for Mobile Devices in D2D Communication

JINGJING GUO[1], JIANFENG MA[2], (Member, IEEE), XINGHUA LI[1], (Member, IEEE), TAO ZHANG[3], AND ZHIQUAN LIU[4]

[1]School of Cyber Engineering, and the Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an 710071, China
[2]School of Cyber Engineering, and the State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China
[3]School of Computer, Xidian University, Xi'an 710071, China
[4]College of Information Science and Technology, and the College of Cyber Security, Jinan University, Guangzhou 510632, China

Corresponding author: Tao Zhang (taozhang@xidian.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61602360, in part by the National High Technology Research and Development Program(863 Program) under Grant 2015AA016007 and Grant 2015AA017203, in part by the National Natural Science Foundation of China under Grant 61602365 and Grant 61372075, and in part by the 111 Project under Grant B16037.

ABSTRACT Device-to-device (D2D) communication is a promising concept for improving user experiences and resource utilization in cellular networks. This type of communication enables two or more mobile devices in proximity to establish local links, coordinated by a base station, to perform direct data exchange. The benefits of D2D communication include ubiquitous computing and communication, enhanced energy efficiency, creation of new services, and so on. However, how to establish the trust relationship between two devices is a base problem that should be solved. In this paper, we propose a situational awareness trust evolution model for mobile devices involved in D2D communication. Compared with available trust evaluation schemes, we consider the comprehensive situation that a mobile device may encounter. We use what a device wants and what it can obtain to depict the situation of the device when given a concrete interaction (transaction). We give the method to get quantitative description of such information, and then the coefficients of the new proposed trust evolution function can be determined. To demonstrate the efficiency of our method, we conduct some experiments to show the properties of our method, and the results show that our trust evolution scheme is consistent with the intuition about trust in real life. Furthermore, we compare our scheme with two state-of-the-art dynamic trust evaluation schemes in different usage scenarios of mobile devices. The results show that our scheme can perform well in all scenarios, whereas the other two schemes can perform well only in some of the tested scenarios.

INDEX TERMS Mobile device, trust evolution mechanism, situational awareness, D2D communication.

I. INTRODUCTION

The increasing awareness that trust is a prerequisite for interactions among entities in distributed networks has led to many trust management schemes for various systems. Most traditional trust models are pre-configured with static behavior, which means that the same behavior will always result in the same trust evaluation result. These methods are designed to protect entities in a certain system with a fixed network structure and communication pattern. Some available works about trust evolution consider the dynamicity of trust in terms of the passing of time [1]–[3]. These works presented how trust value or trust-related evidence decays over time; however, the evolution pattern is also configured manually before the first use of the trust evaluation scheme [4].

Currently, device-to-device (D2D) communication provides a future in which mobile devices can establish a direct connection to perform various tasks. D2D communication is a promising concept for improving user experiences and resource utilization in cellular networks, and it enables two or more mobile devices to establish local links to perform direct data exchange. This means that mobile devices may encounter multifarious environments rather than remain in a single situation [5]; thus, its trust evolution pattern is increasingly dependent on its real-time environment, including the physical location, network environment, the presence of other entities (e.g., objects and people) [6], and so on. Therefore, it is clear that the trust evolution pattern of mobile devices should no longer be static during the entire life of

the network system, even for a given trustor, trustee and transaction.

Although people now realize the dynamicity of the trust model with a given certain trustor, trustee and transaction, the available models generally only take the experience about the involved transaction into account to evaluate a trustee's trust level. In fact, an entity's real-time attitude or standard to establish a trust relationship with others should vary with the situation that it is encountering. In reality, there are many factors that influence a mobile device's trust evolution pattern toward a certain trustee and transaction. In addition to the historical experience of the transaction, environmental factors play an increasingly more important role in the trust evolution process. Both the virtual and physical environment of a mobile device can be variable, e.g., a laptop can be placed in a fixed position or move at a high speed, and it can also be involved in a static or dynamic network topology. If a mobile device adopts a static trust evaluation scheme for a certain transaction, then the effect of the scheme may be heavily discounted or even result in an incorrect result if the involved environment changes. Therefore, mobile devices urgently need an adaptive trust evolution model that can perform well in changing environments such that it can cater to the use features of mobile devices in D2D communication.

Considering the above problem, we present a situational awareness trust evolution scheme for mobile devices in this paper. In this scheme, the trust evaluation standard of a mobile device varies with its changing situation. This property means that given the interaction history between two mobile devices, the trust evaluation results will be different in different situations. Here, the situation of a device depicts a comprehensive picture integrating what it wants and what it can obtain now. We will explain the ''situation'' in detail in the following sections.

The main contributions of this paper are as follows. First, we formalize the situation that a mobile device may encounter. Furthermore, we propose a trust evolution scheme whose independent variable is the amount of net positive interactions between the trustor and trustee devices. The coefficients of the trust evolution function are not constant; rather, they vary with the trustor device's situation information such that the trust evolution pattern can always cater to the current situation and provide a reasonable trust evaluation result. In this case, the same behavior presented by a device's counterpart in different situations will result in different trust levels.

The remainder of this paper is organized as follows. Section II presents the related works. Then, we analyze the situation space of a mobile device in Section III. Section IV introduces the underlying factors that influence the trust evolution pattern of a mobile device. The proposed trust evolution scheme is described in Section V. In Section VI, we present the experiments that we performed to verify the effect of our method, followed by the discussion in Section VII. Finally, we present our conclusions and outline a few directions for future work in Section VIII.

II. RELATED WORKS

Trust as the best long-term rational strategy has been potentially applied to a variety of cases [7]. Many researchers have proposed trust models for different systems using different theories and technologies. Some logical-based methods were proposed many years ago [8], [9]. These credential-based methods use predefined logical inference rules to assert that an entity has a certain attribute [10] or role [11], which is similar to authentication schemes [12]–[15]. In the open network environment, the experience-based computational trust model is the most commonly used model [16]. The past behavior of an entity is used as the evidence for calculating its reputation or trust level, for which probabilistic approaches are widely used [17]. In these models, different trust metrics were taken into account to obtain a more comprehensive and reasonable result [18]. However, they were generally designed for systems with static structures and communication patterns, such as wireless sensor networks [19], [20], cloud computing [21], and ad hoc networks [22], [23]; thus, the behavior of these models is also pre-configured. In these models, given the same interaction history, they will always provide the same evaluation result without considering the factors that may influence the trust evaluation standard or tendency.

Regarding D2D communications, as a promising technology for the next-generation mobile communication networks (5G), its security problem, which is essential for the success of D2D services, has not yet been thoroughly studied in the literature. In such a communication network, a mobile device may encounter various situations, e.g., disconnected from its preferred security infrastructure, surrounded by stranger devices, involved in an emergency task, and so forth. This means that mobile entities should be able to evaluate the performance of other entities and make decisions in the presence of unknown and uncontrollable environments. It is clear that a trust management scheme is a great choice for solving this problem, whereas traditional computational trust models cannot address this problem. One way to address this challenge is to construct a proper trust framework for D2D communication similar to how people use trust in daily communications [24]. Specifically, we should combine the traditional trust management with the dynamics and flexibility of the human notion of trust.

Jensen *et al.* proposed a dynamic trust evolution model that depends on an entity's inclination to trust others [25]. In their scheme, an entity's inclination is influenced by its interaction experience. A successive good experience will lead to an optimistic trust evolution pattern, which makes trust grow more rapidly in the following interactions (the curve of the trust function becomes sharper), and vice versa. Here, the dynamicity of the trust preference is considered to be only influenced by the experience. Saied *et al.* designed a trust management system for the Internet of Things considering the variety of contexts and services [26]. The context that they defined includes the concrete service involved, the capability of the trustee, the trustee's current trust level and the time.

The dynamicity that the authors considered is the update of the recommender's trust level and the trustee's level. Thus, this scheme also did not consider the various scenarios that an entity may encounter. Mhetre *et al.* presented a trust scheme for D2D communications based on fuzzy theory [27], although they only used the fuzzy theory in the calculation process. The core idea of this model is still gathering the direct trust score, indirect trust recommendation and the uncertain of the recommendation to obtain a comprehensive trust score. In fact, referring to the dynamicity, trust management for mobile devices in D2D communications is naturally related to context awareness. Any data that can be used to improve security solutions can be viewed as contextual information, such as social environment, surrounding objects, user habits and so on. Marsh introduced the concept of ''device comfort'', which expects a mobile device to have the comprehensive ability to collect, recognize, and utilize its constantly changing context to infer its security situation and take the corresponding action to protect itself [28]. Marcus *et al.* proposed the logical foundations of an adaptive security infrastructure concept that took the environment into account [29]. There are also some studies in computer security that consider contextual factors [30]–[32].

Regarding the impact of contextual factors in the process of establishing trust, there are also available context-aware trust models [26], [33]–[36]. Reference [26] studied a trust management system for the Internet of Things considering the context. Reference [33] proposed a context-aware computational trust model based on Bayesian networks. In this model, the context and the result of each interaction between two agents are recorded, and the Bayesian network is updated forthwith based on the agent's dynamic behavior. Reference [34] presented a context-aware trust prediction method for distributed networks. In this model, the authors emphasized that the context may influence the behavior of an entity; thus, the same entity has different behaviors in different contexts. Reference [35] described a context-aware trust model for location-based service recommendation (LBSR). The authors took the service type and service price as the context, which is a factor in the trust evaluation function. The function is the weighted sum of four types of factors that influence the trust of a service provider defined by the author.

Although the trust models mentioned above took context into account to reflect the dynamicity of trust, they did not provide an upper level analysis about the dynamicity of trust evolution in a varying environment. We need to determine the mechanism of trust evolution for mobile devices to obtain a trust model that matches the use features of mobile devices.

III. THE SITUATION SPACE OF A MOBILE DEVICE

As described above, the trust evolution of a mobile device is influenced by its real-time situation; thus, we should first analyze the situation space of a mobile device to clearly determine which situations a mobile device may encounter when it is involved in a transaction.

In the real world, if a graduate student has obtained many offers and all of them came from well-known companies with excellent benefits and a promising future, he or she will have a high standard for choosing a job. In this case, it is very difficult for a company to be considered as a good choice in his or her mind. Conversely, a student who needs money to survive but has not received any offers may accept a job that is considered too bad in the aforementioned student's mind. In this case, the student has a strong motivation to receive a job offer because of the limitation of the resource and the imperious demand. Thus, different situations lead to different attitudes, and different attitudes will lead to different evaluation preferences.

According to sociology and psychology, we define a mobile device's situation as ''what does the device want and what it can obtain now''. ''What does a device want'' means its requirement to the counterpart and the degree of urgency of the device to perform an interaction. ''What a device can obtain'' means all the information that the device can gather to assist the trust evaluation. We know that it is not realistic and is unnecessary to consider all aspects and information in the trust evaluation process; thus, we select the most representative factors as the content of what a device can obtain. These factors are the physical environment, virtual environment and the counterpart candidates' trust state. In general, the higher a device's requirements are, the more cautious attitude it will hold when it establishes a trust relationship with others. In addition, the better the quality of the resource that it can obtain, the easier it is for the device to trust others, and vice versa. The requirement of a device to its counterpart in this paper means the requirement to the trustee's behavior. A device may accept a counterpart who performed a considerable amount of negative behavior previously, whereas it may only accept an entity who is always well behaved. Here, the better the candidates' historical behavior (trust level) and the more comfortable the environment (including both physical and virtual) feels, the higher the quality of resources that the device receives.

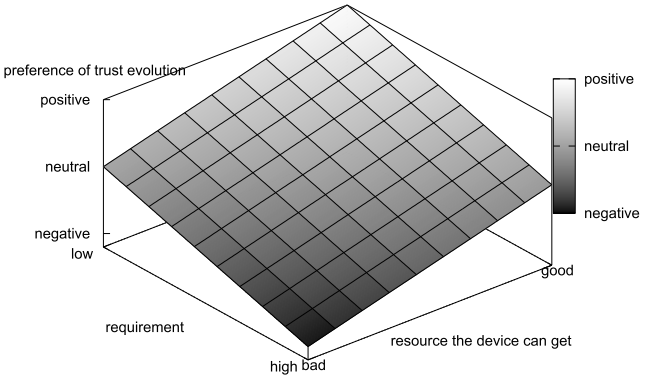


FIGURE 1. Situation space of a mobile device.

In Fig. 1, we depict a mobile device's situation space and its corresponding preference in terms of the trust evaluation.

As shown in this figure, there are four types of situations in which a mobile device may be involved: high requirement and bad resource, high requirement and good resource, low requirement and bad resource, and low requirement and good resource. According to the above analysis, in different situations, a device should have different trust evaluation standards corresponding to different trust evolution patterns. In the next section, we will introduce the underlying factors that influence the trust evolution pattern in detail.

IV. UNDERLYING FACTORS INFLUENCING THE TRUST EVOLUTION PATTERN

In this section, we will analyze the underlying factors that influence a mobile device's trust evolution pattern. Jensen *et al.* introduced three types (neutral, optimistic and cautious) of trust evolution patterns in [25]. Neutral evolution pattern means that the graph of the trust evaluation function is a straight line. Optimistic evolution pattern means that a device tends to trust others based on a few experiences; thus, the slope of the trust function becomes increasingly smaller as the interaction increases, whereas a cautious device presents the opposite behavior. Ultimately, a device's preference of establishing a trust relationship with others is essential for determining the trust evolution pattern.

In the above, we define the trust situation of a mobile device as a combination of all the things that are occurring and related to the trust decision. Specifically, the trust situation includes what does the mobile device want and what it can obtain. In the following, we will analyze the factors that influence a device's preference in the trust establishment process given a concrete transaction.

A. HISTORICAL EVIDENCE ABOUT THE CURRENT TRANSACTION

Given a transaction, the first factor that influences the preference of trust establishment is the historical evidence about the current transaction. As Jensen *et al.* stated, it is reasonable that a device with a pleasant interaction history will have more confidence for the following interactions. Thus, the more successful interactions that a device has experienced, the more positive preference it has to trust others, as well as the higher standard it has for its counterparts, and vice versa.

For example, assume that a smartphone is connected to the WiFi in its owner's office and that there are several neighbors ($N_1, N_2, \cdots, N_s$) that interacted with the smartphone to perform transaction t_i. If $N_1, N_2, \cdots, N_{s-1}$ interacted with the smartphone 1000 times within a period and all of them were successful, while N_s interacted with the smartphone only twice, it is difficult to view N_s as completely trustworthy even though the two interactions were all successful because compared with most other counterparts, the evidence that supports its trustworthiness is relatively weak. If the overall interaction history between the smartphone and its neighbors is unsatisfactory, then the trust level of a counterpart should evolve more rapidly than the former case because the bad experience can lower the exception and standard of the device to its counterpart.

We can use the trust level of the trustor device's counterpart devices in terms of the involved transaction to indicate the trustor's historical evidence. For simplicity and without loss of accuracy, we can use the average trust level (denoted as *atl*) of the trustor device's counterpart devices who have interactions with it in terms of the currently considered transaction and the average number of good interactions (denoted as *ani*) between the trustor and these counterparts to indicate the historical evidence of the trustor. The larger *atl* is, the higher the trustor's requirement will be. Moreover, the larger *ani* is, the more times that good interactions are needed by a trustee to obtain a high trust level.

B. GENERAL COMFORT LEVEL

The second factor is the general comfort level of the trustor device. General comfort level was proposed by Stephen Marsh [37]. It is a general feeling of a device in terms of the security of its environment without considering a specific task. This factor considers the device's physical and virtual location, the trust of the device to its user and the historical behavior to depict the secure status of the device unaffected by the current use of the device. In the trust evolution process, the trust of the device to its user will not influence the trust evolution pattern of the device; thus, we adopt the transformation of Stephen's general comfort level. Our definition of the general comfort level of a device is shown below.

$$ComfortG = Loc_D + Soc_D \tag{1}$$

1) Loc_D is the feeling of the device about its physical environment. In this paper, we only consider the physical location. If the device is in a comfort zone, such as its owner's home, then its value should be high.
2) Soc_D is the feeling of the device about its virtual environment (in other words, its network environment).

We can abstract the environment space of a device using the device's physical location and the dynamics of the topology of the device's network. If the physical location is familiar to the device, we can state that the physical environment is comfortable, and the more familiar the location is, the more comfortable the device feels, and vice versa. If the device is involved in a network in which it has relatively fixed neighbors, we state that its virtual environment is comfortable, whereas if its topology is highly dynamic, we say that the device will feel uncomfortable about the virtual environment, which will result in a cautious attitude in the trust evaluation process. The network topology and the physical location can both be detected by the sensors embedded in mobile devices.

In the following, we use some symbols to represent the elements mentioned above:

1) *loc*: It is the device's current physical location, which can be represented by its latitude and longitude.
2) *S*: It is the set of *SSID* currently detected by the mobile device.

3) $N(t)$: It is the set of the mobile device's one-hop neighbors at the tth time slot.
4) α: It is used to indicate the dynamics of the network topology in which the device is involved.

Now, we show how to calculate each component that influences the general comfort level. The *LocD* can be calculated using the following function:

$$LocD = \begin{cases} 1 & if\ loc \in comfortzone \\ 0 & if\ loc \in uncomfortzone \\ max\{0, 1 - \frac{dis(loc, comfortzone)}{D}\} & else \end{cases} \quad (2)$$

where *comfortzone* and *uncomfortzone* are predefined geographic areas where the device does or does not like to be; when the device is neither in a comfort zone nor in an uncomfort zone, we use a function *dis* to compute the closest physical distance between *loc* and the predefined comfort zone to measure its comfort level to the physical environment. D is a predefined boundary value. We can see that the farther the device is from its comfort zone, the lower its comfort level to the physical environment will be. When the distance exceeds D, its comfort level will decrease to 0.

The *SocD* can be obtained using the following functions:

$$SocD = (S_a + S_c) \cdot \alpha, \quad (3)$$

$$S_a = \Sigma_{i \in S}(familiarity(i) \times signal\_strength(i)) \quad (4)$$

S_a in Eq. 3 reflects the confidence of a mobile device toward its network environment. In Eq. 4, $familiarity(i)$ indicates the familiarity of the device to the network whose *SSID* is i. We can use the proportion of time that the device accesses this network during a predefined period as the familiarity of this network; thus, there is $\Sigma_{i \in S} familiarity(i) \leq 1$. $signal\_strength(i)$ is a function that maps the signal strength of i to a real number falling between 0 and 1. The larger the value of $signal\_strength(i)$ is, the stronger the signal of the network is. Eq. 4 means that the more familiar the network environment is to the device, the more willing the device is to trust others, and vice versa. For example, a device should be more cautious in trusting an entity when involved in an open and strange network environment.

$$S_c = \begin{cases} 1 & if\ x \geq T \\ x/T & else \end{cases} \quad (5)$$

S_c in Eq. 3 reveals the feeling of a mobile device toward its surrounding devices. In Eq. 5, x is the number of known devices currently around the mobile device, and T is a predefined boundary value indicating that if there are no less than T known devices perceived by the mobile device, the value of S_c can reach the maximum. The larger the value of S_c is, the more security the mobile device feels about its surrounding devices, and correspondingly, it has a greater tendency to trust others.

α in Eq. 3 is the different degree of surrounding neighbors of a mobile device between two successive time slots, which can represent the dynamicity of its network topology. Eq. 6 shows how to calculate α.

$$\alpha = \frac{|N(t) \cap N(t-1)|}{|N(t) \cup N(t-1)|} \quad (6)$$

As shown in the above formulas, the general comfort level is proportional to the confidence of the device's physical location and the network environment in terms of security state. It influences the device's preference of the trust evolution pattern. The higher the general comfort level of a device is, in other words, the higher the quality of resource that it receives, the more positive is the attitude that the device will hold toward building a trust relationship with others, and vice versa.

C. EMERGENCY DEGREE OF THE TASK

The third aspect that influences a mobile device's preference to establish a trust relationship is the degree of urgency of the transaction that the device is being or to be involved in. It is reasonable that the more urgent the task is, the more tolerance the mobile device will have toward the environment and its counterpart. As Stephen stated, in some cases, regardless of what may be occurring to cause risk, communication must persist. We use the symbol μ in the following content to indicate the degree of urgency of the communication. The smaller μ is, the more urgent the communication requirement is, and thus, the lower its requirement to the counterpart will be.

V. TRUST EVOLUTION MODEL

Above, we analyzed the influence of each situation factor on the preference of the trust evolution pattern. In this section, we introduce the proposed adaptive trust evolution model. Furthermore, we also describe how to determine the coefficients of the adaptive trust function according to the trustor device's situation. We use the definition of trust value proposed by Stephen Marsh that the trust value is a real number in the closed interval $[-1, 1]$, where -1 represents complete distrust and 1 means complete trust [37]. A value of 0 means that the trustor has an uncertain viewpoint regarding a trustee's trust level.

Assume that there are two mobile devices D_1 and D_2; we use $T_{D_1}^{D_2}$ to denote the trust of D_1 to D_2. The result of every interaction between them will have a certain utility to the evolution of $T_{D_1}^{D_2}$. Here, utility means the quantity of the change of $T_{D_1}^{D_2}$ caused by a certain interaction between D_1 and D_2. Similar to the trust in human society, the utility of different interactions between two devices should not be a constant. In addition, the utility of the same interaction between two devices should also not be a constant in different situations.

We assume that in device D_1's view, a device needs "N" net positive interactions (denoted as *npi*) to achieve the maximum trust value. Here, net positive interaction is the result

of the number of positive interactions minus that of negative interactions considering the aging factor. Given a period of time, assume that there are m interactions between D_1 and D_2. These interactions are $\{e_1, e_2, \cdots, e_m\}$, ordered by the time of their occurrence. The time of occurrence of e_i is earlier than that of e_{i+1}. The value of e_i is 1 if e_i is a successful interaction; otherwise, its value is -1. We denote the forgetting factor as σ. Then, the decay function shown below can compute the net positive interaction between the two devices. In Eq. 7, $\triangle t_i$ represents the time interval between the current time and the time that e_i occurred.

$$npi = \left\lfloor \sum_{i=1}^{m} (e_i \times \sigma^{\triangle t_i}) \right\rfloor \tag{7}$$

From the above, we know that the smaller N is, the more quickly a device's trust can achieve a certain level, which means the more contribution that a positive interaction provides to the device's trust evolution. According to the analysis in Section IV, we know that the value of "N" is influenced by the degree of urgency of D_1's communication requirement. In addition, "N" should also be directly proportional to device D_1's historical evidence (*ani*, mentioned in Section IV.*A*). Therefore, the value of N can be obtained using Eq. 8, where β is the factor to adjust the relationship between *ani* and N. From Eq. 8, we can observe that if D_1 has a weak risk tolerance, then μ can be set to greater than 1 to enhance the evaluation standard. If D_1 is in an emergency situation, then μ can be set to smaller than 1.

$$N = \beta \cdot ani \cdot alt \cdot \mu \tag{8}$$

When $\mu = 0$, it means that any device can be viewed as a trusted object irrespective of how bad its behavior is; this may occur in the urgent situation in which the communication must persist regardless of what may be occurring. In this case, the trust evaluation function will be a constant function. In this paper, we use the notation $T_{D_1}^{D_2}(s)$ to indicate the trust level of device D_1 to device D_2 when D_1 receives s net positive services from D_2. Thus, we have the following:

$$T_{D_1}^{D_2}(s) = 1, \quad if\ N = 0 \tag{9}$$

In the following, we consider the situation in which $N \neq 0$. The following formula shows the evolution of the trust utility given a series of successive interactions between D_1 and D_2. Here, we first consider the utility when the value of *npi* between the two devices is positive. We know that there is a correlation between the trust utilities of successive interactions; thus, we use Eq. 10 to measure the utility of each positive interaction between two devices.

$$a_i = \begin{cases} a_{i-1} + t, & 0 < i \leq N \\ 0, & i > N \end{cases} \tag{10}$$

In Eq. 10, a_i is the utility of a net positive interaction to $T_{D_1}^{D_2}$ when D_1 and D_2 have had $i-1$ net positive interactions. It is a nonnegative number. The same is true that $-a_i$ is the utility of a fallacious interaction.

If mobile device D_2 has $s(s \geq 0)$ net positive interactions with D_1, then the value of $T_{D_1}^{D_2}(s)$ should be the sum of the utilities of these s net positive interactions, which can be expressed as the formula shown below.

$$T_{D_1}^{D_2}(s) = \sum_{i=1}^{s} a_i = \begin{cases} \frac{t}{2}s^2 + \left(\frac{1}{N} - \frac{N \times t}{2}\right)s, & N \geq s \geq 0 \\ 1, & s > N \end{cases} \tag{11}$$

From Eq. 11, we can observe that t decides the preference of the device about trust evolution. If a mobile device holds a neutral attitude regarding trust evolution, then the utility of each positive interaction should be the same and t should be set to 0. If the device has a positive preference, then it means that the positive interactions that occurred earlier would have more utility than the later ones (a_i should be smaller than a_{i-1}), and therefore, t should be a negative number. For the same reason, t should be positive if a mobile device holds a cautious attitude. Thus, we can see that t represents the preference (attitude) of a device about trust evolution.

We know that the value of N is determined by the historical evidence and the degree of urgency of the communication requirement. A device's attitude should be influenced by its general comfort level. If it feels that the environment is not very comfortable (such as the surrounding devices are all unknown), then it will be more cautious when building a trust relationship with others. In the following, we will show how to decide the value of t (the attitude of the device) based on the general comfort level. According to the previous assumption, the trust value of D_2 with N net positive interactions should be 1; then, we have the following:

$$T_{D_1}^{D_2}(N) = \sum_{i=1}^{N} a_i = 1 \tag{12}$$

By substituting Eq. 10 into Eq. 12, we obtain the following:

$$\begin{cases} a_1 = \frac{1}{N} - \frac{N-1}{2}t \\ a_N = a_1 + (N-1)t \end{cases} \tag{13}$$

If $t > 0$, then a_1 is the smallest among a_i; otherwise, a_N is the smallest. Since the utility of any net positive interaction (a_i) should be nonnegative, to guarantee this condition, we have that t should fall between $\frac{2}{N \times (N-1)}$ and $-\frac{2}{N \times (N-1)}$.

From the previous section, we know that the ranges of *LocD* and *SocD* all fall between 0 and 1; thus, we have $0 \leq ComfortG \leq 2$. We now define a function $f : ComfortG \rightarrow t$ to determine t based on *ComfortG*. Its definition is as follows:

$$t = f(ComfortG) = \frac{2}{N \times (N-1)}(1 - ComfortG) \tag{14}$$

When $ComfortG = 2$, which means that the general comfort level of the device is at the highest level, the mobile device will relax its vigilance, and the trust evolution pattern will become optimistic; thus, t should be equal to $-\frac{2}{N \times (N-1)}$, and vice versa.

When the number of net positive interactions between D_1 and D_2 is negative ($npi < 0$), the graph of the trust evolution function should be symmetrical about the origin with the image of Eq. 11 ($npi > 0$); thus, when $s < 0$, we have the following:

$$T_{D_1}^{D_2}(s) = \begin{cases} -\frac{t}{2}s^2 + \left(\frac{1}{N} - \frac{N \times t}{2}\right)s, & -N \le s < 0 \\ -1, & s < -N \end{cases} \quad (15)$$

We now obtain the entire trust evolution model. From Eqs. 11 and 15, we can observe that the trust evolution pattern is influenced by two coefficients, t and N. N decides the overall utility of each positive interaction, and it is influenced by the historical evidence and the degree of urgency of the communication. t decides the preference of the device in terms of trust evolution (including optimistic, neutral and negative), which is decided by the parameter N and the device's general comfort level about the involved environment.

VI. EXPERIMENTAL

In this section, we will present the experiments that we conducted to verify the feasibility and effectiveness of our method. First, we show the features of the proposed method, and then we compare our method with other dynamic trust models to validate its efficiency.

A. FEATURES OF OUR METHOD

From the above, we know that the trust evolution is influenced by two coefficients, t and N; thus, we first test the effect of the two coefficients in the trust evolution process.

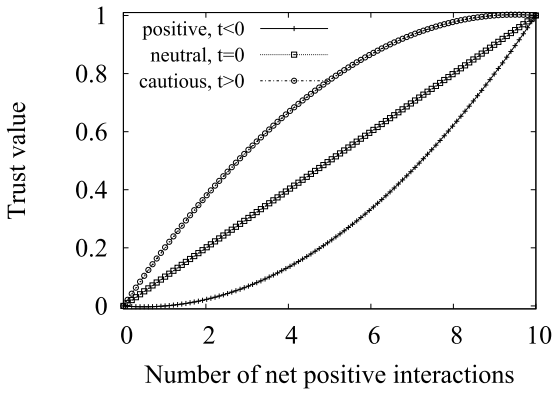


FIGURE 2. Trust evolution pattern under varying preferences (t).

First, we show the trust evolution pattern of $T_{D_1}^{D_2}$ with varying preferences (different values of t). In this experiment, we assume that N equals 10, which means that the trust of D_2 can reach 1 when the number of net positive interactions between D_1 and D_2 is 10. As shown in Fig. 2, the evolution processes of D_2's trust value under the three preferences are different. If D_1 holds a positive preference, then it means that D_1 tends to trust others. A few good interactions can make D_1 assign a high trust level to its counterpart. Conversely, if D_1 holds a negative preference, then there must be sufficient net positive interactions to make it assign a high trust level to its counterpart. In other words, the first few positive interactions have little utility to the trust value evolution.

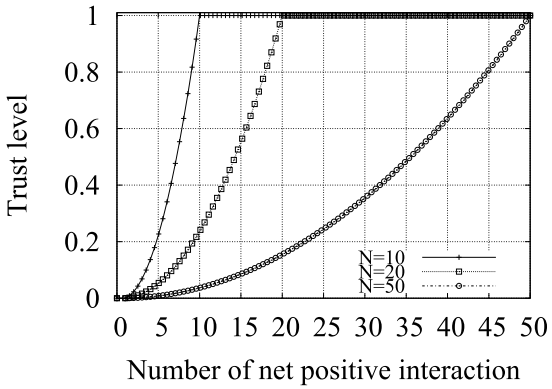


FIGURE 3. Trust evolution pattern under varying N.

Then, given the preference of a mobile device (we assume that the trustor holds a positive preference in this experiment), we test the trust evolution pattern of its counterpart with different values of N (the least number of net positive interactions needed to obtain the highest trust value). As shown in Fig. 3, the smaller the value of N is, the fewer net positive interactions that are needed for the trustee to reach a certain trust level. When $N = 10$, a mobile device's trust value can reach 0.6 if it has 8 net positive interactions with the trustor, whereas its trust value is less than 0.2 when $N = 20$ with the same amount of net positive interactions. Therefore, if the trustor is in an emergency situation, it can set N to a smaller number such that its standard of trusting others can be lower. If a device is being or to be involved in a sensitive interaction including some privacy information, N can be set to a larger number such that only the object that has many net positive interactions with the device can be viewed as trustworthy to perform the interaction.

B. A TRACE-DRIVEN EXPERIMENT-BASED FEASIBILITY ANALYSIS

To validate the feasibility of our method, we conducted a trace-driven experiment. We monitored a mobile device in the real world and collected its usage scenarios for more than one year. The collected information includes its physical location, surrounding devices, accessing network and so on. Here, we name the monitored device as A, and its owner is *Alice*. A may interact with other devices in various environments for a certain task. During the monitored period, on normal days, A is placed in *Alice*'s home and office most of the time. When *Alice* traveled abroad for a week during the summer holiday, she took A with her.

Fig. 4 shows the virtual environment of A during normal days and vacation days. The virtual environment includes its surrounding devices perceived by Bluetooth and its accessing network. We say that the surrounding device or the accessing network is a stranger for A if it is perceived only a few times.

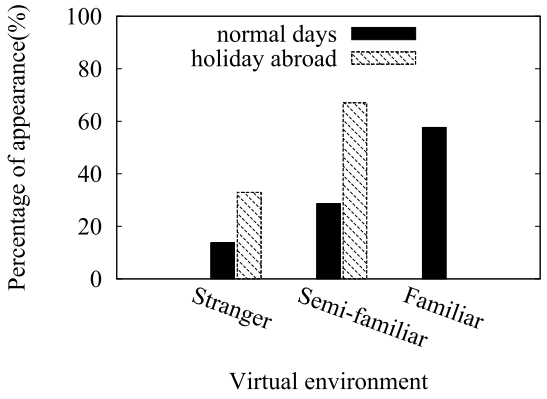


FIGURE 4. Comparison of virtual environment of *D* on normal days and vacation days.

If the times that the surrounding nodes or network appear exceed a certain number, we say that they are the familiar ones. In other cases, the surrounding devices or the accessing network can be viewed as semi-familiar. We explore the proportion of occurrences of A perceiving the familiar devices, strangers and semi-familiar devices. As shown in Fig. 4, A feels more familiar with the virtual environment on normal days than on vacation days. Therefore, its corresponding comfort level is higher on normal days because most times, A communicates with its familiar devices, such as *Alice*'s colleagues' devices in the work place and other devices owned by *Alice* at home.

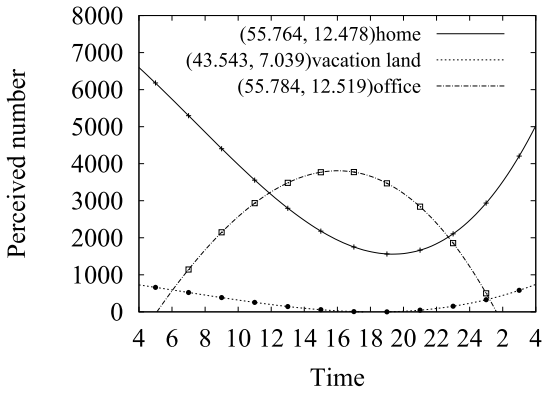


FIGURE 5. Comparison of physical environment of *D* on normal days and vacation days.

Regarding the physical environment, it is clear that A also feels more comfortable on normal days than on vacation days, as shown in Fig. 5. In most cases, A appears in *Alice*'s home or work place, which are all familiar places for it, whereas A is unfamiliar with the vacation location where it rarely appears. According to our method, A should hold a positive preference in terms of the trust evolution on normal days with familiar physical and virtual environments. When A is at the vacation spot, it will hold a cautious attitude toward the interaction counterpart. This means that A will not provide a high trust level to a strange entity after a few positive interactions when it is at the vacation location.

As indicated by the above two figures and analysis, the result of A's trust preference decided by our method in the trace-driven experiment is in accordance with our intuition about trust.

C. COMPARISON WITH OTHER METHODS

In this part, we will compare our method with available trust models considering dynamicity. In existing trust models, we select two state-of-the-art models, which are SecuredTrust [38] (a dynamic trust model for multiagent systems) and dynamic trust model for cloud computing [39](for brevity, we will use CTrust in the following). Both of these models consider the dynamicity of the trust evaluation process.

TABLE 1. Scenarios considered in this experiment.

	devices' behaviors (exclude D_1)	history evidence	General comfort level
1	one confusing and others bad	good	uncomfortable
2	one confusing and others bad	bad	uncomfortable
3	one confusing and others good	good	comfortable
4	one confusing and others good	bad	comfortable

In our experiments, a mobile device named D_1 is connected to a network that has 100 mobile devices within it. To simulate the real world, we assume that there are three types of behaviors among these mobile devices: good behavior, confusing behavior and bad behavior. Well-behaved devices cooperate with others and provide satisfactory service to the counterpart, whereas bad devices always provide unsatisfactory interactions. Confusing devices alternate between exhibiting good and bad behavior. We will show the trust evaluation process of the two selected models and our model under different scenarios, which are shown in Table I. As shown, in each scenario, the behavior of devices, D_1's historical evidence and its general comfort level are different, whereas the transactions involved in each scenario are the same.

TABLE 2. The values of parameters used in this experiment.

parameter	value	meaning
σ	0.95	aging factor of evidence
μ	1	urgency degree of the communication
$Loc_D + Soc_D$	0.2 — bad environment 0.7 — good environment	general comfort level

We assume that D_1 always performs well. In each iteration, D_1 interacts with fixed devices, each of which has different types of behavior, and other devices randomly perform transactions with each other. We use D_1 to evaluate the trust level of each type of device. The values of the parameters used in the experiments are listed in Table II. We set N in the good and bad historical evidence environments as 300 and 100, respectively.

We performed this experiment for a total of 1000 iterations, which are equally divided into four slots. We assume that the

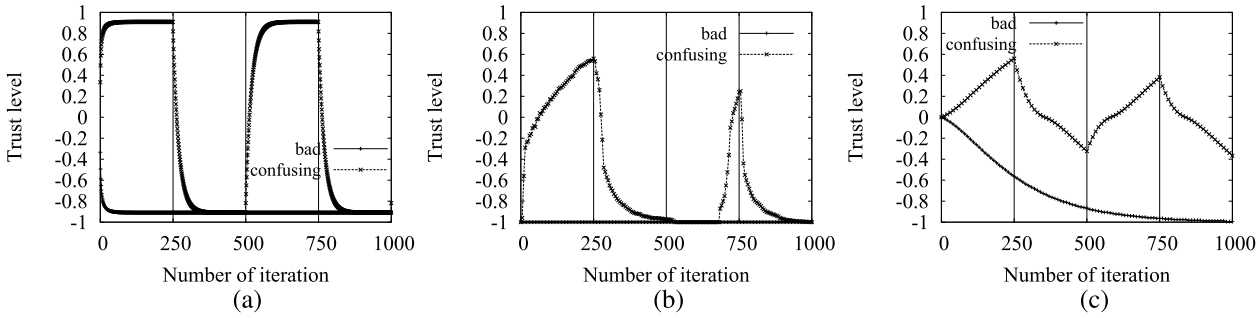


FIGURE 6. Comparison of our method with CTrust and SecuredTrust in scenario 1 shown in Table I. (a) CTrust. (b) SecuredTrust. (c) Our method.

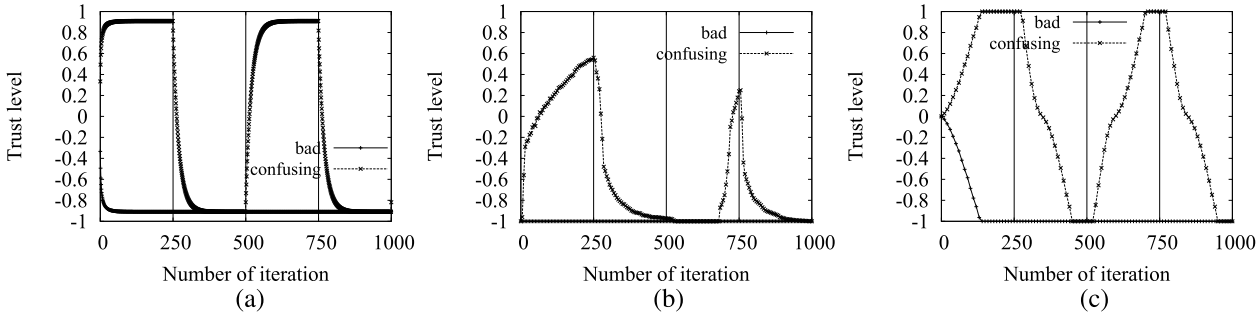


FIGURE 7. Comparison of our method with CTrust and SecuredTrust in scenario 2 shown in Table I. (a) CTrust. (b) SecuredTrust. (c) Our method.

confusing devices' behavior oscillates between good and bad from one slot to the next, starting with good behavior.

In the following, we show the trust level evolution of each type of behavior in D_1's view under different scenarios because it is very important for an effective trust model to distinguish different behaviors in any scenario. Fig. 6 presents the result of trust evolution with each method under scenario 1 in Table 1. In this scenario, the historical evidence of D_1 is good. When it is in a new location and connected to an unknown network, the devices within the network are all ill-behaved except for a confusing device, which alternates between exhibiting good and bad behavior. In such an environment, D_1's general comfort level becomes quite low; thus, it should doubt other entities. For the confusing device, although it does not always perform well, compared with other devices, it is better. Because of the good historical experience, the values of D_1's *atl* and *ani* will be relatively high. Correspondingly, the utility of each interaction to the trust evolution will be relatively low, which means that the trust level evolves smoothly. As shown in Fig. 6, under the CTrust model, the confusing device's trust level increases so fast that it can reach a quite high trust level with a few positive interactions. In the SecuredTrust model, the trust evolution pattern is in agreement with our analysis, whereas during the 500*th* and 750*th* iterations, the trust level of the confusing device is the same as the bad ones even though it performs well. In this situation, D_1 cannot distinguish these two types of behaviors; thus, the success interaction ratio of D_1 will inevitably decrease. Because of considering the comprehensive situation of the mobile device, the result of our method meets the above analysis.

Fig. 7 shows the development of the trust level for each type of behavior in the second scenario. Device D_1 is in the same situation as that used in Fig. 6 except D_1's historical evidence is bad. This means that its historical counterparts mostly have a low trust level, and they have a few good historical interactions; thus, the utility of each interaction may be higher in terms of the trust evolution. Because of the low general comfort level, D_1 should still hold a cautious attitude toward others. We can see that with our method, a device needs less positive interactions to achieve a high trust level, and similarly, a few negative interactions will lead to a relatively low trust level. Furthermore, different behaviors can be distinguished by D_1, except for the beginning of the third slot. For CTrust, it performs reasonably in terms of the fast increase and decrease in trust level. Regarding SecuredTrust, it has the same problem as in the experiment shown in Fig. 6.

We now consider the third scenario in Table I. Because D_1's general comfort level is high, D_1 will hold a positive preference to trust others. Its good historical experience makes the utility of each interaction relatively low. Fig. 8 shows the result with the three methods. Using the CTrust method, a device can obtain a high trust level with only a few positive interactions, which is not reasonable in a environment where there are many high trust level counterparts that previously had many good interactions with D_1. Furthermore, during the third slot, the confusing device can reach the same trust level as the good device in a short

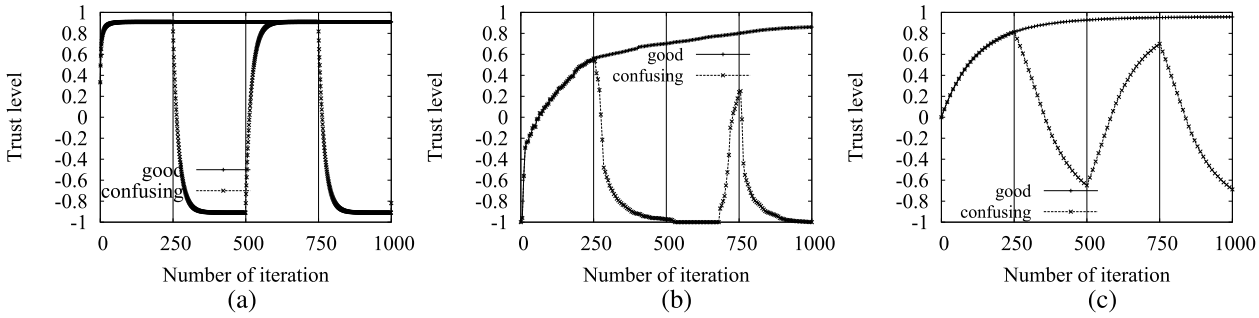


FIGURE 8. Comparison of our method with CTrust and SecuredTrust in scenario 3 shown in Table I. (a) CTrust. (b) SecuredTrust. (c) Our method.

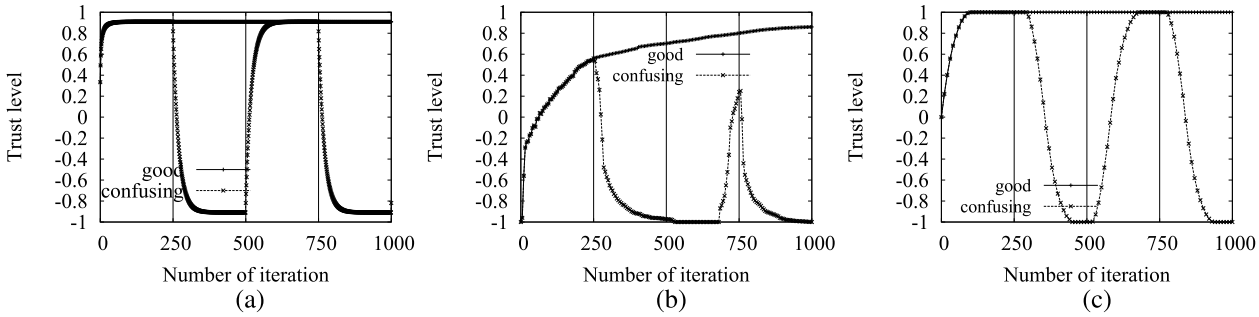


FIGURE 9. Comparison of our method with CTrust and SecuredTrust in scenario 4 shown in Table I. (a) CTrust. (b) SecuredTrust. (c) Our method.

time. Although the confusing device behaves well during this period, it should also be distinguished from those that always perform well; otherwise, it will make some attacks possible, such as a selective behavior attack. For the SecuredTrust method, its performance is reasonable and similar to that of our method.

The final scenario that we test is the same as the third scenario except that the historical experience of D_1 is bad. The result is shown in Fig. 9. According to the previous analysis, we can see that our method is closer to the desired result. Using the CTrust model, the trust level of a device increases and decreases rapidly, which is reasonable because of the bad experience, whereas the problem still exists during the third slot as mentioned above. We can see that the SecuredTrust model's performance is the same as that shown in Fig. 8(b), which means that the trust evolution pattern will not change with the trustor's historical experience. This means that the performance of the SecuredTrust method can only be configured manually rather than adaptively.

As indicated by the above experiments, the available methods for trust evaluation are only suitable for certain scenarios. In different environments or communication patterns, to maintain the efficiency of the trust evaluation, these models need to change the trust evaluation function manually. However, it is clear that mobile devices are currently no longer remaining in an invariable communication environment or managing a certain task. Our model considers the comprehensive situation that a mobile device may be involved in, and the trust evaluation function will adopt the corresponding coefficients to make the function match the current situation such that it can still provide a reasonable trust calculation result.

VII. DISCUSSION

Although we have presented experiments to prove the efficiency of our method, some issues are still worth mentioning and discussing.

In this paper, we do not consider the indirect trust, although it can also be combined into the evaluation process by transforming the indirect interaction into a net positive interaction. For example, we assume that within a predefined period, device A (trustor) has n times of net positive interaction with device B and B has m times of net positive interaction with device C. When A evaluates the trust level of C, it can transform the indirect interaction among A, B and C into a corresponding direct interaction between A and C. We define the minimum net positive interaction (N) that a device A (trustor) requires to assign the highest trust level to another device (trustee) as N_A. One way to obtain the corresponding net positive interaction between A and C is shown in Eq. 16. npi is the corresponding net positive interaction between A and C transformed from the indirect interactions. Then, A can evaluate the trust level of C based on the proposed method. In fact, we can also adopt other methods to transform the indirect interaction into a net positive interaction.

$$npi = m \times min\{1, \frac{n}{N_A}\} \tag{16}$$

Some may say that we can use a static trust evolution pattern and set different trust thresholds for different environments to achieve the same effect as the proposed

method. If so, given a transaction, the net positive interaction that an entity needs to reach the maximum trust value is a fixed number (N is a constant number), but there are some problems. Assume that a mobile device D in any situation needs n times of net positive interactions to assign the maximum trust value to other devices. If there are many mobile devices that successfully interact with D much more than n times within a predefined period, then these entities only need to maintain that there are n net positive interactions with D such that their trust value can always be the maximum. In this case, irrespective of how large the value of the trust threshold is, these devices will all be categorized into the trustworthy class even if they might have exhibited considerable malicious behavior. For example, if $N = 10$, the scheme may be effective when the device is in a situation with high motivation to establish trust with others, whereas when the mobile device is in an environment where most neighbors have more than 1000 times of positive interactions with it within a short time, a device that has made 600 good interactions and 400 bad interactions and a device that has made 1000 good interactions will both have the maximum trust value and will be seen as completely trustworthy, which is obviously unreasonable.

Many available trust models use the success ratio between the trustor and trustee to determine the trustee's trust level rather than define the concrete number of successful interactions needed to obtain a certain trust level according to the involved situation. This method can reflect the trust level of an object to a certain degree. With increasingly more interactions with a certain entity, the device will have more belief in its own experience. Assume that mobile device D interacted with two entities A and B for 10 and 1000 times separately within a certain period and that all of these interactions were successful; then, the trust levels of A and B are the same using the success-ratio-based method. However, our intuition from real life tells us that D has more confidence in B than in A in terms of their future performance. Therefore, it is desirable to have a more adaptive and situational awareness trust mechanism for mobile devices.

VIII. CONCLUSION AND FUTURE WORKS

In this paper, we propose an adaptive trust evolution mechanism for mobile devices that depends on the device's situation. We abstract the situation space of a mobile device as ''what does it want'' and ''what it can obtain''. In the proposed model, we use different coefficients to depict the situation of the device such that the trust evolution pattern of the device will vary with the changing situation. We conduct some experiments to verify the properties and the efficiency of our model. The results show that the performance of our model is in agreement with the intuition about trust in real life. Furthermore, we compare our method with other state-of-the-art dynamic trust schemes. The results show that the trust evaluation process is more reasonable in different scenarios using our model, whereas the compared models perform well only in some of the tested scenarios. In the future, we will continue to explore the trust evolution model for mobile devices in more dynamic contexts. Specifically, in this paper, we only consider the experience of a mobile device in terms of the currently involved transaction, whereas we will take the experience about other transactions into account to depict a more precise situation for mobile devices in the following work.

REFERENCES

[1] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, ''Dynamic trust management for delay tolerant networks and its application to secure routing,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 5, pp. 1200–1210, May 2014.

[2] E. Gray, C. Jensen, P. O'Connell, S. Weber, J.-M. Seigneur, and Y. Chen, ''Trust evolution policies for security in collaborative ad hoc applications,'' *Electron. Notes Theor. Comput. Sci.*, vol. 157, no. 3, pp. 95–111, 2006.

[3] C. M. Jonker, J. J. Schalken, J. Theeuwes, and J. Treur, ''Human experiments in trust dynamics,'' in *Trust Management*. Oxford, U.K.: Springer, 2004, pp. 206–220.

[4] N. Mezzetti, ''A socially inspired reputation model,'' in *Public Key Infrastructure*. Berlin, Germany: Springer, 2004, pp. 191–204.

[5] A. Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing*. San Francisco, CA, USA: New Riders, 2010.

[6] J.-M. Seigneur, G. Lenzini, and B. Hulsebosch, ''Adaptive trust management,'' in *Self-Organising Software*. Berlin, Germany: Springer, 2011.

[7] P. Cofta, ''The dynamics of confidence,'' in *Trust, Complexity and Control: Confidence in a Convergent World*. Hoboken, NJ, USA: Wiley, 2007, pp. 87–102.

[8] M. Blaze, J. Feigenbaum, and A. D. Keromytis, ''KeyNote: Trust management for public-key infrastructures,'' in *Security Protocols*. Berlin, Germany: Springer, 1999, pp. 59–63.

[9] M. Czenko, H. Tran, J. Doumen, S. Etalle, P. Hartel, and J. den Hartog, ''Nonmonotonic trust management for P2P applications,'' *Electron. Notes Theor. Comput. Sci.*, vol. 157, no. 3, pp. 113–130, 2006.

[10] C. Yuan, X. Sun, and R. Lv, ''Fingerprint liveness detection based on multi-scale LPQ and PCA,'' *China Commun.*, vol. 13, no. 7, pp. 60–65, 2016.

[11] N. Li, J. C. Mitchell, and W. H. Winsborough, ''Design of a role-based trust-management framework,'' in *Proc. IEEE Symp. Secur. Privacy*, May 2002, pp. 114–130.

[12] P. Guo, J. Wang, X. H. Geng, C. S. Kim, and J.-U. Kim, ''A variable threshold-value authentication architecture for wireless mesh networks,'' *J. Internet Technol.*, vol. 15, no. 6, pp. 929–935, 2014.

[13] Q. Jiang, Z. Chen, B. Li, J. Shen, L. Yang, and J. Ma, ''Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems,'' *J. Ambient Intell. Hum. Comput.*, vol. 5, pp. 1–13, Jun. 2017.

[14] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, ''Efficient end-to-end authentication protocol for wearable health monitoring systems,'' *Comput. Elect. Eng.*, Apr. 2017, doi: https://doi.org/10.1016/j.compeleceng.2017.03.016

[15] Q. Jiang, S. Zeadally, J. Ma, and D. He, ''Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks,'' *IEEE Access*, vol. 5, pp. 3376–3392, 2017.

[16] K. K. Bharadwaj and M. Y. H. Al-Shamri, ''Fuzzy computational models for trust and reputation systems,'' *Electron. Commerce Res. Appl.*, vol. 8, no. 1, pp. 37–47, 2009.

[17] E. D. Raj and L. D. D. Babu, ''An enhanced trust prediction strategy for online social networks using probabilistic reputation features,'' *Neurocomputing*, vol. 219, pp. 412–421, Jan. 2017.

[18] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, ''Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection,'' *IEEE Trans. Netw. Service Manage.*, vol. 9, no. 2, pp. 169–183, Jun. 2012.

[19] J. Jiang, G. Han, C. Zhu, S. Chan, and J. J. P. C. Rodrigues, ''A trust cloud model for underwater wireless sensor networks,'' *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 110–116, Mar. 2017.

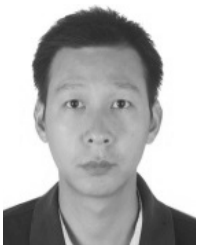
[20] W. Luo, W. Ma, and Q. Gao, ''A dynamic trust management system for wireless sensor networks,'' *Secur. Commun. Netw.*, vol. 9, no. 7, pp. 613–621, 2016.

[21] S. M. Habib, S. Ries, M. Mühlhäuser, and P. Varikkattu, ''Towards a trust management system for cloud computing marketplaces: Using CAIQ as a trust information source,'' *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 2185–2200, 2014.

[22] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.
[23] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1287–1309, 2nd Quart., 2016.
[24] S. Ries, "Trust and accountability," in *Handbook of Research on Ubiquitous Computing Technology for Real-time Enterprises*, M. Muhlhauser and I. Gurevych, Eds. Hershey, PA, USA: IGI Global, 2008, ch. 16, pp. 363–389.
[25] C. D. Jensen and T. R. Korsgaard, "Dynamics of trust evolution—Auto-configuration of dispositional trust dynamics," in *Proc. Int. Conf. Secur. Cryptogr.*, 2008, pp. 509–518.
[26] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Comput. Secur.*, vol. 39, pp. 351–365, Nov. 2013.
[27] N. A. Mhetre, A. V. Deshpande, and P. N. Mahalle, "Trust management model based on fuzzy approach for ubiquitous computing," *Int. J. Ambient Comput. Intell.*, vol. 7, no. 2, pp. 33–46, 2016.
[28] S. Marsh, P. Briggs, K. El-Khatib, B. Esfandiari, and J. A. Stewart, "Defining and investigating device comfort," *J. Inf. Process.*, vol. 19, no. 3, pp. 914–935, 2011.
[29] L. Marcus, "Local and global requirements in an adaptive security infrastructure," in *Proc. Int. Workshop Requirements High Assurance Syst. (RHAS)*, Monterey Bay, CA, USA, 2003, pp. 23–29.
[30] R. Bhatti, E. Bertino, and A. Ghafoor, "A trust-based context-aware access control model for Web-services," *Distrib. Parallel Databases*, vol. 18, no. 1, pp. 83–105, 2005.
[31] L. Korba and G. Yee, "Context-aware security policy agent for mobile Internet services," in *Proc. Int. Federation Inf. Process. Digit. Library*, vol. 190. 2010, pp. 249–259.
[32] Y. Wang *et al.*, "CATrust: Context-aware trust management for service-oriented ad hoc networks," *IEEE Trans. Serv. Comput.*, to be published. [Online]. Available: http://doi.ieeecomputersociety.org/10.1109/TSC.2016.2587259
[33] Y. Wang, M. Li, E. Dillon, L.-G. Cui, J.-J. Hu, and L.-J. Liao, "A context-aware computational trust model for multi-agent systems," in *Proc. IEEE Int. Conf. Netw., Sens. Control (ICNSC)*, Apr. 2008, pp. 1119–1124.
[34] G. Yang, Q. Sun, A. Zhou, J. Li, X. Yuan, and H. Tang, "A context-aware trust prediction method based on behavioral data analysis in distributed network environments," in *Proc. IEEE 14th Int. Conf. Dependable, Autonomic Secure Comput., 14th Int. Conf. Pervasive Intell. Comput., 2nd Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr.*, Aug. 2016, pp. 674–680.
[35] Z. Liu, J. Ma, Z. Jiang, and Y. Miao, "FCT: A fully-distributed context-aware trust model for location based service recommendation," *Sci. China Inf. Sci.*, vol. 60, no. 8, p. 082102, 2017.
[36] H. Fang, L. Xu, and X. Huang, "Self-adaptive trust management based on game theory in fuzzy large-scale networks," *Soft Comput.*, vol. 21, no. 4, pp. 907–921, 2017.
[37] M. Stephen, "Formalising trust as a computational concept," Ph.D. dissertation, Dept. Comput. Sci. Math., Univ. Stirling, Stirling, U.K., 1994.
[38] A. Das and M. M. Islam, "SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems," *IEEE Trans. Depend. Sec. Comput.*, vol. 9, no. 2, pp. 261–274, Mar./Apr. 2012.
[39] W. Wang, G. Zeng, J. Zhang, and D. Tang, "Dynamic trust evaluation and scheduling framework for cloud computing," *Secur. Commun. Netw.*, vol. 5, no. 3, pp. 311–318, 2012.

JINGJING GUO received the M.Sc. and Ph.D. degrees in computer science from Xidian University, Xi'an, China, in 2012 and 2015, respectively. She is currently a Lecturer with the School of Cyber Engineering, Xidian University. Her research interests include trust management, social networks, access control, and information security.

JIANFENG MA (M'16) received the M.E. and Ph.D. degrees in computer software and communications engineering from Xidian University in 1988 and 1995, respectively. He is currently a Full Professor and a Ph.D. Supervisor with Xidian University. His main research interests include information security, coding theory, and cryptography. He is a member of the China Computer Federation.



XINGHUA LI (M'12) received the M.E. and Ph.D. degrees in computer science from Xidian University, in 2004 and 2007, respectively. He is currently a Full Professor and a Ph.D. Supervisor with Xidian University. His main research interests include wireless networks security, privacy protection, cloud computing, software defined network, and security protocol formal methodology.

TAO ZHANG received the M.Sc. and Ph.D. degrees in computer science from Xidian University, Xi'an, China, in 2011 and 2015, respectively. He is currently an Assistant Professor with the School of Computer Science, Xidian University. His research interests include trust management, social networks, web services, and information security.

ZHIQUAN LIU received the Ph.D. degree in computer science from Xidian University, Xi'an, China, in 2017. He will serve as a Lecturer with Jinan University, Guangzhou, China. His research interests include trust management, vehicular network, and information security.